VAUTRON
RECHENZENTRUM AG

mailrepo.de — Compliance Documentation Guide

April 2026 · Version 1.0

Vautron Rechenzentrum AG

Contents

1 About This Guide 1

2 GoBD Requirements for Email Archiving 2

3 Template: System Description 2

4 Template: Immutability 2

5 Template: Completeness 3

6 Template: Internal Control System 3

7 Template: Deletion Concept 4

8 Template: Data Backup 4

9 Template: Machine Readability 4

10 Checklist for Your Procedural Documentation 5

11 Contact 5

1 About This Guide

This document helps you create the procedural documentation required under German GoBD regulations (Principles for the Proper Management and Storage of Books, Records and Documents in Electronic Form and for Data Access — BMF letter dated 28.11.2019, BStBl. I p. 1269).

GoBD regulations require you to describe the use of an email archiving system in your procedural

documentation. This guide provides the necessary text templates and technical details about mailrepo.de that you can incorporate into your existing documentation.

Note: This guide does not replace tax or legal advice. Responsibility for complete procedural documentation lies with the taxpayer.

2 GoBD Requirements for Email Archiving

GoBD sets the following requirements for the retention of electronic business correspondence:

Requirement	GoBD Reference	Implementation in mailrepo.de
Immutability	Para. 104–106	Cryptographic audit chain with timestamps (RFC 3161)
Completeness	Para. 36–47	Automatic archiving of all inbound and outbound emails
Timely capture	Para. 48–51	Real-time archiving upon mail delivery
Order	Para. 52–58	UUID-based assignment, complete metadata
Traceability	Para. 59–63	Every action is logged in the Ledger
Retention periods	Para. 119–120	Configurable retention duration (1–100 years)
Machine readability	Para. 124–128	Search functionality on metadata and content
Internal controls	Para. 97–100	Role concept, 2FA, audit log

3 Template: System Description

You can adopt and adapt the following text for your procedural documentation.

System name: mailrepo.de — Email Archiving Service

Provider: Vautron Rechenzentrum AG, Obermünsterstraße 9, 93047 Regensburg, Germany

System type: Cloud-based email archiving service (SaaS), operated in German data centers (ISO/IEC 27001-certified).

Purpose: Automatic archiving of inbound and outbound emails to fulfill retention obligations under HGB §§ 238, 257 and AO § 147.

Functionality: Incoming emails are delivered via the Postfix mail system as blind copies to the archiving system. The system encrypts each email with a customer-specific RSA-4096 key (AES-256-GCM), logs it in a cryptographic audit chain and indexes it for search. Decryption takes place exclusively in the authorized user's browser (zero-knowledge principle).

Retention period: [Please enter: e.g. 10 years / 6 years per § 257 HGB / § 147 AO]

---

4 Template: Immutability

The immutability of archived emails is ensured through the following technical measures:

1. **Encryption on receipt:** Each email is encrypted immediately upon delivery using AES-256-GCM. The encryption key (DEK) is protected with the customer's RSA-4096 public key. Any subsequent modification of the content would invalidate the authenticated encryption tag.
2. **Cryptographic audit chain (Ledger):** Each archived email is entered into a hash chain. The chain is append-only — existing entries cannot be modified or deleted without breaking the chain.
3. **Qualified timestamps:** Commits in the audit chain are signed with RFC 3161 timestamps from independent timestamping authorities. These prove the time of archiving to third parties.
4. **Merkle tree integrity:** The hash chain uses a Merkle tree (RFC 6962) with domain separation. For each email, an integrity proof (proof bundle) can be exported and verified offline.
5. **Signed commits:** Commits are signed with cryptographic signatures (Ed25519, ECDSA or ML-DSA-65). Signature keys are rotated regularly.

---

5 Template: Completeness

The completeness of archiving is ensured through the following measures:

1. **Automatic delivery:** The customer's mail server forwards all inbound and outbound emails via BCC/journal to a tenant-specific archive address (format: `archive-<tenant>-<cno>@mailrepo.de`). Archiving requires no manual intervention.
2. **Transaction safety:** Emails are only acknowledged as delivered (LMTP acknowledge) after they have been fully written to disk and persisted via `fsync`.
3. **Monitoring:** Archiving status is monitored via the dashboard and optionally via real-time monitoring (mailtop). Processing errors are logged and require reprocessing.
4. **Quarantine:** Emails that cannot be processed are moved to quarantine and flagged for manual review. No emails are lost.

---

6 Template: Internal Control System

The internal control system for email archiving comprises:

1. **Access control:**
   - Login with password (min. 14 characters) and two-factor authentication (TOTP or FIDO2/WebAuthn)
   - Session management with IP and user-agent binding, automatic expiry after 30 minutes of inactivity
   - Account lockout after 5 failed attempts
2. **Role concept:**
   - Tenant administrator: management of users and settings
   - User: search and view archived emails

- The operator (Vautron) has no access to email plaintext (zero-knowledge)

3. **Logging:**
   - All actions (archiving, search, deletion, configuration changes) are logged in the audit log
   - The audit chain (Ledger) is cryptographically secured and tamper-proof
4. **Retention periods:**
   - Configurable retention duration (1–100 years)
   - Changes to retention periods require password + two-factor authentication + explicit confirmation (triple-factor)
   - Automatic deletion after expiry
5. **Responsibilities:**
   - [Name]: Administration and monitoring of archiving
   - [Name]: Completeness review (monthly/quarterly)

---

7 Template: Deletion Concept

Scheduled deletion after expiry: After the configured retention period expires, emails are automatically deleted. Deletion covers the encrypted blob, encryption keys, search vectors and queue entries.

Early deletion: Upon customer request (e.g. data subject rights under Art. 17 GDPR). Deletion is logged in the audit log (timestamp, user, reason). A reset record is entered in the Ledger as a cryptographic proof of deletion.

Auditability: The audit chain documents every deletion. The hash chain remains intact and verifiable from the reset point onwards.

---

8 Template: Data Backup

Data backup is managed by the operator (Vautron Rechenzentrum AG):

- **Storage:** CEPH/RADOS cluster with 3× replication across independent nodes, self-healing on node failure, block-level checksums
- **Database:** Daily backups with point-in-time recovery (PostgreSQL)
- **Audit chain:** Append-only journals with CRC32 checksums, snapshots and JSON export
- **Location:** Exclusively German data centers, no third-country transfers

---

9 Template: Machine Readability

Archived emails can be evaluated via the following channels:

1. **Web portal:** Full-text search across subject, sender, recipient, date and content. Results can be viewed individually or as collections.
2. **Semantic search:** Search uses AI-based vectors for content similarity matching. The search index contains no plaintext — personal data is automatically removed before indexing.
3. **Audit chain:** Every entry in the Ledger can be retrieved via the user interface or API. Proof bundles enable offline verification of individual entries.
4. **Data export:** Archived emails can be exported in their original format (RFC 5322).

---

10 Checklist for Your Procedural Documentation

Item	Done?
System description with provider, purpose and functionality	☐
Retention period documented (6 or 10 years)	☐
Description of immutability measures	☐
Archive address and BCC configuration on mail server documented	☐
Responsibilities for monitoring and review named	☐
Internal control system described	☐
Deletion concept documented	☐
Data backup concept documented	☐
Data processing agreement (DPA) with Vautron concluded	☐
Procedural documentation reviewed by tax advisor/auditor	☐

11 Contact

Vautron Rechenzentrum AG
Obermünsterstraße 9
93047 Regensburg
Germany

Data Protection Officer: datenschutz@vautron.de
Technical Support: server@vautron.de