VAUTRON
RECHENZENTRUM AG

mailrepo.de — Technisch-organisatorische Maßnahmen (TOMs)

April 2026 · Version 1.0

Vautron Rechenzentrum AG

Inhaltsverzeichnis

1 Vorbemerkung

Dieses Dokument beschreibt die technisch-organisatorischen Maßnahmen (TOMs) gemäß Art. 32 DSGVO, die die Vautron Rechenzentrum AG als Auftragsverarbeiter für den Dienst **mailrepo.de** umsetzt. Es dient als Anlage zum Vertrag zur Auftragsverarbeitung (ADV) gemäß Art. 28 DSGVO.

Betreiber:
Vautron Rechenzentrum AG
Obermünsterstraße 9
93047 Regensburg
E-Mail: server@vautron.de

2 Zutrittskontrolle

Maßnahmen zur Verhinderung des unbefugten physischen Zutritts zu Datenverarbeitungsanlagen.

- Das Rechenzentrum der Vautron Rechenzentrum AG ist ISO 27001-zertifiziert und befindet sich ausschließlich an Standorten in Deutschland.
- Zutrittssicherung durch elektronische Zutrittskontrollsysteme mit personenbezogener Protokollierung (Transponder/Chipkarte).
- Besucherregelung mit Anmeldepflicht, Begleitung und Protokollierung.
- Videoüberwachung der Zugangsbereiche rund um die Uhr.
- Alarmgesicherte Sicherheitsbereiche (Serverräume) mit separatem Zutrittssystem.
- Regelmäßige Überprüfung der Zutrittsberechtigungen nach dem Minimalprinzip.

3 Zugangskontrolle

Maßnahmen zur Verhinderung der unbefugten Nutzung von Datenverarbeitungssystemen.

- Anmeldung am mailrepo.de-Kundencenter ausschließlich mit E-Mail-Adresse und Passwort.
- Verpflichtende Zwei-Faktor-Authentifizierung (TOTP oder FIDO2/Passkey) für alle Nutzer — Zugang ohne 2FA ist nicht möglich.
- Brute-Force-Schutz durch Rate-Limiting auf Login-Endpunkte.
- Automatische Sitzungsinvalidierung nach konfigurierbarer Inaktivitätszeit.
- Sitzungsverwaltung mit Möglichkeit, alle aktiven Sitzungen einzeln zu beenden.
- Administrative Systemzugänge (SSH) ausschließlich über schlüsselbasierte Authentifizierung; Passwort-Login deaktiviert.

4 Zugriffskontrolle

Maßnahmen zur Gewährleistung, dass ausschließlich berechtigte Personen auf Daten zugreifen können.

- Strikte Mandantentrennung: Jeder Kunde sieht ausschließlich seine eigenen Daten.
- Ende-zu-Ende-Verschlüsselung aller archivierten E-Mails mit kundenindividuellen Schlüsseln (AES-256-GCM). Im vorgesehenen Sicherheitsmodell hat der Betreiber keinen Zugriff auf Klartextinhalte.
- Schlüsselhierarchie mit Data Encryption Key (DEK) und Key Encryption Key (KEK); der KEK ist durch das Benutzerpasswort geschützt.
- Rollenbasiertes Berechtigungskonzept mit minimalen Privilegien (Principle of Least Privilege).
- Sämtliche Entschlüsselungsvorgänge werden im Audit-Log unveränderlich protokolliert.
- Konfigurierbare Aufbewahrungsfristen mit automatischer kryptografischer Löschung (Crypto-Shredding).

5 Weitergabekontrolle

Maßnahmen zum Schutz personenbezogener Daten bei Transport, Übertragung und Speicherung.

- Alle Netzwerkkommunikation erfolgt ausschließlich über TLS 1.2/1.3 (LMTP-Einlieferung, HTTPS-Zugriff, interne Dienste).
- E-Mails werden unmittelbar bei Eingang verschlüsselt und in verschlüsselter Form auf georedundantem Speicher mit Erasure Coding abgelegt.
- Kein unverschlüsselter Export von Daten. PDF-Downloads und Suchzugriffe erfordern aktive Entschlüsselung durch den authentifizierten Benutzer.
- Jede archivierte E-Mail wird in eine kryptografische Integritätskette (Merkle-Ledger) eingetragen und durch einen qualifizierten Zeitstempel abgesichert.
- Eine Weitergabe personenbezogener Daten an Dritte oder in Drittstaaten findet nicht statt.

6 Eingabekontrolle

Maßnahmen zur nachträglichen Feststellung, ob und von wem Daten verarbeitet wurden.

- Vollständiges Audit-Log über alle sicherheitsrelevanten Aktionen: Login, Entschlüsselung, Löschung, Schlüsseländerungen, Einstellungsänderungen.
- Unveränderliche Protokollierung — Audit-Einträge können weder durch Nutzer noch durch Administratoren gelöscht oder manipuliert werden.
- Jede E-Mail erhält beim Eingang einen kryptografischen Hash (SHA-256), der in der Merkle-Integritätskette verankert wird.
- Qualifizierte RFC 3161-Zeitstempel von einer externen TSA belegen den Archivierungszeitpunkt gerichtsfest.
- Die Manipulationsfreiheit des gesamten Archivs ist jederzeit durch Dritte unabhängig prüfbar (Proof Bundles mit Merkle-Beweis und TSA-Zeitstempel).

7 Verfügbarkeitskontrolle

Maßnahmen zum Schutz personenbezogener Daten gegen zufällige Zerstörung oder Verlust.

- Georedundante Datenspeicherung mit Erasure Coding — Ausfall einzelner Speicherknoten führt nicht zu Datenverlust.
- Regelmäßige automatisierte Integritätsprüfungen der gespeicherten Daten.
- Unterbrechungsfreie Stromversorgung (USV) und Notstromgeneratoren im Rechenzentrum.
- Brandschutzanlage und Klimatisierung der Serverräume.
- Überwachung aller Systemkomponenten rund um die Uhr mit automatischer Alarmierung.

8 Trennungskontrolle

Maßnahmen zur Gewährleistung, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden.

- Logische Mandantentrennung auf Datenbank- und Anwendungsebene: Jeder Mandant besitzt einen eigenen Schlüsselraum.
- Kundenindividuelle Verschlüsselungsschlüssel stellen sicher, dass eine technische Vermischung von Daten verschiedener Mandanten ausgeschlossen ist.
- Getrennte Speicherbereiche pro Mandant.
- Testdaten und Produktivdaten werden in strikt getrennten Umgebungen verarbeitet.

9 Organisatorische Maßnahmen

- Alle Mitarbeiter der Vautron Rechenzentrum AG mit Zugang zu personenbezogenen Daten sind auf das Datengeheimnis verpflichtet.
- Regelmäßige Schulungen und Sensibilisierung der Mitarbeiter zu Datenschutz und Informationssicherheit.
- Dokumentiertes Informationssicherheits-Management-System (ISMS) nach ISO 27001.
- Regelmäßige interne und externe Audits.
- Definierter Prozess zur Meldung von Datenschutzverletzungen gemäß Art. 33/34 DSGVO.
