VAUTRON
RECHENZENTRUM AG

mailrepo.de — Leitfaden zur Verfahrensdokumentation

April 2026 · Version 1.0

Vautron Rechenzentrum AG

Inhaltsverzeichnis

1 Über diesen Leitfaden 1

2 Anforderungen der GoBD an die E-Mail-Archivierung 2

3 Textbaustein: Systembeschreibung 2

4 Textbaustein: Unveränderbarkeit 3

5 Textbaustein: Vollständigkeit 3

6 Textbaustein: Internes Kontrollsystem 3

7 Textbaustein: Löschkonzept 4

8 Textbaustein: Datensicherung 4

9 Textbaustein: Maschinelle Auswertbarkeit 5

10 Checkliste für Ihre Verfahrensdokumentation 5

11 Kontakt 5

1 Über diesen Leitfaden

Dieses Dokument unterstützt Sie bei der Erstellung Ihrer Verfahrensdokumentation gemäß GoBD (Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugang — BMF-Schreiben vom 28.11.2019, BStBl. I S. 1269).

Die GoBD verlangen, dass Sie den Einsatz eines E-Mail-Archivierungssystems in Ihrer Verfahrensdokumentation beschreiben. Dieser Leitfaden liefert Ihnen die notwendigen Textbausteine und technischen Angaben zu mailrepo.de, die Sie in Ihre bestehende Dokumentation übernehmen können.

Hinweis: Dieser Leitfaden ersetzt keine steuerliche oder rechtliche Beratung. Die Verantwortung für die vollständige Verfahrensdokumentation liegt beim Steuerpflichtigen.

2 Anforderungen der GoBD an die E-Mail-Archivierung

Die GoBD stellen folgende Anforderungen an die Aufbewahrung elektronischer Geschäftspost:

Anforderung	GoBD-Referenz	Umsetzung in mailrepo.de
Unveränderbarkeit	Rz. 104–106	Kryptographische Audit-Kette mit Zeitstempeln (RFC 3161)
Vollständigkeit	Rz. 36–47	Automatische Archivierung aller ein- und ausgehenden E-Mails
Zeitgerechte Erfassung	Rz. 48–51	Archivierung erfolgt in Echtzeit bei Mailzustellung
Ordnung	Rz. 52–58	UUID-basierte Zuordnung, vollständige Metadaten
Nachvollziehbarkeit	Rz. 59–63	Jede Aktion wird im Ledger protokolliert
Aufbewahrungsfristen	Rz. 119–120	Konfigurierbare Aufbewahrungsdauer (1–100 Jahre)
Maschinelle Auswertbarkeit	Rz. 124–128	Suchfunktion auf Metadaten und Inhalt
Internes Kontrollsystem	Rz. 97–100	Rollenkonzept, 2FA, Audit-Log

3 Textbaustein: Systembeschreibung

Den folgenden Text können Sie in Ihre Verfahrensdokumentation übernehmen und anpassen.

Bezeichnung des Systems: mailrepo.de — E-Mail-Archivierungsdienst

Anbieter: Vautron Rechenzentrum AG, Obermünsterstraße 9, 93047 Regensburg

Art des Systems: Cloud-basierter E-Mail-Archivierungsdienst (SaaS), betrieben in deutschen Rechenzentren (ISO/IEC 27001-zertifiziert).

Einsatzzweck: Automatische Archivierung ein- und ausgehender E-Mails zur Erfüllung der Aufbewahrungspflichten nach HGB §§ 238, 257 und AO § 147.

Funktionsweise: Eingehende E-Mails werden über das Postfix-Mailsystem per Blind Copy an das Archivierungssystem zugestellt. Das System verschlüsselt jede E-Mail mit einem kundenindividuellen RSA-4096-Schlüssel (AES-256-GCM), protokolliert sie in einer kryptographischen Audit-Kette und indexiert sie für die Suche. Die Entschlüsselung erfolgt ausschließlich im Browser des berechtigten Nutzers (Zero-Knowledge-Prinzip).

Aufbewahrungsdauer: [Bitte eintragen: z. B. 10 Jahre / 6 Jahre gemäß § 257 HGB / § 147 AO]

---

4 Textbaustein: Unveränderbarkeit

Übernehmen oder anpassen:

Die Unveränderbarkeit der archivierten E-Mails wird durch folgende technische Maßnahmen sichergestellt:

1. **Verschlüsselung bei Eingang:** Jede E-Mail wird unmittelbar bei Zustellung mit AES-256-GCM verschlüsselt. Der Verschlüsselungsschlüssel (DEK) wird mit dem öffentlichen RSA-4096-Schlüssel des Kunden geschützt. Eine nachträgliche Veränderung des Inhalts würde den Authenticated Encryption Tag invalidieren.
2. **Kryptographische Audit-Kette (Ledger):** Jede archivierte E-Mail wird in eine Hash-Kette eingetragen. Die Kette ist append-only — bestehende Einträge können nicht verändert oder gelöscht werden, ohne die Kette zu brechen.
3. **Qualifizierte Zeitstempel:** Commits in der Audit-Kette werden mit RFC-3161-Zeitstempeln unabhängiger Zeitstempeldienste versehen. Diese belegen den Zeitpunkt der Archivierung gegenüber Dritten.
4. **Merkle-Baum-Integrität:** Die Hash-Kette nutzt einen Merkle-Baum (RFC 6962) mit Domain Separation. Für jede E-Mail kann ein Integritätsnachweis (Proof Bundle) exportiert und offline verifiziert werden.
5. **Signierte Commits:** Commits werden mit kryptographischen Signaturen versehen (Ed25519, ECDSA oder ML-DSA-65). Die Signaturschlüssel werden regelmäßig rotiert.

---

5 Textbaustein: Vollständigkeit

Die Vollständigkeit der Archivierung wird durch folgende Maßnahmen gewährleistet:

1. **Automatische Zustellung:** Der Mailserver des Kunden leitet alle ein- und ausgehenden E-Mails per BCC/Journal an eine mandantenspezifische Archivadresse weiter (Format: `archive-<tenant>-<cno>@mailrepo.de`). Die Archivierung erfolgt ohne manuellen Eingriff.
2. **Transaktionssicherheit:** E-Mails werden erst als zugestellt bestätigt (LMTP-Acknowledge), nachdem sie vollständig auf die Festplatte geschrieben und per `fsync` persistiert wurden.
3. **Monitoring:** Der Archiverungsstatus wird über das Dashboard und optional über Echtzeit-Monitoring (mailtop) überwacht. Verarbeitungsfehler werden protokolliert und erfordern eine Nachverarbeitung.
4. **Quarantäne:** Nicht verarbeitbare E-Mails werden in eine Quarantäne verschoben und zur manuellen Prüfung vorgemerkt. Es gehen keine E-Mails verloren.

---

6 Textbaustein: Internes Kontrollsystem

Das interne Kontrollsystem für die E-Mail-Archivierung umfasst:

1. **Zugriffskontrolle:**
   - Anmeldung mit Passwort (mind. 14 Zeichen) und Zwei-Faktor-Authentifizierung (TOTP oder FIDO2/WebAuthn)
   - Sitzungsverwaltung mit IP- und User-Agent-Binding, automatischer Ablauf nach 30 Minuten Inaktivität
   - Kontosperre nach 5 Fehlversuchen
2. **Rollenkonzept:**
   - Mandanten-Administrator: Verwaltung von Benutzern und Einstellungen
   - Benutzer: Suche und Einsicht archivierter E-Mails
   - Der Betreiber (Vautron) hat keinen Zugriff auf E-Mail-Klartext (Zero-Knowledge)
3. **Protokollierung:**
   - Alle Aktionen (Archivierung, Suche, Löschung, Konfigurationsänderungen) werden im Audit-Log protokolliert
   - Die Audit-Kette (Ledger) ist kryptographisch gesichert und nicht manipulierbar
4. **Aufbewahrungsfristen:**
   - Konfigurierbare Aufbewahrungsdauer (1–100 Jahre)
   - Änderungen der Aufbewahrungsfrist erfordern Passwort + Zwei-Faktor-Authentifizierung + explizite Bestätigung (Triple-Factor)
   - Automatische Löschung nach Fristablauf
5. **Verantwortlichkeiten:**
   - [Name]: Administration und Überwachung der Archivierung
   - [Name]: Prüfung der Vollständigkeit (monatlich/quartalsweise)

---

7 Textbaustein: Löschkonzept

Reguläre Löschung nach Fristablauf: Nach Ablauf der konfigurierten Aufbewahrungsfrist werden E-Mails automatisch gelöscht. Die Löschung umfasst den verschlüsselten Blob, die Verschlüsselungsschlüssel, die Suchvektoren und die Warteschlangeneinträge.

Vorzeitige Löschung: Auf Antrag des Kunden (z. B. bei Betroffenenrechten nach Art. 17 DSGVO). Die Löschung wird im Audit-Log protokolliert (Zeitstempel, Benutzer, Grund). Im Ledger wird ein Reset-Record als kryptographischer Löschnachweis eingetragen.

Nachweisbarkeit: Die Audit-Kette dokumentiert jede Löschung. Die Hash-Kette bleibt ab dem Reset-Punkt intakt und verifizierbar.

---

8 Textbaustein: Datensicherung

Die Datensicherung erfolgt durch den Betreiber (Vautron Rechenzentrum AG):

- **Speicherung:** CEPH/RADOS-Cluster mit 3-facher Replikation auf unabhängigen Knoten, Selbstheilung bei Knotenausfall, Checksummen auf Blockebene
- **Datenbank:** Tägliche Backups mit Point-in-Time-Recovery (PostgreSQL)

- **Audit-Kette:** Append-only Journals mit CRC32-Checksummen, Snapshots und JSON-Export
- **Standort:** Ausschließlich deutsche Rechenzentren, keine Drittland-Übertragung

---

9 Textbaustein: Maschinelle Auswertbarkeit

Archivierte E-Mails sind über folgende Wege auswertbar:

1. **Web-Portal:** Volltextsuche über Betreff, Absender, Empfänger, Datum und Inhalt. Ergebnisse können einzeln oder als Sammlung eingesehen werden.
2. **Semantische Suche:** Die Suche nutzt KI-basierte Vektoren für inhaltliche Ähnlichkeitssuche. Der Suchindex enthält keine Klartexte — personenbezogene Daten werden vor der Indexierung automatisch entfernt.
3. **Audit-Kette:** Jeder Eintrag im Ledger kann über die Benutzeroberfläche oder die API abgerufen werden. Proof Bundles ermöglichen die Offline-Verifikation einzelner Einträge.
4. **Datenexport:** Archivierte E-Mails können im Originalformat (RFC 5322) exportiert werden.

---

10 Checkliste für Ihre Verfahrensdokumentation

Punkt	Erledigt?
Systembeschreibung mit Anbieter, Zweck und Funktionsweise	☐
Aufbewahrungsfrist dokumentiert (6 oder 10 Jahre)	☐
Beschreibung der Maßnahmen zur Unveränderbarkeit	☐
Archivadresse und BCC-Konfiguration am Mailserver dokumentiert	☐
Zuständigkeiten für Überwachung und Prüfung benannt	☐
Internes Kontrollsystem beschrieben	☐
Löschkonzept dokumentiert	☐
Datensicherungskonzept dokumentiert	☐
Auftragsverarbeitungsvertrag (AVV) mit Vautron abgeschlossen	☐
Verfahrensdokumentation vom Steuerberater/WP geprüft	☐

11 Kontakt

Vautron Rechenzentrum AG
Obermünsterstraße 9

93047 Regensburg
Deutschland

Datenschutzbeauftragter: datenschutz@vautron.de
Technischer Support: server@vautron.de