Data Retention and Protection Policy

Organization: Caliber Technologies Inc. (Calimatic Mail) **Document Version:** 1.0 **Effective Date:** February 14, 2026 **Last Reviewed:** February 14, 2026 **Classification:** Confidential

---

1. Purpose

This policy defines how Calimatic Mail collects, stores, protects, retains, and deletes user data, with specific attention to data processed through third-party integrations such as Zoom and Google.

2. Scope

This policy covers all data processed by the Calimatic Mail platform, including:

- User account information
- Email content and metadata
- Calendar events and meeting data
- OAuth integration data (Zoom, Google)
- Application logs and analytics

3. Data Classification

Classification	Description	Examples
Public	Freely available information	Marketing website content, pricing
Internal	Non-sensitive operational data	System logs, performance metrics
Confidential	User PII and business data	Email addresses, names, calendar events
Restricted	Authentication and security data	OAuth tokens, passwords, API keys

4. Data Collection

4.1 User Account Data

- Email address, name, organization
- Collected at account registration
- Required for service operation

4.2 OAuth Integration Data (Zoom, Google)

- **Collected:** Provider user ID, provider email, display name, profile picture URL
- **Stored:** OAuth access token, refresh token, token expiration, scopes granted
- **Purpose:** Create and manage video meetings on behalf of the user
- **Collection Method:** OAuth 2.0 authorization flow with explicit user consent

4.3 Meeting Data

- Meeting join URL, meeting ID, host URL
- Created when user adds a video meeting to a calendar event
- Stored as part of the calendar event record

5. Data Storage and Protection

5.1 Storage Location

- All data is stored in PostgreSQL database within the application infrastructure.

- No data is stored in third-party cloud services beyond what the integration providers (Zoom, Google) require.

5.2 Encryption

- **At Rest:** AES-256 encryption for sensitive fields in the database.
- **In Transit:** TLS 1.3 for all external communications.
- **Tokens:** OAuth access tokens and refresh tokens are stored encrypted.

5.3 Access Controls

- Database is accessible only within the internal Docker network.
- Application-level RBAC ensures users can only access their own data.
- Multi-tenancy isolation prevents cross-organization data access.
- No direct database access is provided to end users.

5.4 Response Security

- OAuth tokens are never included in HTTP responses to clients.
- Sensitive fields are actively stripped from all API responses via `onSend` hooks.
- Cache-Control: no-store headers prevent browser/proxy caching of sensitive data.

6. Data Retention

6.1 Retention Periods

Data Type	Retention Period	Trigger for Deletion
User account data	Duration of account + 30 days	Account closure request
Email content	Duration of account	Account closure or user deletion
Calendar events	Duration of account	Account closure or user deletion
OAuth tokens (Zoom/Google)	Until disconnection or expiration	User disconnects integration, or deauthorization webhook
OAuth user info (email, name)	Until disconnection	User disconnects integration
Meeting data (URLs, IDs)	Tied to calendar event	Calendar event deletion
Application logs	90 days	Automatic rotation
Analytics data	12 months	Automatic purge

6.2 Zoom-Specific Data Handling

When a user disconnects the Zoom integration:

1. OAuth access token is revoked via Zoom's `/oauth/revoke` endpoint.
2. Access token, refresh token, and associated metadata are deleted from the database.
3. The integration record is permanently removed.

When Zoom sends a deauthorization webhook (`app_deauthorized` event):

1. The application verifies the `client_id` matches.
2. A data compliance request is sent to `https://api.zoom.us/oauth/data/compliance`.
3. All integration records for the deauthorized Zoom user are deleted.

6.3 Google-Specific Data Handling

When a user disconnects the Google integration:

1. OAuth tokens are deleted from the database.
2. The integration record is permanently removed.

3. Google Calendar events created by the app remain on the user's Google Calendar (owned by the user).

7. Data Deletion

7.1 User-Initiated Deletion

- Users can disconnect integrations at any time from Settings > Calendar > Video Conferencing.
- Users can request full account deletion by contacting support.
- Account deletion triggers removal of all associated data within 30 days.

7.2 Automatic Deletion

- Expired OAuth tokens are cleaned up during the refresh cycle.
- Deauthorization webhooks trigger immediate data deletion.
- Application logs are automatically rotated after 90 days.

7.3 Data Export

- Users can request a data export within 30 days of account closure.
- Export includes account information, email data, and calendar events.
- OAuth tokens and internal system data are excluded from exports.

8. Third-Party Data Sharing

- Calimatic Mail does **not** sell, rent, or share user data with third parties.
- Data is shared with Zoom and Google only as required for the integration to function (creating meetings, reading user profiles).
- No analytics, tracking, or advertising data is shared with any third party.
- No third-party tracking cookies are used.

9. Compliance

This policy is designed to be compatible with:

- **GDPR** (General Data Protection Regulation)
- **CCPA** (California Consumer Privacy Act)
- **Zoom Marketplace** data handling requirements
- **Google API Services User Data Policy**

10. Review Cycle

This policy is reviewed annually or when:

- New data types are collected
- New integrations are added
- Regulatory requirements change
- After any data breach or incident

Approved by: Engineering Team, Caliber Technologies Inc. **Contact:** privacy@calimatic.app