Data Retention Policy

Title:	Data Retention Policy
Document Version:	1.0
Document Type:	Policy
Company:	InboxTidy Ltd.
Document Number	IT-POL-101

1. Purpose

This document defines the data retention, storage, and deletion principles applied by InboxTidy. It ensures that customer data is handled in a secure, compliant, and transparent manner, aligned with data protection regulations and customer expectations.

2. Scope

This policy applies to all data processed by InboxTidy within a customer's Microsoft 365 tenant, including:

- Email content processed for categorisation and drafting
- Metadata generated by InboxTidy (e.g., categories, classifications)
- System logs and operational telemetry
- Configuration and user-defined settings

3. Revision History

Revision	Change Description	Date (DD-MMM-YYYY)
1.0	Initial Draft	28-04-2026

4. Sign-Off

Version	Signed off by	Position	Date (DD-MMM-YYYY)
1.0	Steve Brown	CEO and Chief Architect	28-04-2026

5. Core Principle: Tenant-Hosted Data Control

InboxTidy is designed to operate **within the customer's Microsoft 365 tenant**. As a result:

- Customer data **remains within the customer's environment at all times**
- InboxTidy does **not persistently store email content externally**
- Data governance and retention policies are primarily controlled by the customer's existing Microsoft 365 configuration

6. Data Categories and Retention Rules

6.1. Email Content

- InboxTidy processes email content **in-memory only** for classification and drafting purposes
- No persistent storage of raw email content occurs outside the customer tenant
- Retention is governed by the customer's Microsoft 365 retention policies

6.2. AI Processing Data

- Temporary processing data (e.g., prompts, classifications) may be generated during execution
- This data is:
    - Not stored long-term
    - Not used for model training outside the customer environment
    - Automatically discarded after processing

6.3. Metadata and Categorisation

- Metadata such as:
    - Email categories
    - Priority flags
    - Classification tags
- Stored within the customer's tenant (e.g., mailbox properties or associated data structures)
- Retained in line with the lifecycle of the email unless explicitly removed

6.4. System Logs and Telemetry

InboxTidy generates limited operational telemetry for service support, fault investigation, and performance monitoring.

Telemetry includes:

- Processing timestamps
- System events and error logs
- Session IDs, flow run IDs, and event IDs
- Service URLs and technical operation references

InboxTidy telemetry does not include:

- Email body content
- Attachments
- Mailbox content
- Personal identifiers taken from emails or users

Telemetry stored by InboxTidy is limited to high level technical data only. It is not sufficient on its own to identify an individual or reconstruct email activity.

Storage and retention:

Customer environment data is stored within the customer's Microsoft 365 and Power Platform environment, subject to the customer's own retention settings and controls.

InboxTidy support telemetry stored outside the customer environment is kept only in a separate, secure logging environment and is limited to technical support and service monitoring data.

External support telemetry is retained for the duration of the customer contract, unless a shorter period is required by law, contract, or specific deletion request.

InboxTidy personnel cannot view customer email content from telemetry data alone. Any access to customer data for support purposes requires authorised access to the customer environment.

7. Data Deletion

7.1. Customer-Controlled Deletion

- Deletion of emails or mailbox data within Microsoft 365 results in corresponding removal of InboxTidy-associated metadata
- InboxTidy does not maintain independent copies requiring separate deletion workflows

7.2. Log Deletion

- Logs are automatically deleted after the defined retention period
- Customers may request earlier deletion where applicable

7.3. Service Decommissioning

Upon termination of the InboxTidy service:

- No customer email data is retained by InboxTidy
- Any associated logs or configuration data are deleted within 30 days.

Data Residency

- Primary data residency is determined by the customer's Microsoft 365 tenant location
- InboxTidy does not transfer or replicate email content outside the tenant boundary
- Any supporting services (if used) will adhere to defined regional hosting constraints

8. Compliance and Regulatory Alignment

- InboxTidy is designed to support compliance with:
  - UK GDPR
  - EU GDPR
  - Applicable data protection and privacy regulations
- Key compliance principles include:
  - Data minimisation
  - Purpose limitation
  - Storage limitation
  - Security and confidentiality

9. Security Considerations

- No long-term storage of sensitive email content outside customer control
- Encryption in transit (TLS 1.2+) and at rest (via Microsoft 365 controls)
- Strict access controls for any operational logging environments

10. Customer Responsibilities

Customers remain responsible for:

- Configuring Microsoft 365 retention and deletion policies
- Managing mailbox lifecycle and access controls
- Ensuring compliance with their internal data governance standards

11. Policy Review

This policy will be reviewed at least annually or upon:

- Significant architectural changes
- Regulatory updates
- Customer or audit requirements