Technische und organisatorische Maßnahmen (TOMs)

Version 1.4 · Stand: 18. Mai 2026

(gemäß Art. 32 DSGVO)

Dieser Anhang konkretisiert die technischen und organisatorischen Maßnahmen („TOMs“), welche die Stratify Marketing S.L.U., Pl. d’ Espanya 11, 1º, 07002 Palma, Spanien (nachfolgend “Anbieter”) als Auftragsverarbeiter zum Schutz personenbezogener Daten umsetzt.

Die Maßnahmen orientieren sich am Stand der Technik, an Art, Umfang, Umständen und Zweck der Verarbeitung sowie an der Eintrittswahrscheinlichkeit und Schwere möglicher Risiken.

---

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

1.1 Zutrittskontrolle

- Betrieb der Infrastruktur in gesicherten Rechenzentren von Amazon Web Services (AWS), Region eu-central-1, Frankfurt am Main
- AWS ist zertifiziert nach ISO/IEC 27001, SOC 2 Type II, BSI C5 (Bundesamt für Sicherheit in der Informationstechnik) und ISO/IEC 27017/27018
- Physischer Zutritt zu Rechenzentren nur für autorisiertes Personal des Infrastrukturbetreibers gemäß dessen Sicherheitskonzept

---

1.2 Zugangskontrolle

- Benutzerkonten mit individuellen Zugangsdaten
- Rollen- und Berechtigungskonzepte
- Passwort- und Authentifizierungsmechanismen
- Schutz vor unbefugtem Zugriff auf Benutzerkonten

- Rollenbasierte Zugriffskontrolle (RBAC) mit strikter Durchsetzung auf Datenbankebene (Row Level Security)
- Mehrstufige Authentifizierung (MFA) verfügbar
- Kurzlebige Zugangstokens (1 Stunde Gültigkeit) mit automatischer Erneuerung
- Session-Timeout bei Inaktivität

1.3 Zugriffskontrolle

- Trennung von System- und Nutzerrechten

- Anwendung des Prinzips der minimalen Rechtevergabe (Least Privilege / Need-to-know)

- Zugriff auf personenbezogene Daten ausschließlich durch befugte Personen mit dokumentiertem Bedarf

- Protokollierung sicherheitsrelevanter Zugriffe (Login, Datenexport, administrative Aktionen)

- Regelmäßige Überprüfung und Entzug nicht mehr benötigter Zugriffsrechte

- Sensible Konfigurationswerte (insb. API-Schlüssel, Service-Credentials, Datenbankzugänge) werden ausschließlich in den verschlüsselten Secret-Stores der eingesetzten Plattformbetreiber (Vercel Environment Variables, Supabase Function Secrets) verwaltet, die at-rest verschlüsselt und auf das Need-to-know-Prinzip beschränkt sind. Im Quellcode oder in versionierten Konfigurationsdateien werden keine Geheimnisse hinterlegt. Kundenspezifische Zugangsdaten für angebundene Drittsysteme (z. B. Integrations-Credentials für ERP-/Sensor-Anbindungen) werden zusätzlich in einem applikationsseitigen, symmetrisch verschlüsselten Vault gespeichert und nur zur Laufzeit für den jeweiligen Aufruf entschlüsselt.

---

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

2.1 Weitergabekontrolle

- Verschlüsselung der Datenübertragung (z. B. TLS)

- Absicherung externer Schnittstellen

- Schutz vor unbefugter Datenübermittlung
- Content Security Policy (CSP) zur Verhinderung von Cross-Site-Scripting und unbefugtem Laden externer Ressourcen
- HMAC-basierter Replay-Schutz für sicherheitskritische API-Endpunkte
- Rate-Limiting auf öffentlich zugänglichen Endpunkten zur Abwehr von Brute-Force- und Denial-of-Service-Angriffen

---

2.2 Eingabekontrolle

- Technische Protokollierung von Änderungen an Daten (z. B. Zeitstempel, Nutzerkennung)
- Nachvollziehbarkeit sicherheitsrelevanter Ereignisse

---

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

3.1 Verfügbarkeitskontrolle

- Einsatz redundanter Cloud-Infrastruktur (AWS eu-central-1, Multi-Availability-Zone)
- Automatisierte tägliche Datenbankbackups mit einer Aufbewahrungsdauer von mindestens 7 Tagen (Supabase/PostgreSQL)
- Point-in-Time Recovery (PITR) für Datenbankdaten
- Angestrebte Recovery Time Objective (RTO): < 24 Stunden
- Angestrebte Recovery Point Objective (RPO): < 24 Stunden

3.2 Belastbarkeit

- Nutzung skalierbarer Cloud-Dienste
- Monitoring von Systemzuständen
- Maßnahmen zur Stabilisierung bei erhöhter Last

---

4. Trennung (Art. 32 Abs. 1 DSGVO)

- Logische Mandantentrennung innerhalb der Software
- Trennung von Kunden- und Nutzerdaten
- Trennung von Produktiv-, Test- und Entwicklungsumgebungen, soweit praktikabel

---

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

- Verschlüsselung aller Datenübertragungen mittels TLS 1.2 (Minimum) und TLS 1.3 (Standard)
- HTTPS mit HSTS (HTTP Strict Transport Security) für alle Client-Server-Kommunikation
- Verschlüsselung gespeicherter personenbezogener Daten at-rest mittels AES-256 auf Infrastrukturebene (AWS/Supabase)
- Verschlüsselung von Datenbankverbindungen (PostgreSQL über TLS)
- Schlüsselverwaltung durch den Infrastrukturbetreiber (AWS KMS)

---

6. Verfahren zur regelmäßigen Überprüfung (Art. 32 Abs. 1 lit. d DSGVO)

- Regelmäßige Überprüfung der Sicherheitsmaßnahmen
- Monitoring sicherheitsrelevanter Ereignisse
- Anpassung der TOMs bei geänderten technischen oder rechtlichen Anforderungen

---

7. Umgang mit Sicherheitsvorfällen

- Sicherheitsmeldungen an den Anbieter: security@gutautomatisiert.ch
- Interne Meldewege
- Unterstützung des Verantwortlichen bei der Erfüllung gesetzlicher Meldepflichten gemäß AVV
- Benachrichtigung des Verantwortlichen bei bekannten Datenschutzverletzungen unverzüglich, spätestens innerhalb von 72 Stunden

---

8. Vertraulichkeitspflichten

- Verpflichtung der mit der Verarbeitung betrauten Personen auf Vertraulichkeit
- Sensibilisierung für Datenschutz und Informationssicherheit

---

9. Keine Erfolgsgarantie

Die beschriebenen technischen und organisatorischen Maßnahmen stellen keine Garantie für die vollständige Vermeidung von Sicherheitsvorfällen dar, sondern dienen der angemessenen Risikominimierung gemäß Art. 32 DSGVO.

---

10. Aktualisierung der TOMs

Der Anbieter ist berechtigt, diese TOMs weiterzuentwickeln oder anzupassen, sofern dadurch das Datenschutzniveau nicht unterschritten wird.
