VAUTRON
RECHENZENTRUM AG

mailrepo.de — Customer Handbook

March 2026 · Version 1.0

Vautron Rechenzentrum AG

Contents

1 What is mailrepo.de?

mailrepo.de is an email archiving service for businesses. It supports compliance with legal retention requirements (e.g., GoBD, HGB §§ 238, 257).

After a one-time setup, incoming and outgoing emails are automatically archived, encrypted, tamper-proof logged, and made searchable via intelligent search — without manual intervention.

2 Core Principles

- **End-to-End Encryption:** The server never has access to the plaintext of your emails. Decryption takes place exclusively in your browser.
- **Tamper Protection:** Every archived email receives a cryptographic entry in an audit chain with independent timestamps.
- **Automation:** After initial setup, archiving runs fully automatically.
- **Data Minimisation:** Only data necessary for operation is stored.

3 How Does Archiving Work?

4 Overview

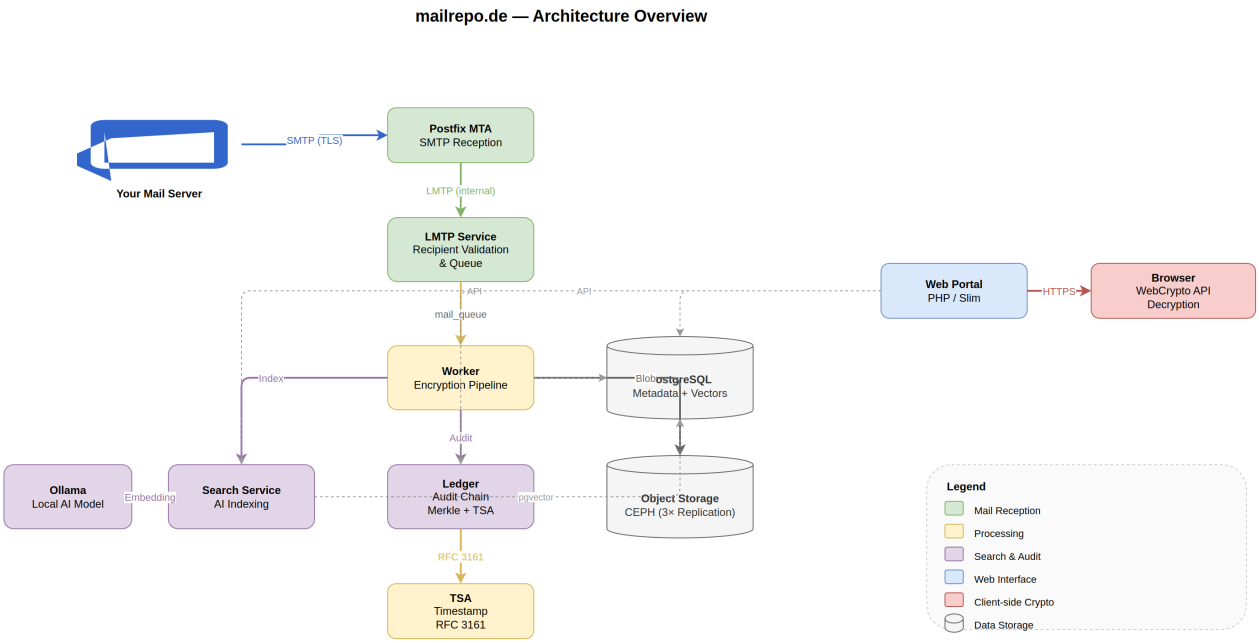


Figure 1: Architecture Overview

You configure your mail server to forward a copy of every incoming and outgoing email via SMTP to mailrepo.de. From that point, everything runs automatically:

1. **Reception:** Your mail server sends the email via SMTP to mailrepo.de.
2. **Compression & Encryption:** The email is first compressed (gzip) to save storage space and then encrypted with a randomly generated key. This key is in turn secured with your personal public key (details in Chapter 3).
3. **Storage:** The encrypted content is stored on a distributed storage system with triple replication.
4. **Logging:** A cryptographic entry in the audit chain proves the time and content of archiving (details in Chapter 5).
5. **Indexing:** The email is prepared for semantic search — without storing the plaintext (details in Chapter 6).

5 Mail Delivery Flow

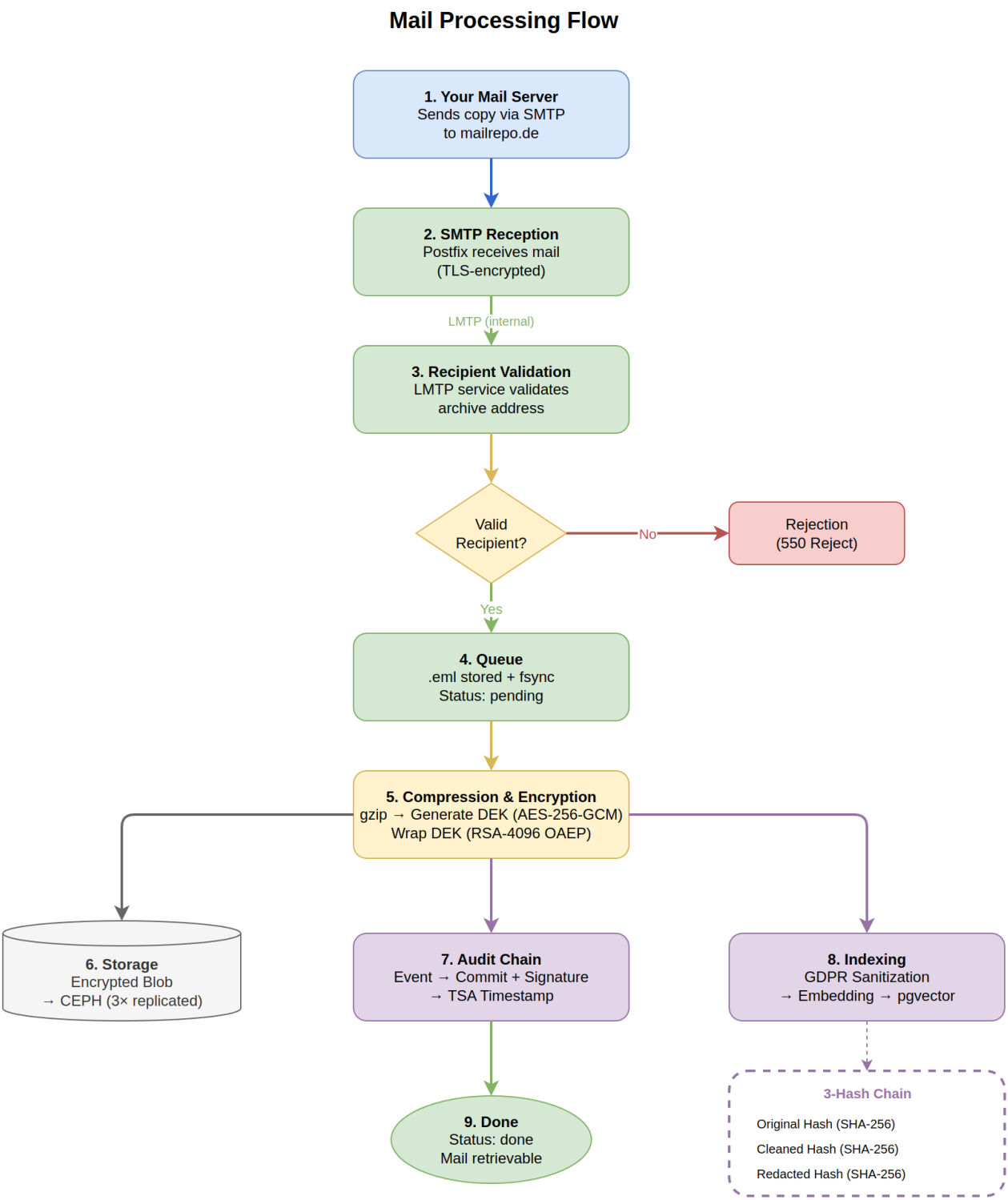
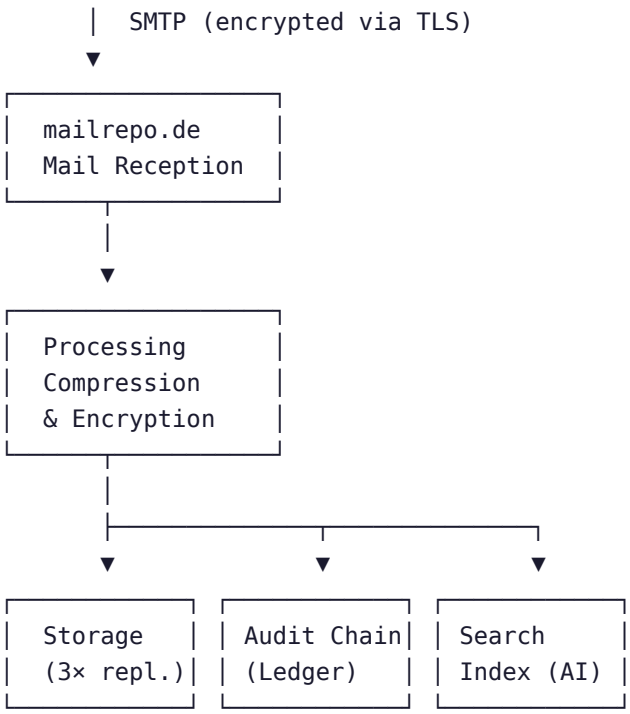


Figure 2: Mail Processing Flow

```
Your Mail Server
      |
```



6 Address Format

Your archiving address follows a fixed scheme:

`archive-vautron-<customernumber>@mailrepo.de`

Optional tags for categorisation (e.g., departments) are appended with +:

`archive-vautron-<customernumber>+accounting@mailrepo.de`

---

7 Security & Encryption

8 Zero-Knowledge Principle

The security model is based on the **zero-knowledge principle:** The server stores and processes only encrypted data. Decryption happens exclusively in your browser. Neither the operator nor any administrator can read your emails.

9 Key Hierarchy

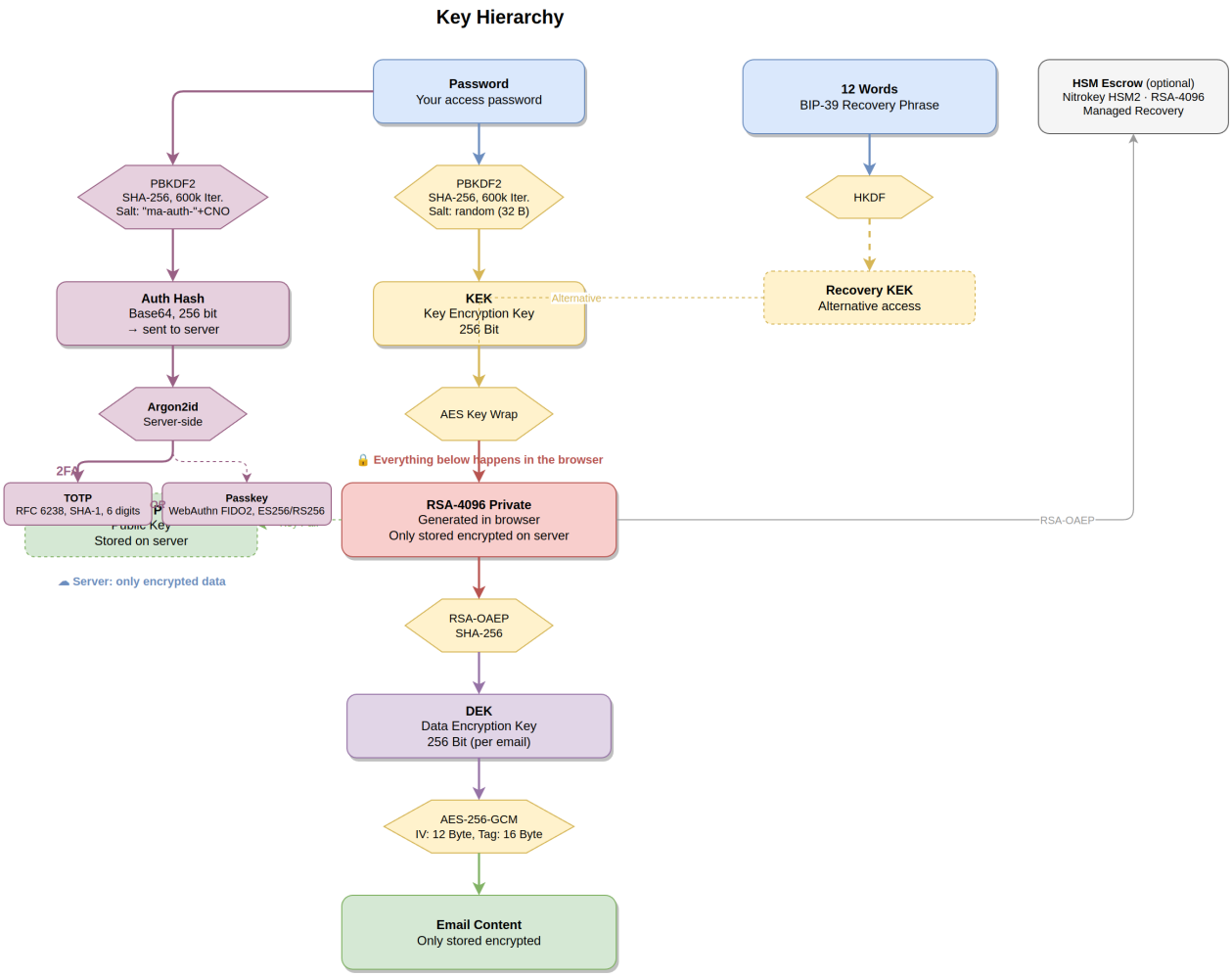
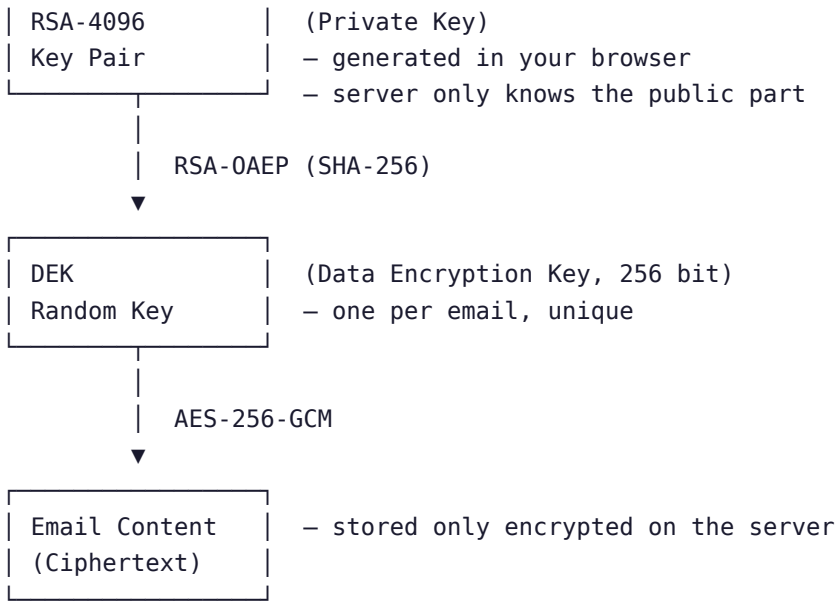


Figure 3: Key Hierarchy

Your emails are protected through a multi-level key hierarchy:

```
Your Password
    │
    ├── PBKDF2 ("ma-auth-"+CNO, 600,000 iter.)
    │   ▼
    │   Auth Hash ──────────────► Server (secure verification)
    │
    │   PBKDF2 (random salt, 600,000 iterations)
    ▼
┌─────────────────┐
│ KEK             │  (Key Encryption Key, 256 bit)
│ AES Key Wrap    │  – protects your private key
└─────────────────┘  – stays in browser, NEVER transmitted
        │
        ▼
┌─────────────────
```



10 Encryption Algorithms in Detail

Level	Algorithm	Parameters	Purpose
Email content	AES-256-GCM	256-bit key, 12-byte IV, 16-byte tag	Email encryption
DEK wrapping	RSA-OAEP	4096-bit RSA, SHA-256	Email key encryption
Private key	AES Key Wrap	256-bit KEK	Private key protection
KEK derivation	PBKDF2	SHA-256, 600,000 iterations, 16-byte salt	Password → key
Recovery KEK	HKDF	BIP-39 entropy → key	Alternative key derivation
Ledger signature	Ed25519 / ECDSA P-256 / ML-DSA-65	Variable	Audit chain signing
Timestamps	RFC 3161 TSA	External	Independent time proof

11 Decryption Process

When you open an email in the web portal, the following happens — entirely in your browser:

1. The encrypted email content is loaded from the server.
2. The encrypted key (DEK) is loaded from the server.
3. Your password is derived to the KEK via PBKDF2.
4. The KEK unwraps your private RSA key.
5. The private RSA key unwraps the DEK.
6. The DEK decrypts the email via AES-256-GCM.
7. If compressed, the email is automatically decompressed (gzip).
8. The decrypted email is displayed in the browser — it never leaves your machine.

All of these steps are performed by the **WebCrypto API** — a standardised cryptography interface built into your browser.

12 Recovery Phrase (12 Words)

During initial setup, you receive a **12-word recovery phrase** (following the BIP-39 standard). This phrase serves as an alternative backup of your private key.

Important: The recovery phrase is the only way to restore access to your emails if you forget your password. The operator has no access to your private key and cannot perform decryption on your behalf.

> **Optional: HSM Escrow**
> On request, your private key can additionally be encrypted and deposited on a certified hardware security module (HSM, Nitrokey HSM2). This enables assisted recovery in an emergency — even if you have lost both your password and your recovery phrase. The operator can only decrypt your key with physical access to the HSM and the HSM PIN. Activation is available during initial setup or later in your account settings.

13 Authentication

Measure	Details
Password	Your password never leaves your browser — it is locally converted into an auth hash and only this hash is sent to the server, where it is additionally hashed with Argon2id.
TOTP (2FA)	Time-based one-time password, 30-second interval
Passkeys	Phishing-resistant alternative to TOTP codes. Uses your device's fingerprint sensor, Face ID, or a USB security key (FIDO2/WebAuthn).
Backup codes	One-time emergency codes in case of TOTP device loss
Account lockout	Locked for 15 minutes after 5 failed attempts
Session protection	Sessions bound to IP and browser fingerprint

---

14 Web Portal — Your Archive Access

15 Dashboard

After logging in, you see at a glance:

- Total number of archived emails and today's arrivals
- Storage usage and quota
- Email volume over the last 30 days as a chart

- Distribution by status and top recipients

16 Email Search

- **Semantic search:** AI-based similarity search understands synonyms and related terms — you find what you mean, not just what you type.
- **Chronological search:** Sort by date, filter by period, status, tag, recipient, and size.
- **Email detail view:** Decryption and display directly in the browser.

17 Audit Chain (Ledger)

- View cryptographic entries for your archived emails
- Verify integrity of individual emails
- Display independent timestamp authority certificates

18 Deletion Log

- Overview of all deleted emails
- Timestamp, user, and deletion reason for each deletion

19 Settings

- **TOTP management:** Set up and manage your two-factor authentication. You can register multiple authenticator devices or reset your TOTP secret.
- **Passkeys:** Add, rename or remove passkeys as a phishing-resistant alternative to TOTP codes (FIDO2/WebAuthn)
- **Backup codes:** Generate one-time emergency codes for when your authenticator device is unavailable
- **Recovery phrase:** Display your 12-word phrase or regenerate a new one (the previous phrase becomes invalid)
- **Key export:** Export your encrypted private key
- **Session management:** View active sessions and remote logout
- **GDPR data export:** Download all data stored about you as a ZIP file
- **Password change:** Automatic re-wrapping of your key

20 Help & FAQ

The help section includes:

- Introduction and getting started
- Security model explained
- Decryption process step by step
- FAQ with the most common questions
- Glossary of technical terms

---

21 Tamper Protection — The Audit Chain

22 What Does the Audit Chain Prove?

Every archived email receives a tamper-proof entry in a cryptographic audit chain (ledger). This entry proves:

- **When** the email was archived — with an independent timestamp (RFC 3161 TSA)
- **What** was archived — via the cryptographic hash of the content (SHA-256)
- **That** the order has not been altered — via a chained hash chain

23 Four-Level Hierarchy

The audit chain organises its entries in four levels:

24 Level 1 — Events (per email)

Each email generates an entry with the content hash, file size, and timestamp. Each entry references the previous one, forming an immutable chain.

25 Level 2 — Commits (batch summary)

Multiple events are periodically combined into a commit: - A **Merkle tree** (RFC 6962) combines all events into a single hash. - The commit is **digitally signed** (Ed25519, ECDSA P-256, or ML-DSA-65). - An **RFC 3161 timestamp** from an independent timestamp authority is attached.

26 Level 3 — Tenant Heads (per tenant)

Commits are aggregated per tenant into a summary.

27 Level 4 — Root Heads (global)

All tenant summaries are combined into a global integrity anchor.

28 Merkle Proof (Individual Verification)

For any individual email, a **Merkle proof** can be generated. This proves that a specific email is part of a signed and timestamped commit — without revealing the contents of other emails.

A Merkle proof contains: - The hash of the email in question - The sibling hashes in the Merkle tree - The digital signature of the commit - The TSA timestamp

This proof is **offline verifiable** — it requires no access to the archive system.

29 Post-Quantum Security

The ledger already supports **ML-DSA-65** (formerly CRYSTALS-Dilithium), a post-quantum-secure signature algorithm. This protects the integrity of the audit chain even against future quantum computers.

30 Cryptographic Algorithms

Purpose	Algorithm	Key Length
Hashing	SHA-256	256 bit
Signature	Ed25519 / ECDSA P-256 / ML-DSA-65	256 / 256 / PQC
Timestamps	RFC 3161 TSA	external

---

31 Searching the Archive

32 Semantic Search

The search in mailrepo.de does not work like a classic full-text search. Instead, it uses **AI-based similarity search:**

- You find emails even if you don't know the exact words used in the email.
- Synonyms and related terms are recognised.
- The search "understands" the meaning of your query.

33 How Does It Work Without Plaintext?

Emails are not stored as text in the search index. Instead:

1. Upon receipt, the email is converted into **numerical vectors** (number values) that represent its meaning.
2. Only these vectors are stored — reconstruction of the original text is not possible according to the current state of the art.
3. When you search, your search text is also converted into a vector and compared with all stored vectors.

34 Privacy During Indexing

Before vector generation, seven categories of personal data are automatically detected and removed:

1. Passwords and credentials
2. API keys and tokens
3. IBANs and bank details
4. Phone numbers
5. Postal addresses
6. Email addresses
7. Customer numbers

AI processing takes place entirely locally — no email content leaves the data centre.

35 Three-Hash Traceability

For each email, three cryptographic hashes are calculated to ensure data minimisation is traceable:

Hash	Timing	Purpose
Original hash	After receipt	Verification of source data
Cleaned hash	After normalisation	Traceability of sanitisation
Redacted hash	After privacy sanitisation	Proof of data minimisation

---

36 Retention & Deletion

37 Automatic Retention

Archived emails are stored according to configured retention periods. After expiry, deletion occurs automatically in two stages:

1. **Soft delete:** The email is marked as deleted.
2. **Final purge:** After a grace period, the encrypted content, keys, search vectors, and metadata are irrevocably removed.

38 Changing the Retention Period (Professional Plan)

On the Professional plan, you can adjust the retention period under **Settings → Retention** (365–36,500 days). Before the change, you will be shown how many mails would be affected.

As a security measure, you must confirm with three factors:

1. Your **password**
2. A valid **TOTP code** — or a registered **passkey**
3. Type the consent text verbatim: *“I agree to change the retention period”*

On the Basis plan, retention changes are only available via support.

39 Manual Deletion

Manual deletion is disabled by default and must be individually activated for your account. Once activated, individual emails can be marked for deletion via the detail view in the web portal.

40 Documentation

All deletions are documented in the deletion log with timestamp, user, and reason. The audit chain accounts for deletions via a generation system (see Chapter 5).

---

41 Data Protection & GDPR

42 Data Minimisation

- Only data necessary for operation is stored
- Email content exists only in encrypted form
- The search index contains only numerical vectors, no text
- IP addresses in exports are automatically anonymised
- Sensitive fields are automatically redacted in logs

43 Location

All data is processed and stored in a **German data centre**. No transfer to third countries takes place.

44 Right of Access (Art. 15 GDPR) and Data Portability (Art. 20 GDPR)

Under **Settings → Data Export**, you can download all data stored about you as a ZIP file. The export contains:

- User profile (without password)
- TOTP devices (names only)
- Passkeys (names and creation date only)
- Login history (last 100 entries)
- Active sessions
- Public key
- Complete audit log
- Ledger statistics, current ledger head, and chain verification
- Event detail view: click on a commit to inspect all associated journal events

IP addresses are automatically anonymised in the export.

45 Right to Erasure (Art. 17 GDPR)

- Individual emails can be marked for deletion via the detail view.
- Deleted emails are permanently purged in a two-stage process.
- The audit chain accounts for deletions via a generation system.
- All deletions are documented in the deletion log.

46 Audit Trail

The following actions are logged:

Action	Logged
Login (success/failure)	Timestamp, IP (anonymised), browser ID
Email decryption	Timestamp, email ID
Email deletion	Timestamp, email ID, reason
Settings change	Timestamp, action
Password change	Timestamp

The audit log can be exported as CSV or PDF.

---

47 Getting Started

48 Sign In

Open `https://www.mailrepo.de` and sign in with your credentials.

49 Setup Wizard

On your first sign-in, a three-step wizard guides you through the setup:

1. **Set up TOTP:** Scan the QR code with an authenticator app (e.g., Google Authenticator, Authy) and confirm with a generated code. You can then add a passkey as an alternative to TOTP codes under **Settings → Passkeys**.
2. **Generate encryption keys:** Your browser automatically generates an RSA-4096 key pair. The private key is protected with your password (PBKDF2, 600,000 iterations).
3. **Note your recovery phrase:** 12 BIP-39 words are displayed. **Write them down and store them securely** — they are your last resort backup.

50 Configure Your Mail Server

Configure your mail server to forward a copy of every incoming and outgoing email via SMTP to your archiving address. The connection must be secured with **TLS** (port 25 with STARTTLS or port 587).

51 Your Archiving Address

The base format is:

`archive-vautron-<customernumber>@mailrepo.de`

You can optionally append **tags** for categorization — e.g., to distinguish departments, domains, or locations:

```
archive-vautron-<customernumber>+accounting@mailrepo.de
archive-vautron-<customernumber>+sales@mailrepo.de
archive-vautron-<customernumber>+example-com@mailrepo.de
archive-vautron-<customernumber>+office-berlin@mailrepo.de
```

Which tagging scheme fits best is up to you. In the web portal under **Mail Setup**, you will find a configuration generator that produces the appropriate settings for your mail server.

52 Postfix

To send a BCC copy of **all mails** (incoming and outgoing):

```
# /etc/postfix/main.cf
always_bcc = archive-vautron-100123@mailrepo.de
```

For **outgoing mails only** (by sender):

```
# /etc/postfix/main.cf
sender_bcc_maps = hash:/etc/postfix/sender_bcc
```

```
# /etc/postfix/sender_bcc
@example.com    archive-vautron-100123+outbound@mailrepo.de
```

For **incoming mails only** (by recipient):

```
# /etc/postfix/main.cf
recipient_bcc_maps = hash:/etc/postfix/recipient_bcc
```

```
# /etc/postfix/recipient_bcc
@example.com    archive-vautron-100123+inbound@mailrepo.de
```

For **multiple domains** with separate tags:

```
# /etc/postfix/sender_bcc
@company-a.com  archive-vautron-100123+company-a@mailrepo.de
@company-b.com  archive-vautron-100123+company-b@mailrepo.de
```

After each change: `postmap /etc/postfix/sender_bcc && systemctl reload postfix`

Enforce TLS: To ensure the BCC copy is transmitted encrypted, add to `/etc/postfix/main.cf`:

```
smtp_tls_policy_maps = hash:/etc/postfix/tls_policy
```

```
# /etc/postfix/tls_policy
mailrepo.de    encrypt
```

```
postmap /etc/postfix/tls_policy && systemctl reload postfix
```

53 Microsoft 365 / Exchange Online

1. Open the **Exchange Admin Center** → **Mail flow** → **Rules**.
2. Click **Add a rule** → **Create a new rule**.
3. **Name:** e.g., "Archive to mailrepo.de"
4. **Condition:** *The sender is internal* (for outbound) or *The recipient is internal* (for inbound) — or both.
5. **Action:** *BCC the message to* → `archive-vautron-100123@mailrepo.de`
6. Save and activate.

For separate tags, create two rules — one for inbound, one for outbound.

Enforce TLS: Under **Mail flow → Connectors**, create a partner connector to mailrepo.de with the option *Always use TLS and require a valid certificate*.

54 Google Workspace

1. Open the **Google Admin Console** → **Apps** → **Google Workspace** → **Gmail** → **Routing**.
2. Click **Add another rule**.
3. **Affected messages:** Inbound, Outbound, Internal (as needed).
4. **Add recipient:** `archive-vautron-100123@mailrepo.de`
5. **Delivery option:** *Add BCC recipient*
6. Save.

Enforce TLS: Under **Compliance → TLS compliance**, create a rule for the domain `mailrepo.de` with *Require TLS connection*.

55 Other Mail Servers

Mail Server	Configuration
Exim	Router of type `redirect` with `unseen`
Sendmail	`.mc` configuration with `FEATURE(always_bcc)`
Dovecot + Sieve	`redirect` action in a global Sieve script
Zimbra	Admin Console → Postfix settings → `always_bcc`
MDaemon	Security → Content Filter → BCC rule
Kerio Connect	Delivery rules → Forward copy

Contact support if you need assistance with configuration.

56 Use the Archive

After setup, emails are archived automatically. The dashboard shows the current status. Use the search to find archived emails — decryption occurs on demand directly in your browser.

---

57 Frequently Asked Questions (FAQ)

Can the operator read my emails?
No. Decryption takes place exclusively in your browser. The server stores only encrypted data.

What happens if I forget my password?
You can restore access using your 12-word recovery phrase. Without both the password and the phrase, decryption is impossible — even for the operator. If HSM escrow is enabled, the operator can perform an assisted recovery: your private key is securely decrypted on the HSM, re-wrapped, and you receive a new recovery mnemonic.

How long are my emails retained?
The retention period depends on your contract and legal requirements (e.g., GoBD: up to 10 years).

Can I delete individual emails?
Yes, via the detail view in the web portal. Deletions are logged and recorded in the audit chain.

How do I find a specific email?
The semantic search understands synonyms and related terms. Simply describe what you're looking for — even if you don't know the exact words.

What does the audit chain prove?
The audit chain proves when each email was archived and that the order has not been tampered with. Each entry is confirmed by an independent timestamp authority.

Is the system protected against quantum computers?
The audit chain already supports ML-DSA-65, a post-quantum-secure algorithm. For email encryption (RSA-4096), the zero-knowledge architecture provides additional protection: since the server never sees the plaintext, an attacker would need to directly break your private key.

Where is my data stored?
All data is stored in a German data centre. No transfer abroad takes place. The storage uses triple replication for maximum resilience.

---

58 Glossary

Term	Explanation
AES-256-GCM	Symmetric encryption algorithm with 256-bit key and authenticated encryption.
Argon2id	Password hashing algorithm specifically resistant to brute-force attacks with specialised hardware.
BIP-39	Standard for mnemonic recovery phrases (12 words).
DEK	Data Encryption Key — random key generated per email.
Ed25519	Digital signature scheme based on elliptic curves.

Term	Explanation
GDPR	General Data Protection Regulation of the EU.
GoBD	German regulations for proper management and storage of books, records, and documents in electronic form.
HKDF	HMAC-based Key Derivation Function — deterministically derives keys from a master secret.
HSM	Hardware Security Module — specialised hardware for secure key storage.
KEK	Key Encryption Key — a key that encrypts other keys.
Merkle tree	Binary hash structure that summarises many entries into a single root hash.
ML-DSA-65	Post-quantum-secure signature algorithm (formerly CRYSTALS-Dilithium).
OAEP	Optimal Asymmetric Encryption Padding — padding scheme for RSA encryption.
PBKDF2	Password-Based Key Derivation Function 2 — derives a cryptographic key from a password.
RFC 3161	Standard for trusted timestamp services (TSA).
RSA-4096	Asymmetric encryption scheme with 4096-bit keys.
TOTP	Time-based One-Time Password — time-based one-time password for two-factor authentication.
TSA	Timestamp Authority — independent timestamp service.
WebAuthn / Passkey	Web Authentication standard (W3C/FIDO2) — enables login via fingerprint, Face ID, or USB security key instead of a TOTP code.
WebCrypto API	Browser-native cryptography interface per W3C standard.
Zero-knowledge	Architectural principle where the server has no knowledge of unencrypted data.

This handbook describes the usage and security of the mailrepo.de archiving system from the customer's perspective.