

Technical and Organizational Measures (TOMs)

Security-control description under Article 32 GDPR. Controls marked planned must be completed and evidenced before the related feature launches.

DRAFT FOR REVIEW

1. Data minimization

- Current-message and share surfaces send parsed fields only.
- Raw email, message and image content is processed in memory and is not written to the check history.
- Check history stores verdict, category, signal identifiers, timestamp, content hash, surface and latency.
- Feedback stores a label plus signal identifiers, without message content.

2. Access control

- Passwordless verified-email access for personal accounts; MFA available and required for workspace administrators before background mailbox scanning launches.
- Every workspace request is checked against the signed-in membership and exact verified workspace ID.
- Roles separate owners, administrators, checkers, approvers and operators. Sensitive actions produce append-only audit events.

3. Cryptography

- TLS is required in transit.
- Provider-managed database encryption protects data at rest.
- IBANs in the workspace vendor master are stored as SHA-256 hashes with only the last four characters displayed.
- Secrets and mailbox OAuth tokens must use a managed KMS before Mode B scanning launches.

4. Isolation and logging

- Application queries bind account or workspace ownership before returning private records.
- Logs and analytics exclude request bodies, message text, email addresses and raw URLs.

- Application logs target 14-day retention. Product metrics use bounded categories and identifiers.

5. Availability and recovery

- Stateless web and check workers can be replaced without customer-content recovery.
- Database backups, restore tests, incident ownership and EU secondary-region failover are required before general availability.
- External intelligence failures become unknown evidence and never become an OK result.

6. Secure development

- Automated type, lint, security and behavioral tests run before deployment.
- Deterministic signal changes must pass a labeled evaluation gate before launch.
- Dependency and static security audits are recorded with each release.
- An independent penetration test is required before background mailbox access launches.

7. Retention

Record	Default
Raw content	Not stored; target disposal within 60 seconds.
Extracted dedupe fields	90 days.
Personal check record	12 months.
Workspace check and audit record	Three years by default; configurable target.
Application logs	14 days, content-free.

8. Current implementation boundary

The shared web engine, current-message Outlook package, Gmail Mode A package, mobile web share target and browser extension source exist. EU-only hosting, signed store distribution, mailbox Mode B, managed KMS, external pen test and legal review remain release gates and must not be represented as complete until evidenced.