Technisch-organisatorische Maßnahmen

1. Allgemeine Angaben

Die nachfolgenden technischen und organisatorischen Maßnahmen (TOM) beschreiben die von Swat.io im Rahmen der Auftragsverarbeitung (Art. 28 DSGVO) implementierten Maßnahmen zur Gewährleistung eines angemessenen Schutzniveaus gemäß Art. 32 DSGVO. Sie gelten für sämtliche Verarbeitungen personenbezogener Daten im Auftrag des Auftraggebers über das Swat.io Social Media Management Tool.

1.1 Hosting

Die Verarbeitung erfolgt primär in Rechenzentren von Amazon Web Services EMEA SARL (Luxemburg) innerhalb der Europäischen Union. Backups werden zusätzlich in einer zweiten AWS-Region innerhalb der EU geführt. Sämtliche personenbezogenen Daten werden ausschließlich innerhalb der EU verarbeitet und gespeichert. Eine Übermittlung in Drittländer findet nur in dem unter Abschnitt 8 beschriebenen, optionalen und vertraglich abgesicherten Umfang statt.

2. Vertraulichkeit

Maßnahmen, die sicherstellen, dass nur Berechtigte personenbezogene Daten zur Kenntnis nehmen können (Art. 32 Abs. 1 lit. b DSGVO).

2.1 Zutrittskontrolle

Die Büroräume von Swat.io in Wien enthalten keine produktiv genutzten Server.

AWS-Rechenzentren

Der Betrieb der Rechenzentren liegt vollständig bei AWS. Die folgenden physischen Sicherheitsmaßnahmen sind von AWS in den öffentlich dokumentierten Datacenter-Controls zugesichert:

- Unterbringung der Server in dedizierten Sicherheitszonen mit kontrolliertem Zutritt
- Mehrstufige Zutrittskontrollen, u.a. Multi-Faktor-Authentifizierung und biometrische Verfahren
- Sicherheitspersonal rund um die Uhr
- Videoüberwachung sämtlicher Eingänge und sicherheitsrelevanter Bereiche
- Lückenlose Protokollierung der Zutritte
- Zutritt ausschließlich für autorisierte Personen mit dokumentierter geschäftlicher Notwendigkeit
- Brand-Erkennungs- und -Löschsysteme
- Klima- und Temperaturüberwachung

- Redundante Stromversorgung mit USV und Notstromaggregaten (AWS Data Center Controls)
- Aktuelle Liste der Zertifizierungen: AWS Compliance Programs

Swat.io Büroräume

- Zutritt geregelt durch Schlüssel und elektronische Türöffner.
- Empfangsbereich; externe Personen werden begleitet.
- Videoüberwachung der Eingangs- und Allgemeinbereiche.
- Clean-Desk-Policy (siehe Abschnitt 7.5).

2.2 Zugangskontrolle

Maßnahmen, die verhindern, dass datenverarbeitende Systeme von Unbefugten genutzt werden:

- Multi-Faktor-Authentifizierung (MFA) für alle administrativen Konten und sicherheitskritische interne Tools.
- Passwort-Policy gemäß ISMS.
- Verschlüsselung sämtlicher Endgeräte.
- Zugriff auf produktive Systeme ausschließlich über VPN bzw. SSH mit Schlüsselauthentifizierung.
- Fern-Sperrung von Endgeräten bei Verlust, Diebstahl oder Kompromittierung über das MDM.

2.3 Zugriffskontrolle

Maßnahmen, die sicherstellen, dass Berechtigte nur auf die ihnen zugewiesenen Daten zugreifen können:

- Rollenbasiertes Berechtigungskonzept (Role Based Access Control, RBAC) auf Basis des Need-to-know- und Least-Privilege-Prinzips.
- Granulare Rollenstufen auf Benutzer-, Account- und Workspace-Ebene.
- Standardisierter Prozess für Vergabe, Änderung und Entzug von Berechtigungen, integriert in den On-/Offboarding-Prozess.
- Jährliche Überprüfung sämtlicher vergebener Berechtigungen, insbesondere administrativer Konten.
- Protokollierung sicherheitsrelevanter Zugriffe.
- Zugriffe von Swat.io-Support-Mitarbeitenden auf Auftraggeberdaten erfolgen nur nach ausdrücklicher Zustimmung des Auftraggebers im Einzelfall.
- Trennung von Produktiv-, Test- und Entwicklungsumgebung.

2.4 Trennungskontrolle

- Logische Mandantentrennung: Daten verschiedener Auftraggeber werden über die Anwendungsschicht und Datenbank-Segmentierung strikt voneinander isoliert.
- Berechtigungsprüfungen erfolgen mehrstufig auf API- und Datenbankebene.
- Produktiv- und Testdaten sind voneinander getrennt. Testumgebungen enthalten keine personenbezogenen Daten.

2.5 Pseudonymisierung und Datenklassifikation

- Pseudonymisierung wird gemäß Art. 32 Abs. 1 lit. a DSGVO eingesetzt, soweit dies mit dem Verarbeitungszweck vereinbar ist.
- Datenklassifikationsschema gemäß ISMS.

3. Integrität

Maßnahmen, die die Unversehrtheit personenbezogener Daten gewährleisten (Art. 32 Abs. 1 lit. b DSGVO).

3.1 Weitergabekontrolle

- Sämtliche Datenübertragungen über öffentliche Netze erfolgen verschlüsselt mittels TLS 1.3 (Mindestversion TLS 1.2).
- Interner Datenverkehr zwischen produktiven Systemen erfolgt innerhalb der AWS-VPC. Verbindungen zu Drittsystemen sind ebenfalls TLS-verschlüsselt.
- Web Application Firewall (WAF) aktiv auf Anwendungsebene. Schutz vor DDoS-Angriffen über AWS-eigene Mechanismen sowie WAF-Regeln.
- Mitarbeiterzugriff auf Produktivsysteme ausschließlich über VPN.
- Verwendung von Wechseldatenträgern (USB-Sticks, externe Festplatten o.ä.) ist nicht zulässig.

3.2 Eingabekontrolle

- Sicherheitsrelevante Ereignisse, Authentifizierungen und Geschäftsdatenänderungen werden protokolliert.
- Activity-Log auf Anwendungsebene: Auftraggeber sehen im Tool nachvollziehbar, welcher Benutzer welche Aktion an Postings, Tickets etc. vorgenommen hat.
- Logs werden vor Manipulation durch eingeschränkte Zugriffsrechte und Integritätsprüfung (eindeutiger Fingerprint) geschützt.
- Aufbewahrungsdauer System-Logs: 1–3 Monate, ausgewählte Logs bis zu 12 Monate.
- Regelmäßige Auswertung sicherheitsrelevanter Logs durch DevOps und IT-Security gemäß ISMS-Prüfplan.

4. Verfügbarkeit und Belastbarkeit

Maßnahmen zur Sicherstellung der Verfügbarkeit, Belastbarkeit und raschen Wiederherstellbarkeit (Art. 32 Abs. 1 lit. b und c DSGVO).

4.1 Verfügbarkeitskontrolle

- Redundanter Betrieb über mindestens zwei AWS-Availability Zones in der Region Frankfurt; Off-Site-Backups in einer zweiten EU-Region.
- USV und Notstromaggregate werden vom Rechenzentrumsbetreiber AWS bereitgestellt.

- Web Application Firewall, Intrusion Detection (AWS GuardDuty), kontinuierliches Monitoring.
- Schadsoftwareschutz: Cloud-basierte Architektur mit MDM-verwalteten Endgeräten. Datei-Uploads in der Swat.io Application werden auf zulässige MIME-Typen beschränkt.
- Die Verfügbarkeit von Drittplattform-APIs (Meta, X, LinkedIn etc.) liegt außerhalb der Kontrolle von Swat.io. Ausfälle dieser Plattformen wirken sich nicht auf die Verfügbarkeit des Swat.io-Tools selbst aus.

4.2 Wiederherstellungs- und Backup-Kennzahlen

Kennzahl	Zielwert
Recovery Time Objective (RTO)	max. 24 Stunden, Zielwert 12 Stunden
Recovery Point Objective (RPO)	Bei Teilausfällen i.d.R. < 24 Stunden.
Datenbank-Backups	tägliche Backups
Off-Site-Backups	täglich in einer zweiten AWS-EU-Region, AES-256 verschlüsselt
Aufbewahrung Backups	6 Monate; Point-in-Time-Recovery bis zu 1 Monat
Immutable Backups	ja — Schutz gegen Ransomware-Verschlüsselung
Restore-Test	mindestens jährlich
Vertragliche Verfügbarkeit	99 % im Kalenderjahr (siehe AGB) — Statusinformation: status.swat.io

4.3 Notfallmanagement (BCM/DRP)

- Business Continuity Management (BCM) und Disaster Recovery Plan vorhanden, dokumentiert und mindestens jährlich getestet.
- Krisenkommunikationsplan; Eskalationswege definiert.
- Klar geregelte Notfallpläne, Meldewege und Standardprozesse für den Wechsel oder das Ausscheiden von Mitarbeitenden.

5. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Maßnahmen zur kontinuierlichen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der TOM (Art. 32 Abs. 1 lit. d DSGVO).

5.1 Informationssicherheits-Managementsystem (ISMS)

- Implementiertes ISMS nach ISO/IEC 27001:2022.
- Jährliche externe Überwachungs- und Re-Zertifizierungsaudits.
- Datenschutzmanagement gemäß DSGVO; Datenschutzbeauftragte gemäß Art. 37 DSGVO benannt.
- Verzeichnis von Verarbeitungstätigkeiten gemäß Art. 30 Abs. 2 DSGVO wird für sämtliche Auftragsverarbeitungen geführt und regelmäßig aktualisiert.
- Risikomanagement-Prozess: jährliche Risikoanalyse, kontinuierliche Bewertung neuer Risiken.
- Internes Audit-Programm gemäß ISMS.

5.2 Auftragskontrolle

- Keine Auftragsdatenverarbeitung ohne Weisung des Auftraggebers (Art. 28 DSGVO).
- Abschluss eines Auftragsverarbeitungsvertrags (AVV/DPA) mit jedem Auftraggeber
- Strenge Auswahl und Sicherheits-/Datenschutz-Due-Diligence aller Sub-Auftragsverarbeiter.
- Transparente Liste der eingesetzten Sub-Auftragsverarbeiter.
- Vorab-Information über geplante Änderungen mit einer Frist von mindestens 30 Tagen. Widerspruchsrecht innerhalb von 30 Tagen an privacy@swat.io.
- Jährliche Überprüfung. Audit-Reports und Zertifikate werden eingeholt.

5.3 Incident-Response-Management

- Formaler Incident-Response-Prozess als Teil des ISMS.
- Phasen: Identifikation, Eindämmung, Untersuchung, Benachrichtigung, Wiederherstellung, Lessons Learned.
- Information des Auftraggebers im Falle einer Datenschutzverletzung mit Auswirkungen auf seine Daten unverzüglich nach Kenntnisnahme.

5.4 Privacy by Design & Default

- Sicherheits- und Datenschutzanforderungen sind integraler Bestandteil des Software Development Lifecycle (Secure SDLC).
- Datenminimierung als Grundprinzip; restriktive Voreinstellungen in der Anwendung.
- Datenschutzfolgenabschätzungen (DSFA) nach Art. 35 DSGVO werden bei neuen Verarbeitungstätigkeiten mit hohem Risiko durchgeführt.

5.5 Penetration Testing und Vulnerability Management

- Jährliche externe Penetrationstests durch ein spezialisiertes externes Unternehmen.
- Sanitisierte Auszüge der Testberichte werden auf Anfrage zur Verfügung gestellt.
- Formaler Vulnerability-Management-Prozess mit CVSS-basierter Priorisierung.
- Automatisierte wöchentliche Patch-Updates und Einsatz von Tools zur automatischen Überwachung von Drittabhängigkeiten.
- Sicherheitsrelevante Schwachstelleninformationen werden Auftraggebern auf Anfrage bereitgestellt.

5.6 Unterstützung bei Betroffenenrechten, Löschung und Rückgabe

- Während der Vertragslaufzeit: Löschungsregime für Tickets durch Auftraggeber (Nutzer-Admin) konfigurierbar.
- Nach Vertragsende: Swat.io löscht oder retourniert die Auftragsdaten nach Wahl des Auftraggebers (Art. 28 Abs. 3 lit. g DSGVO). Standardmäßig erfolgt eine gesicherte Aufbewahrung von bis zu 4 Monaten zur etwaigen Reaktivierung des Kundenkontos; auf Wunsch wird sofort gelöscht. Nach Ablauf der Frist werden die Daten endgültig gelöscht, sofern keine gesetzlichen Aufbewahrungspflichten entgegenstehen.
- Datenexport vor Vertragsende auf Anfrage in einem gängigen, maschinenlesbaren Format.
- Swat.io unterstützt den Auftraggeber bei der Wahrnehmung der Rechte der betroffenen Personen gemäß Art. 12–23 DSGVO. Anfragen sind an privacy@swat.io zu richten. Die Beantwortung erfolgt im Rahmen der gesetzlichen Frist von einem Monat (Art. 12 Abs. 3 DSGVO).
- Auskunft (Art. 15) und Berichtigung (Art. 16): Daten können durch den Auftraggeber direkt im Tool eingesehen und korrigiert werden.
- Einschränkung der Verarbeitung (Art. 18) und Widerspruch (Art. 21): Operative Umsetzung durch den Auftraggeber; Swat.io stellt die technischen Mittel bereit und unterstützt auf Anfrage.

5.7 Mitwirkungspflichten gegenüber dem Verantwortlichen (Art. 28 Abs. 3 lit. f DSGVO)

Swat.io unterstützt den Auftraggeber bei der Erfüllung seiner Pflichten aus Art. 32–36 DSGVO:

- Mitwirkung bei Datenschutz-Folgenabschätzungen (Art. 35): Bereitstellung der erforderlichen Informationen zu Verarbeitungstätigkeiten, Sub-Auftragsverarbeitern, Sicherheitsmaßnahmen und Datenflüssen.
- Mitwirkung bei vorheriger Konsultation der Aufsichtsbehörde (Art. 36).
- Bereitstellung von TOM, Sub-Auftragsverarbeiter-Liste, sanitisierten Penetrationstest-Berichten und Compliance-Zertifikaten auf Anfrage (Art. 32).
- Meldung von Datenschutzverletzungen mit Auswirkungen auf Auftraggeberdaten gemäß Abschnitt 5.3 (Art. 33–34).

Anfragen sind an privacy@swat.io zu richten.

6. Verschlüsselung

Pseudonymisierung und Verschlüsselung personenbezogener Daten (Art. 32 Abs. 1 lit. a DSGVO).

Bereich	Maßnahme
At rest	AES-256 für sämtliche produktiven Datenbanken, Suchindizes, Object Storage und Backups. Endgeräte: Full Disk Encryption durchgesetzt via MDM.
In transit	TLS 1.3 für sämtlichen Web- und API-Verkehr; Mindestversion TLS 1.2.
Schlüsselmanagement	Zentrales Schlüsselmanagement über AWS Key Management Service (KMS). Private Schlüssel ausschließlich bei AWS gespeichert. Kein Klartext-Export.

7. Organisationskontrolle

Organisatorische Maßnahmen zur Absicherung des Personals, der Endgeräte und der internen Prozesse.

7.1 Mitarbeiterauswahl, Verschwiegenheit und Background-Checks

- Sicherheits- und Hintergrundüberprüfung vor Aufnahme der Tätigkeit. Art und Umfang abhängig von Rolle und sicherheitsrelevanter Verantwortung.
- Schriftliche Verpflichtung sämtlicher Mitarbeitender und externer Dienstleister auf das Datengeheimnis (Art. 28 Abs. 3 lit. b DSGVO) sowie auf die Verschwiegenheitspflicht.
- Fortgeltung der Verschwiegenheitspflicht über das Ende des Beschäftigungsverhältnisses hinaus.

7.2 Schulung und Awareness

- Verpflichtende jährliche Schulung aller Mitarbeitenden zu Informationssicherheit und Datenschutz.
- Teilnahme dokumentiert und nachweisbar.
- Onboarding-Schulung für neue Mitarbeitende.

7.3 On- und Offboarding

- Standardisierter Onboarding-Prozess: Vergabe und Dokumentation aller Berechtigungen, Geräteausgabe, Schulung, Verschwiegenheitserklärung.
- Standardisierter Offboarding-Prozess: sofortiger Entzug sämtlicher Berechtigungen, Rückgabe und Wipe der Geräte, Entzug physischer Zutritte.

7.4 Mobile Device Management (MDM)

- Sämtliche von Swat.io ausgegebenen Endgeräte werden zentral via MDM verwaltet.
- Erzwungene Sicherheitsmaßnahmen: aktuelle Betriebssystem-Updates, Full Disk Encryption, Bildschirmsperre, Möglichkeit zur Fernlöschung.
- Geräte werden vor Wiederverwendung oder Aussonderung sicher gelöscht.
- Swat.io arbeitet remote-first. Sämtliche hier genannten Schutzmaßnahmen gelten auch im Home Office bzw. außerhalb der Büroräume.

7.5 Clean-Desk- und Clear-Screen-Policy

- Vertrauliche Unterlagen werden außerhalb der Bürozeiten verschlossen aufbewahrt.
- Bildschirme werden bei Verlassen des Arbeitsplatzes gesperrt.

7.6 Netzwerksicherheit am Standort

- Keine kritischen Server im Bürozugangsnetz.
- Trennung von Produktiv- und Office-Netzwerk.

7.7 Change-Management

- Sämtliche Code-Änderungen erfolgen über ein zentrales Git-Repository mit verpflichtendem Pull-Request-Review und Verknüpfung zum Issue-Tracking.
- Infrastructure-as-Code; Sicherheitsbetrachtungen sind durchgängiger Bestandteil des Entwicklungslebenszyklus.

7.8 Asset-Management und sichere Entsorgung von Datenträgern

- Sämtliche IT-Assets (Endgeräte, Software, Cloud-Services) sind im Rahmen des ISMS inventarisiert und einem benannten Asset-Owner zugeordnet.
- Endgeräte-Inventar wird zentral über das Mobile Device Management geführt.
- Aussonderung von Endgeräten erfolgt nach kryptografischer Löschung sämtlicher Datenträger durch das MDM bzw. das Betriebssystem.
- Das Löschverfahren orientiert sich an anerkannten Standards für sichere Datenlöschung.
- Defekte oder nicht mehr löschbare Datenträger werden physisch zerstört.

8. Drittlandtransfer und ergänzende Maßnahmen

Die Datenverarbeitung findet ausschließlich innerhalb der EU statt. Eine Datenübermittlung in die USA findet ausschließlich im Rahmen des optional zubuchbaren Postmark-/Active-Campaign-Dienstes statt (Funktionen „Ticket per E-Mail weiterleiten“ und „E-Mail-Kanäle“). Diese Funktion kann auf Wunsch jederzeit deaktiviert werden.

8.1 Rechtsgrundlagen

- Angemessenheitsbeschluss EU-US Data Privacy Framework (Juli 2023).
- Standardvertragsklauseln (SCCs) gemäß Durchführungsbeschluss (EU) 2021/914.

9. KI-Funktionen und EU AI Act

- KI-Funktionen sind optional und müssen vom Administrator des Auftraggebers explizit auf Organisationsebene aktiviert werden.
- Eingesetzte Modelle: Modelle von OpenAI und/oder Anthropic (Claude über AWS Bedrock); jeweils in EU-Regionen gehostet.
- Auftraggeberdaten werden weder zum Training noch zum Fine-Tuning von KI-Modellen verwendet.
- Nach derzeitigem Stand der Bewertung erfüllen die KI-Funktionen die Voraussetzungen für Hochrisiko-KI-Systeme nicht.
- Interne und Drittpartei-Risikobewertungen für KI-Funktionen werden regelmäßig durchgeführt; Die KI-Ergebnisse werden regelmäßig auf Verzerrungen (Bias) hin überprüft.
- Technische Schutzmaßnahmen gegen Prompt Injection und Data Poisoning auf Infrastrukturebene.

Review und Freigabe

Erstellt durch	Patrick Diem (ISO), Judit Palotai (DPO)
Freigabedatum	01.Juli 2026
Version	1.0
Nächste Überprüfung	spätestens 12 Monate nach Freigabe oder bei wesentlichen Änderungen