Data Retention & Deletion Policy

1. Purpose

This policy defines retention periods for data processed by Subcontext and the procedures for secure deletion. It puts into practice the storage limitation principle of the UK GDPR: personal data is kept no longer than is necessary for the purposes it is processed for, and is then deleted or anonymised.

2. Scope

This policy covers:

- Customer data Subcontext processes as a processor on behalf of its customers, including contacts, conversations, call recordings, applications, policies, claims, agent configurations and knowledge content
- Data Subcontext holds as a controller, including platform user accounts, billing and payment records, sales and marketing contacts, and employee records
- Operational and security data, including audit logs, application logs, request logs and AI model call logs
- Data in every place it is held: the production database, file storage, logs, exports and backups, and data held by sub-processors on Subcontext's behalf

3. Principles

- **Purpose-led:** each category of data has a defined purpose, and its retention period is set by that purpose, by law or by contract
- **Automated where possible:** retention is enforced by scheduled jobs in the platform rather than relying on people remembering to delete data
- **Customer-controlled:** customers, as controllers, can set shorter or longer periods for certain data within the limits in this policy, and can delete data themselves at any time
- **Legal hold overrides deletion:** data subject to a legal hold, regulatory investigation or live dispute is preserved until the hold is lifted
- **Records that must be kept are kept:** where the law or regulation requires a record to be retained, for example billing records or an insurance file, deletion is refused or deferred and the reason is recorded

4. Roles and Responsibilities

Role	Responsibility
Directors	Approve this policy and its retention schedule, and approve legal holds and exceptions
Security Officer	Maintains this policy, oversees the automated retention jobs, handles deletion requests on termination and confirms deletion in writing on request

Role	Responsibility
Engineering	Builds retention into every new data store and feature, and makes sure retention jobs run and are monitored
Customers	Set retention for configurable data, delete data they no longer need, and respond to their own data subjects' erasure requests

5. Retention Schedule

Data Category	Retention Period	Basis
Customer account data	Duration of account + 12 months	Contractual + legitimate interests
Conversation content and messages	Duration of account + 90 days	Contractual
Contact data and consent records	Duration of account + 90 days	Contractual (processor obligation)
AI-generated memories	Duration of account + 90 days	Contractual
Audit logs	24 months	Legitimate interests (security)
LLM API call logs	12 months	Legitimate interests (cost management)
Payment and billing records	7 years	Legal obligation (HMRC)
Security logs	12 months	Legitimate interests (security)
Web crawl data	Duration of knowledge base	Contractual
Escalation records	Duration of account + 90 days	Contractual
Integration credentials	Deleted on removal or account closure	Contractual
Employee records	Duration of employment + 6 years	Legal obligation

5.1 Automatically enforced periods

The platform deletes or scrubs the following on a schedule, without manual action:

Data	Kept for
Visitor IP addresses and browser details on conversations and enquiries	90 days (1 year where the conversation was escalated or flagged as spam)
Website page-view analytics, voice call events and inbound email logs	1 year
Audit log, email delivery logs and email events	2 years
Integration request logs	90 days
API request logs	3 months
AI model call logs	13 months
Application error reports	90 days

Data	Kept for
Performance monitoring data	10 days
Voice call recordings	365 days by default, configurable per customer (or kept until the customer deletes them); recordings under legal hold are exempt
Raw lead data received from customers' systems	365 days by default, configurable per customer
Lead activity events	180 days by default, configurable per customer
Compliance decision records (tamper-evident, hash-chained)	6 years by default, configurable per customer between 3 and 25 years
Data exports	7 days
Inbound email held for processing	30 days
Signed-in sessions	Expire after 30 days of inactivity; records deleted after 1 year
Payment provider event records	7 years
Unclaimed trial accounts	90 days

5.2 Notes on the schedule

- **Conversations** are closed automatically after 7 days without activity. Closing a conversation does not delete it: its content is kept in line with the schedule above
- **Infrastructure logs:** application logs, network flow logs and web application firewall logs are kept for 30 days, as set out in the Logging & Monitoring Policy
- **Compliance decision records** cannot be purged if their hash chain has been broken, so that tampering is never hidden by deletion
- **Configurable periods** are set by the customer in the platform. Where a customer has not set a period, the default applies

6. Deletion Procedures

6.1 On termination

- Upon account termination, customer data is deleted within 90 days of the effective termination date
- Customers may request data export during a 30-day post-termination window
- Deletion includes removal from primary databases and search indices
- Encrypted backups containing deleted data are rotated in the ordinary course (typically within 30 days)
- Deletion of data held by sub-processors is handled through contractual obligations

Deletion of a whole customer organisation is carried out on request, following these steps:

1. The request is confirmed with an owner of the customer organisation, and the effective termination date is recorded
2. The customer is reminded of the export options in the Exit Plan & Data Return Policy and of the 30-day post-termination export window

3. Any data that must be kept, such as payment and billing records, or data the customer has instructed us in writing to retain, is identified
4. The organisation's data is deleted from the primary database and search indices, and its integration credentials are deleted
5. Phone numbers and messaging sender identities are released, and sub-processors holding the organisation's data are instructed to delete it where they do not do so automatically
6. The deletion is recorded, and confirmed to the customer in writing on request

6.2 During the life of an account

- Customers can remove data they no longer need, for example by erasing a lead or deleting voice recordings
- Data covered by an automatic period in section 5.1 is deleted or scrubbed by the platform when that period ends
- Integration credentials are deleted when the integration is removed
- When a platform user deletes their account, their personal details are removed and their sessions, tokens and devices are revoked

6.3 Methods

- Data in the database is deleted, or scrubbed so that it no longer identifies anyone where a minimal record must be kept (for example to make sure an erased contact is not contacted again)
- Files in storage are deleted, and inbound email objects expire automatically after 30 days
- Data in backups is not edited, but expires as backups are rotated, and is never restored into live use without the deletion being re-applied

7. Data Subject Deletion Requests

- Customers (as data controllers) are responsible for responding to data subject erasure requests
- Subcontext will assist customers in fulfilling erasure requests in accordance with the Data Processing Agreement
- Direct requests from data subjects are forwarded to the relevant customer

Customers can erase a lead themselves, as described in the Data Subject Rights Procedure. Erasure is refused, with the reason given, where the person holds a live insurance policy, has an application in progress or has made a claim.

8. Legal Holds and Exceptions

- A legal hold may be placed on data where it is needed for a legal claim, a regulatory investigation, a complaint or an incident investigation. A hold is approved by a director, recorded with its reason, and reviewed at least every six months
- Data under legal hold is exempt from automatic deletion until the hold is lifted, after which normal retention resumes
- Any other exception to this schedule, such as keeping data longer at a customer's written instruction, must be documented, approved by a director and limited in time

9. Compliance and Monitoring

- Retention jobs run automatically, and failures are reported through the platform's error monitoring
- The Security Officer checks at least annually that each retention job is running and that data older than its period is not being kept
- Every new data store or category of data is given a retention period before it goes live

10. Review

This schedule is reviewed annually to ensure alignment with legal requirements and business needs.

11. Related Documents

- Data Classification Policy
- Data Subject Rights Procedure
- Exit Plan & Data Return Policy
- Logging & Monitoring Policy
- Business Continuity & Disaster Recovery Policy
- Sub-Processor List
- Data Protection Impact Assessment

12. Document Control

Item	Detail
Owner	Security Officer
Approved by	The directors of Subcontext Ltd
Review	At least annually, and when legal requirements or the platform's data change significantly
Effective	October 2026

Subcontext Ltd, registered in England and Wales, Company No. 17019645. Registered office: 124 City Road, London, EC1V 2NX. The current version of this document is published at subcontext.com.