Technical and Organizational Measures

1. General Information

The technical and organizational measures (TOM) described below set out the measures implemented by Swat.io in the context of processing on behalf of a controller (Art. 28 GDPR) to ensure an appropriate level of protection pursuant to Art. 32 GDPR. They apply to all processing of personal data carried out on behalf of the controller via the Swat.io social media management tool.

1.1 Hosting

Processing takes place primarily in data centers of Amazon Web Services EMEA SARL (Luxembourg) within the European Union. Backups are additionally maintained in a second AWS region within the EU. All personal data is processed and stored exclusively within the EU. Any transfer to third countries takes place only to the optional and contractually safeguarded extent described in Section 8.

2. Confidentiality

Measures ensuring that only authorized persons can access personal data (Art. 32(1)(b) GDPR).

2.1 Physical Access Control

Swat.io's office premises in Vienna do not contain any servers used for production purposes.

AWS Data Centers

- The operation of the data centers lies entirely with AWS. The following physical security measures are assured by AWS in its publicly documented data center controls:
- Housing of servers in dedicated security zones with controlled access
- Multi-level access controls, including multi-factor authentication and biometric procedures
- Security personnel around the clock
- Video surveillance of all entrances and security-relevant areas
- Complete logging of access events
- Access only for authorized persons with a documented business need
- Fire detection and suppression systems
- Climate and temperature monitoring
- Redundant power supply with UPS and emergency power generators (AWS Data Center Controls)
- Current list of certifications: AWS Compliance Programs

Swat.io Office Premises

- Access controlled by keys and electronic door openers.
- Reception area; external persons are accompanied.
- Video surveillance of entrance and common areas.
- Clean desk policy (see Section 7.5).

2.2 System Access Control

- Measures that prevent data processing systems from being used by unauthorized persons:
- Multi-factor authentication (MFA) for all administrative accounts and security-critical internal tools.
- Password policy in accordance with the ISMS.
- Encryption of all end-user devices.
- Access to production systems exclusively via VPN or SSH with key-based authentication.
- Remote locking of end-user devices in the event of loss, theft, or compromise via MDM.

2.3 Data Access Control

Measures ensuring that authorized persons can only access the data assigned to them:

- Role-based authorization concept (Role Based Access Control, RBAC) based on the need-to-know and least-privilege principles.
- Granular role levels at user, account, and workspace level.
- Standardized process for granting, changing, and revoking authorizations, integrated into the on-/offboarding process.
- Annual review of all granted authorizations, in particular administrative accounts.
- Logging of security-relevant access.
- Access by Swat.io support staff to controller data only takes place after the controller's explicit consent on a case-by-case basis.
- Separation of production, test, and development environments.

2.4 Separation Control

- Logical multi-tenancy separation: data of different controllers is strictly isolated from one another via the application layer and database segmentation.
- Authorization checks are performed at multiple levels, at the API and database layer.
- Production and test data are kept separate. Test environments contain no personal data.

2.5 Pseudonymization and Data Classification

- Pseudonymization is used in accordance with Art. 32(1)(a) GDPR insofar as this is compatible with the purpose of processing.
- Data classification scheme in accordance with the ISMS.

3. Integrity

Measures ensuring the integrity of personal data (Art. 32(1)(b) GDPR).

3.1 Transfer Control

- All data transmissions over public networks are encrypted using TLS 1.3 (minimum version TLS 1.2).
- Internal data traffic between production systems takes place within the AWS VPC. Connections to third-party systems are likewise TLS-encrypted.
- Web Application Firewall (WAF) active at the application layer. Protection against DDoS attacks via AWS's own mechanisms as well as WAF rules.
- Employee access to production systems exclusively via VPN.
- The use of removable media (USB sticks, external hard drives, etc.) is not permitted.

3.2 Input Control

- Security-relevant events, authentications, and changes to business data are logged.
- Activity log at the application layer: controllers can see in the tool, in a traceable manner, which user performed which action on postings, tickets, etc.
- Logs are protected against manipulation through restricted access rights and integrity verification (unique fingerprint).
- Retention period for system logs: 1–3 months, selected logs up to 12 months.
- Regular evaluation of security-relevant logs by DevOps and IT Security in accordance with the ISMS audit plan.

4. Availability and Resilience

Measures to ensure availability, resilience, and rapid recoverability (Art. 32(1)(b) and (c) GDPR).

4.1 Availability Control

- Redundant operation across at least two AWS Availability Zones in the Frankfurt region; off-site backups in a second EU region.
- UPS and emergency power generators are provided by the data center operator AWS.
- Web Application Firewall, intrusion detection (AWS GuardDuty), continuous monitoring.
- Malware protection: cloud-based architecture with MDM-managed end-user devices. File uploads in the Swat.io application are restricted to permitted MIME types.
- The availability of third-party platform APIs (Meta, X, LinkedIn, etc.) is beyond Swat.io's control. Outages of these platforms do not affect the availability of the Swat.io tool itself.

4.2 Recovery and Backup Metrics

Metric	Target Value
Recovery Time Objective (RTO)	max. 24 hours, target value 12 hours
Recovery Point Objective (RPO)	In the event of partial outages, generally < 24 hours.
Database backups	daily backups
Off-site backups	daily in a second AWS EU region, AES-256 encrypted
Backup retention	6 months; point-in-time recovery up to 1 month
Immutable backups	yes — protection against ransomware encryption
Restore test	at least annually
Contractual availability	99% per calendar year (see Terms and Conditions) — status information: status.swat.io

4.3 Emergency Management (BCM/DRP)

- Business Continuity Management (BCM) and Disaster Recovery Plan in place, documented, and tested at least annually.
- Crisis communication plan; escalation paths defined.
- Clearly defined contingency plans, reporting channels, and standard processes for the change or departure of employees.

5. Procedures for Regular Review, Assessment, and Evaluation

Measures for the continuous review, assessment, and evaluation of the effectiveness of the TOM (Art. 32(1)(d) GDPR).

5.1 Information Security Management System (ISMS)

- Implemented ISMS in accordance with ISO/IEC 27001:2022.
- Annual external surveillance and re-certification audits.
- Data protection management in accordance with the GDPR; data protection officer appointed pursuant to Art. 37 GDPR.
- A record of processing activities pursuant to Art. 30(2) GDPR is maintained for all processing on behalf of controllers and regularly updated.
- Risk management process: annual risk analysis, continuous assessment of new risks.
- Internal audit program in accordance with the ISMS.

5.2 Commissioning Control

- No processing on behalf of the controller without the controller's instructions (Art. 28 GDPR).
- Conclusion of a data processing agreement (DPA) with each controller.
- Strict selection and security/data protection due diligence of all sub-processors.
- Transparent list of the sub-processors used.
- Advance information about planned changes with a notice period of at least 30 days. Right to object within 30 days to privacy@swat.io.
- Annual review. Audit reports and certificates are obtained.

5.3 Incident Response Management

- Formal incident response process as part of the ISMS.
- Phases: identification, containment, investigation, notification, recovery, lessons learned.
- Notification of the controller in the event of a personal data breach affecting its data, without undue delay after becoming aware of it.

5.4 Privacy by Design & Default

- Security and data protection requirements are an integral part of the Software Development Lifecycle (Secure SDLC).
- Data minimization as a basic principle; restrictive default settings in the application.
- Data protection impact assessments (DPIA) pursuant to Art. 35 GDPR are carried out for new processing activities with a high risk.

5.5 Penetration Testing and Vulnerability Management

- Annual external penetration tests by a specialized external company.
- Sanitized excerpts of the test reports are made available upon request.
- Formal vulnerability management process with CVSS-based prioritization.
- Automated weekly patch updates and use of tools for the automatic monitoring of third-party dependencies.
- Security-relevant vulnerability information is made available to controllers upon request.

5.6 Support with Data Subject Rights, Deletion, and Return

- During the term of the contract: deletion regime for tickets configurable by the controller (user admin).
- After the end of the contract: Swat.io deletes or returns the commissioned data at the controller's discretion (Art. 28(3)(g) GDPR). By default, data is securely retained for up to 4 months for the possible reactivation of the customer account; upon request, immediate deletion takes place. After the period expires, the data is permanently deleted, unless statutory retention obligations preclude this.
- Data export before the end of the contract upon request in a common, machine-readable format.

- Swat.io supports the controller in fulfilling the rights of data subjects pursuant to Art. 12–23 GDPR. Requests are to be directed to privacy@swat.io. Responses are provided within the statutory period of one month (Art. 12(3) GDPR).
- Access (Art. 15) and rectification (Art. 16): data can be viewed and corrected directly in the tool by the controller.
- Restriction of processing (Art. 18) and objection (Art. 21): operational implementation by the controller; Swat.io provides the technical means and supports upon request.

5.7 Obligations to Cooperate with the Controller (Art. 28(3)(f) GDPR)

Swat.io supports the controller in fulfilling its obligations under Art. 32–36 GDPR:

- Cooperation in data protection impact assessments (Art. 35): provision of the required information on processing activities, sub-processors, security measures, and data flows.
- Cooperation in prior consultation of the supervisory authority (Art. 36).
- Provision of TOM, sub-processor list, sanitized penetration test reports, and compliance certificates upon request (Art. 32).
- Notification of personal data breaches affecting controller data in accordance with Section 5.3 (Art. 33–34).

Requests are to be directed to privacy@swat.io.

6. Encryption

Pseudonymization and encryption of personal data (Art. 32(1)(a) GDPR).

Area	Measure
At rest	AES-256 for all production databases, search indexes, object storage, and backups. End-user devices: full disk encryption enforced via MDM.
In transit	TLS 1.3 for all web and API traffic; minimum version TLS 1.2.
Key management	Central key management via AWS Key Management Service (KMS). Private keys stored exclusively at AWS. No plaintext export.

7. Organizational Control

Organizational measures to safeguard personnel, end-user devices, and internal processes.

7.1 Employee Selection, Confidentiality, and Background Checks

- Security and background check before commencement of employment. Type and scope depend on role and security-relevant responsibility.
- Written commitment of all employees and external service providers to data secrecy (Art. 28(3)(b) GDPR) as well as to the confidentiality obligation.
- Confidentiality obligation continues beyond the end of the employment relationship.

7.2 Training and Awareness

- Mandatory annual training of all employees on information security and data protection.
- Participation documented and verifiable.
- Onboarding training for new employees.

7.3 On- and Offboarding

- Standardized onboarding process: granting and documentation of all authorizations, device issuance, training, confidentiality declaration.
- Standardized offboarding process: immediate revocation of all authorizations, return and wipe of devices, revocation of physical access.

7.4 Mobile Device Management (MDM)

- All end-user devices issued by Swat.io are centrally managed via MDM.
- Enforced security measures: up-to-date operating system updates, full disk encryption, screen lock, remote wipe capability.
- Devices are securely erased before reuse or decommissioning.
- Swat.io operates remote-first. All protective measures mentioned here also apply in the home office or outside the office premises.

7.5 Clean Desk and Clear Screen Policy

- Confidential documents are stored securely outside office hours.
- Screens are locked when leaving the workstation.

7.6 Network Security at the Location

- No critical servers in the office access network.
- Separation of production and office networks.

7.7 Change Management

- All code changes are made via a central Git repository with mandatory pull-request review and linkage to issue tracking.
- Infrastructure-as-code; security considerations are a continuous part of the development lifecycle.

7.8 Asset Management and Secure Disposal of Data Media

- All IT assets (end-user devices, software, cloud services) are inventoried within the ISMS and assigned to a named asset owner.
- The end-user device inventory is maintained centrally via the Mobile Device Management.
- Decommissioning of end-user devices takes place after cryptographic erasure of all data media via the MDM or the operating system.
- The erasure procedure is based on recognized standards for secure data deletion.
- Defective or no longer erasable data media are physically destroyed.

8. Third-Country Transfer and Supplementary Measures

Data processing takes place exclusively within the EU. A data transfer to the USA takes place exclusively within the scope of the optionally bookable Postmark/ActiveCampaign service (the "Forward ticket by email" and "Email channels" functions). This function can be deactivated at any time upon request.

8.1 Legal Bases

- Adequacy decision EU-US Data Privacy Framework (July 2023).
- Standard Contractual Clauses (SCCs) pursuant to Implementing Decision (EU) 2021/914.

9. AI Functions and the EU AI Act

- AI functions are optional and must be explicitly activated by the controller's administrator at the organization level.
- Models used: models from OpenAI and/or Anthropic (Claude via AWS Bedrock); each hosted in EU regions.
- Controller data is used neither for training nor for fine-tuning AI models.
- According to the current state of assessment, the AI functions do not meet the requirements for high-risk AI systems.
- Internal and third-party risk assessments for AI functions are carried out regularly; the AI results are regularly checked for bias.
- Technical protective measures against prompt injection and data poisoning at the infrastructure level.

Review and Approval

Created by	Patrick Diem (ISO), Judit Palotai (DPO)
Approval date	July 1, 2026
Version	1.0
Next review	no later than 12 months after approval or in the event of significant changes