

MERCURY ECHO CLOUD

Data Retention, Storage, and Deletion Policy

Effective Date: 8 June 2026 | Version 1.0 | Forms part of the Terms and Conditions of Service

This Policy forms an integral part of the Mercury Echo Cloud Terms and Conditions of Service and should be read in conjunction with them. Defined terms used herein have the meanings given to them in the Terms and Conditions.

1. PURPOSE AND SCOPE

1.1 This Data Retention, Storage, and Deletion Policy ("Retention Policy") sets out the rules governing how long Mercury Echo Cloud ("the Company") retains User data, the conditions under which storage fees may be applied, and the circumstances in which data may be deleted or made unavailable.

1.2 This Retention Policy applies to all Users, Authorised Users, and data processed through the Mercury Echo Cloud platform, including Evidence Trails, messages, records, translations, audit logs, attachments, and any other content stored on the platform.

1.3 Data retention is closely linked to the User's subscription status and, specifically, to the highest user-count tier reached during the subscription. Changes to the subscription level — including downward adjustments to the number of Authorised Users — may affect the applicable retention arrangements and fees as set out in this Policy.

2. CORE RETENTION PRINCIPLE — SUBSCRIPTION-LINKED RETENTION

2.1 The Company's foundational retention principle is as follows:

Data will be retained for the full duration of an active subscription, provided the subscription is maintained at or above the highest user-count tier previously held by the User. Where this condition is met, no additional storage fee will be imposed solely on the basis of data volume or age.

2.2 The retention period is defined by the life of the subscription. So long as the subscription remains active and the user count is maintained at its historical peak level, the User's data — including all Evidence Trails, audit logs, message records, translations, and associated metadata — will be preserved in its entirety and made available to the User through the platform.

2.3 For the avoidance of doubt: the Company does not impose an arbitrary maximum retention period (e.g., 12 months or 36 months) upon active subscriptions held at the qualifying user-count level. Retention is open-ended for the subscription term.

3. DETERMINATION OF HIGHEST USER-COUNT TIER

3.1 The "highest user-count tier" refers to the maximum number of Authorised Users for which the User was subscribed and billed at any point during the lifetime of the account. This is measured by reference to the billing records held by the Company and is not subject to retroactive revision.

3.2 Where a User upgrades their subscription to accommodate additional Authorised Users, the new higher tier becomes the reference point for this Policy going forward from the date of that upgrade.

3.3 Trial periods, promotional allocations, or complimentary user seats that were never billed do not count toward the highest user-count tier for the purposes of this Policy.

4. DOWNWARD ADJUSTMENT OF USER COUNT — STORAGE FEES

WHERE A USER'S SUBSCRIPTION USER COUNT IS REDUCED CONSIDERABLY BELOW THE HISTORICAL PEAK, THE COMPANY RESERVES THE RIGHT TO IMPOSE STORAGE FEES AT ITS DISCRETION. ANY SUCH FEE WILL NOT EXCEED THE EQUIVALENT COST OF THE REDUCED USER-COUNT TIER.

4.1 Right to Apply Storage Fees. Where the Company, in its reasonable discretion, determines that a User's user count has been reduced considerably relative to the historical peak tier, the Company may apply a recurring storage fee to cover the cost of retaining data accumulated during the period of higher user-count activity. The assessment of whether a reduction is "considerable" is made by the Company and takes into account the proportional change in user count, the volume of data retained, and the duration of the higher tier.

4.2 Fee Cap. Any storage fee imposed under this clause shall not exceed the amount that would have been payable for the equivalent tier corresponding to the reduced user count. For example: if a User reduces from a 100-user tier to a 10-user tier, the storage fee for retained data shall not exceed the cost differential between the 100-user and 10-user pricing plans, or the cost of the 10-user tier, whichever is the lesser. The Company will not use storage fees as a mechanism to recover revenue beyond what is proportionate to the reduced subscription level.

4.3 Notice of Storage Fee. Before imposing any storage fee under this clause, the Company will provide the User with written notice (via the registered email address or in-platform notification) specifying:

- The applicable fee amount and billing frequency;
- The basis for the fee (i.e., the reduction in user count and the volume of data affected);
- The date from which the fee will be charged (no earlier than 14 days from the notice date);
- The User's options: pay the storage fee, export and delete the relevant data, or upgrade the subscription to the qualifying tier to remove the fee.

4.4 User's Options Upon Notice. Upon receipt of a storage fee notice, the User may:

- Accept the storage fee, which will be charged in advance on the next billing date;
- Export and permanently delete the relevant data within 14 days of notice, in which case no storage fee will apply in respect of the deleted data;
- Reinstate the subscription to the qualifying historical peak tier, in which case no storage fee will be applied.

4.5 Failure to Act. If the User does not respond to the storage fee notice within 14 days, the Company reserves the right to apply the notified storage fee automatically or, at its election, to commence a data archival process pending the User's instruction. The Company will not delete data without separate specific notice under Clause 7.

4.6 No Retrospective Fees. Storage fees will not be applied retrospectively to periods before the notice date. They will apply prospectively from the date specified in the notice.

5. DATA SECURITY, INTEGRITY, AND PRESERVATION

IMPORTANT: WHILE THE COMPANY WILL USE ITS BEST EFFORTS TO KEEP DATA SAFE AND PRESERVED AT ALL TIMES, THE COMPANY DOES NOT GUARANTEE ABSOLUTE DATA SECURITY OR UNINTERRUPTED AVAILABILITY. NO SYSTEM IS ENTIRELY IMMUNE FROM TECHNICAL FAILURE, CYBERATTACK, OR FORCE MAJEURE.

5.1 Best Efforts Standard. The Company will use commercially reasonable and technically appropriate measures to maintain the security, integrity, and availability of User data at all times during an active subscription. These measures include, but are not limited to:

- Encryption of data at rest and in transit using industry-standard protocols;
- Regular automated backups to geographically distributed storage systems;
- Access controls and authentication mechanisms to prevent unauthorised access;
- Activity monitoring and anomaly detection;

- Physical and logical security controls at data centre facilities;
- Incident response procedures for data security events.

5.2 Honest Limitation. Despite the above measures, the Company honestly acknowledges that:

- No technical system provides an absolute guarantee against data loss, corruption, or breach;
- Events outside the Company's reasonable control — including cyberattacks, zero-day vulnerabilities, natural disasters, force majeure events, or failure of third-party infrastructure providers — may result in data unavailability or loss;
- The Company's obligation is one of best efforts and reasonable care, not an absolute guarantee of preservation.

5.3 User's Own Backup Obligation. The User is strongly advised to maintain independent, off-platform backups of any critical data, Evidence Trails, or records. The Company's retention obligations complement but do not substitute for the User's own data management responsibilities. The Company shall not be liable for any loss or damage arising from the User's failure to maintain independent backups.

5.4 Evidence Trail Integrity. The Company employs specific technical controls designed to maintain the tamper-evident nature of Evidence Trail records. These include cryptographic hashing, audit logging, and write-once storage mechanisms where technically feasible. However, the Company does not guarantee that these mechanisms will satisfy any particular legal or evidentiary standard in any jurisdiction.

5.5 Security Incident Notification. In the event of a data security incident that materially affects the User's data, the Company will notify the User within a reasonable time after the incident is identified, to the extent legally permissible and operationally feasible.

6. DATA ACCESS AND RETRIEVAL DURING ACTIVE SUBSCRIPTION

6.1 During an active subscription, the User may access and retrieve their data through the standard platform interface at no additional charge, subject to the functionality available at the applicable subscription tier.

6.2 Enhanced Retrieval Services — including certified exports, bulk extraction, custom format requests, or retrieval for legal proceedings — may be subject to Retrieval Service fees as set out in Clause 5 of the Terms and Conditions.

6.3 Where a storage fee has been applied under Clause 4 of this Policy, access to the relevant data remains available to the User pending the User's decision regarding that data.

7. SUBSCRIPTION EXPIRY, CANCELLATION, AND POST-TERMINATION DATA HANDLING

7.1 Grace Period. Upon expiry or cancellation of a subscription (for any reason other than termination for breach), the Company will retain the User's data for a grace period of thirty (30) calendar days from the effective date of expiry or cancellation ("Grace Period"). During the Grace Period, the User may log in and export their data.

7.2 Retrieval During Grace Period. Data retrieval during the Grace Period is subject to the Retrieval Service fees in the Terms and Conditions where the retrieval exceeds the functionality available through the standard interface.

7.3 Post-Grace Period Deletion. After the Grace Period has elapsed without renewal or reinstatement of the subscription, the Company reserves the right to permanently and irrecoverably delete all User data. The Company will provide no less than 7 days' written notice of its intention to delete data before doing so.

7.4 No Guarantee of Post-Termination Recovery. After data has been deleted following the Grace Period, the Company provides no guarantee that any data can be recovered. The User acknowledges

and accepts this risk. If recovery is technically feasible, it will be subject to Retrieval Service fees and is at the Company's sole discretion.

7.5 Termination for Breach. Where the Company terminates the User's account for breach of the Terms and Conditions, data retention is at the Company's discretion. The Company may retain data for a minimum of 30 days to facilitate any legal, regulatory, or dispute-resolution processes, and may make data available to the User (subject to Retrieval Service fees) during that period. After 30 days, the Company may delete the data without further notice.

7.6 Regulatory Hold. Notwithstanding the above, the Company may retain User data beyond the standard retention period where it is required to do so by applicable law, court order, regulatory direction, or for the purpose of ongoing legal proceedings. The User will be notified of any such hold where legally permissible.

8. DATA DELETION AND PURGING

8.1 Permanent Deletion. Where data is deleted in accordance with this Policy, deletion means permanent and irrecoverable removal from the Company's active systems. Residual copies may persist in backup systems for a period of up to 90 days following deletion from active systems, after which they will be purged in the ordinary course of backup rotation.

8.2 User-Requested Deletion. The User may request deletion of specific data or their entire account at any time. Such requests will be processed within 30 days. Data deletion is irreversible, and the Company will not be liable for any consequences arising from deletion requested by the User. No refund will be issued in connection with User-initiated deletion.

8.3 Evidence Trail Records. Where Evidence Trail records are subject to a legal hold, regulatory requirement, or are the subject of ongoing proceedings notified to the Company, the Company will not delete those records notwithstanding a User request, until the relevant hold is lifted.

9. RETENTION SUMMARY TABLE

The following table summarises the key retention scenarios for reference. In the event of any conflict between this table and the body of the Policy, the body of the Policy shall prevail.

Scenario	Retention Period	Storage Fee	Notes
Active subscription at highest-ever user count	Full duration of subscription	None	All data retained without additional charge
Active subscription — user count reduced but above threshold	Full duration of subscription	None initially; discretionary fee may apply	Company may apply storage fees at its discretion if reduction is considerable
Active subscription — user count reduced considerably (at Company discretion)	Full duration of subscription	May be charged; capped at equivalent cost of the reduced user-count tier	Written notice provided before fee is applied
Subscription cancelled / expired	Grace period of 30 days post-expiry	Standard retrieval fees may apply	User must export data within grace period
Post-grace period (expired subscription)	Data may be permanently deleted	Retrieval fee required (if technically feasible)	No guarantee of recovery after grace period
Post-termination for breach	Company discretion (minimum 30 days)	Retrieval fees apply	Company may impose additional conditions

10. ADDITIONAL PROTECTIONS AND ACKNOWLEDGEMENTS

10.1 Third-Party Infrastructure

The Company may utilise third-party cloud infrastructure, data centre, or storage providers in delivering the Service. The Company takes reasonable steps to ensure such providers maintain appropriate security standards but cannot guarantee the conduct of third parties. The Company is not liable for data loss or breach attributable to third-party infrastructure providers beyond what is recoverable under the Company's agreements with those providers.

10.2 Data Sovereignty

User data may be stored, processed, or backed up in data centres located in multiple jurisdictions. The User acknowledges and consents to cross-border data transfers as may be necessary for the provision and resilience of the Service. Where the User has specific data sovereignty requirements (e.g., data must remain within a particular country), the User must notify the Company in writing prior to account creation. The Company will endeavour to accommodate such requirements where technically and commercially feasible, but makes no guarantee of doing so without a specific written agreement.

10.3 Audit and Compliance Records

Certain data — including access logs, billing records, compliance records, and security incident logs — may be retained by the Company for its own regulatory and legal purposes for periods exceeding the User's subscription retention period. This retention is separate from the retention of User-generated content and does not entitle the User to continued platform access.

10.4 Changes to This Policy

The Company reserves the right to amend this Retention Policy at any time. Material changes will be notified to the User at least 30 days in advance via registered email or in-platform notice. Continued use of the Service after the effective date of the change constitutes acceptance of the revised Policy. Where a proposed change would materially reduce retention periods or increase storage fees beyond those set out herein, the Company will provide Users with a reasonable opportunity to export their data before the change takes effect.

10.5 No Property Right in Retained Data

Retention of data by the Company under this Policy does not create any property right, lien, or charge in favour of the Company over the User's data. The Company holds data solely as a processor and custodian on behalf of the User, subject to the terms of this Policy and the Terms and Conditions.

10.6 Evidence Trail Admissibility — Further Disclaimer

Even where the Company retains Evidence Trail records in accordance with this Policy, the User acknowledges that the format, metadata, and provenance of retained records may be affected by storage, compression, migration, or backup processes. The Company does not warrant that retained Evidence Trail records will satisfy any chain-of-custody, authenticity, or admissibility requirement. Users who require court-standard evidence preservation should obtain independent legal advice and consider instructing a specialist digital forensics provider.

10.7 Liability for Storage Fee Disputes

The User's sole remedy in respect of a disputed storage fee under Clause 4 is to raise the dispute in writing within 14 days of the fee being charged, as provided in the Terms and Conditions. The

Company's liability in respect of any storage fee wrongly charged shall not exceed the amount of the fee paid. The User may not withhold payment of undisputed amounts pending resolution of a storage fee dispute.

10.8 Interaction with Data Protection Laws

This Retention Policy is subject to and must be read in conjunction with applicable data protection laws, including any personal data retention requirements imposed by law. Where applicable law requires shorter retention periods for personal data than those specified herein, the shorter period will apply to that personal data. The User is responsible for ensuring that their use of the Service, and their own instructions regarding retention and deletion, comply with applicable data protection law.

11. CONTACT AND REQUESTS

For all data retention queries, deletion requests, storage fee disputes, or legal hold notifications, please contact the Company through the platform support portal at www.mercuryecho.cloud. The Company will acknowledge requests within 5 business days and endeavour to respond substantively within 30 days.

This Data Retention, Storage, and Deletion Policy forms part of the Mercury Echo Cloud Terms and Conditions of Service. In the event of any conflict, the Terms and Conditions shall prevail.

Last updated: 8 June 2026 | Mercury Echo Cloud | Version 1.0