

Security Measures

Version 2026-10 Published 18 October 2026 Wecheer SA, Lausanne

This Schedule describes the technical and organizational measures Provider maintains to protect the Platform and the data processed through it. It also forms Annex B of the Data Processing Agreement (Schedule 4). Provider reviews these measures at least once a year and may update them, provided the overall level of protection is not reduced. Further detail, including penetration test summaries and security policies, is available to Client on request under confidentiality, as set out in Section 10 of the DPA.

Measures

AREA	MEASURES
Framework	Information security programme aligned with ISO/IEC 27001 and 27002, with security, asset management and data protection policies approved by management. The Platform is hosted on Amazon Web Services, whose infrastructure is ISO/IEC 27001 certified.
Encryption	Data encrypted in transit (TLS 1.2 or higher) and at rest (AES-256), including backups.
Access control	Role-based access on a least-privilege, need-to-know basis, reviewed periodically. Multi-factor authentication on administrative access. Personal credentials only. Access removed promptly when no longer needed.
Infrastructure	Cloud-native architecture on managed cloud services. Logical segregation of each client's data on the shared Platform. Data stores not exposed to the public internet. Public endpoints protected against abuse.
Application security	Authenticated, rate-limited APIs over HTTPS. Secure development practices, including code review, dependency management and automated code analysis.
Testing	Regular independent security assessments of the production Platform, and a penetration test by an independent third party at least once every 12 months. Findings prioritised by severity and remediated.

AREA	MEASURES
Monitoring	Security-relevant events on production systems logged and monitored. Administrative actions on the infrastructure recorded.
Backup and recovery	Encrypted automated backups, retained for up to 30 days. Restoration tested at least once a year.
Incident management	Documented incident response process covering identification, containment, notification and post-incident review. Personal data breaches notified to Client within 48 hours, as set out in Section 8 of the DPA.
Personnel	Confidentiality obligations for personnel and contractors. Information security training at least once a year. Approved devices and an acceptable use policy.
Data minimization and deletion	Consumer self-service account deletion, with a 30-day dormancy period, then permanent deletion or anonymization. Program-level deletion on Client's instruction. Aggregation and anonymization for analytics. Retention and deletion as set out in Section 9 of the DPA.
Sub-processors	Security due diligence before engagement. Written obligations at least as protective as this Schedule. List and locations in Annex C of the DPA.