VAUTRON
RECHENZENTRUM AG

# mailrepo.de — Technical and Organizational Measures (TOMs)

April 2026 · Version 1.0

Vautron Rechenzentrum AG

## Contents



## 1 Preamble

This document describes the technical and organizational measures (TOMs) pursuant to Art. 32 GDPR implemented by Vautron Rechenzentrum AG as data processor for the **mailrepo.de** service. It serves as an annex to the Data Processing Agreement (DPA) pursuant to Art. 28 GDPR.

**Operator:**
Vautron Rechenzentrum AG
Obermünsterstraße 9
93047 Regensburg, Germany
Email: server@vautron.de

## 2 Physical Access Control

*Measures to prevent unauthorized physical access to data processing facilities.*

- The data center operated by Vautron Rechenzentrum AG is ISO 27001-certified and located exclusively in Germany.
- Access secured by electronic access control systems with personalized logging (transponder/chip card).
- Visitor policy requiring registration, escort, and logging.
- 24/7 video surveillance of all entry areas.
- Alarm-secured security zones (server rooms) with separate access control systems.
- Regular review of access authorizations based on the principle of least privilege.

## 3 System Access Control

*Measures to prevent unauthorized use of data processing systems.*

- Login to the mailrepo.de customer portal exclusively via email address and password.
- Mandatory two-factor authentication (TOTP or FIDO2/Passkey) for all users — access without 2FA is not possible.
- Brute-force protection through rate limiting on login endpoints.
- Automatic session invalidation after a configurable inactivity period.
- Session management with the ability to terminate all active sessions individually.
- Administrative system access (SSH) exclusively via key-based authentication; password login disabled.

## 4 Data Access Control

*Measures to ensure that only authorized persons can access data.*

- Strict tenant separation: Each customer can only see their own data.
- End-to-end encryption of all archived emails with customer-specific keys (AES-256-GCM). Under the designed security model, the operator has no access to plaintext content.
- Key hierarchy with Data Encryption Key (DEK) and Key Encryption Key (KEK); the KEK is protected by the user's password.
- Role-based access control with minimal privileges (Principle of Least Privilege).
- All decryption operations are immutably logged in the audit log.
- Configurable retention periods with automatic cryptographic deletion (crypto-shredding).

## 5 Data Transfer Control

*Measures to protect personal data during transport, transmission, and storage.*

- All network communication exclusively via TLS 1.2/1.3 (LMTP delivery, HTTPS access, internal services).
- Emails are encrypted immediately upon receipt and stored in encrypted form on geo-redundant storage with erasure coding.

- No unencrypted data export. PDF downloads and search queries require active decryption by the authenticated user.
- Every archived email is recorded in a cryptographic integrity chain (Merkle ledger) and secured by a qualified timestamp.
- No transfer of personal data to third parties or third countries.

## 6 Input Control

*Measures to retrospectively verify whether and by whom data was processed.*

- Complete audit log of all security-relevant actions: login, decryption, deletion, key changes, settings modifications.
- Immutable logging — audit entries cannot be deleted or manipulated by users or administrators.
- Every email receives a cryptographic hash (SHA-256) upon receipt, which is anchored in the Merkle integrity chain.
- Qualified RFC 3161 timestamps from an external TSA provide legally admissible proof of the archiving time.
- The tamper-proof integrity of the entire archive can be independently verified by third parties at any time (proof bundles with Merkle proof and TSA timestamp).

## 7 Availability Control

*Measures to protect personal data against accidental destruction or loss.*

- Geo-redundant data storage with erasure coding — failure of individual storage nodes does not result in data loss.
- Regular automated integrity checks of stored data.
- Uninterruptible power supply (UPS) and backup generators in the data center.
- Fire protection systems and climate control in server rooms.
- 24/7 monitoring of all system components with automatic alerting.

## 8 Separation Control

*Measures to ensure that data collected for different purposes is processed separately.*

- Logical tenant separation at database and application level: Each tenant has its own key space.
- Customer-specific encryption keys ensure that technical commingling of data from different tenants is excluded.
- Separate storage areas per tenant.
- Test data and production data are processed in strictly separated environments.

## 9 Organizational Measures

- All employees of Vautron Rechenzentrum AG with access to personal data are bound by data secrecy obligations.

- Regular training and awareness programs for employees on data protection and information security.
- Documented Information Security Management System (ISMS) according to ISO 27001.
- Regular internal and external audits.
- Defined process for reporting data breaches pursuant to Art. 33/34 GDPR.

---