POLICY DOCUMENT

Data Retention & Disposal Policy

Retention and disposal aligned to UK GDPR / GDPR storage limitation

DOCUMENT TYPE	Policy
VERSION	1.1 · Effective 7 May 2026
SUPERSEDES	v1.0 · 12 December 2025
OWNER	Remote-I Ltd — Data Protection Lead
CLASSIFICATION	Internal / Customer Assurance
REVIEW CYCLE	Annual, and after changes to data categories or legal requirements

ORGANISATION

Remote-I Ltd

Company No: 15293974
Registered Office: 45 Fitzroy Street, 4th Floor, Silverstream House, London, England, W1T 6EB

Privacy contact: compliance@remote-i.com
Operational support: support@remote-i.com
Data Protection Lead: Remote-I Ltd — Data Protection Lead

V1.1 · EFFECTIVE 7 MAY 2026 · SUPERSEDES V1.0 (12 DECEMBER 2025)

> *This Data Retention & Disposal Policy defines how Remote-I retains and disposes of data processed via the Platform in a manner consistent with UK GDPR / GDPR storage limitation, confidentiality, and governance requirements.*

1. Purpose

This Policy is operationally linked to:

- The Remote-I **Privacy Policy** (Section 8 — Data Retention) which mirrors this schedule for Data Subjects;
- The Remote-I **Data Processing Agreement (DPA)** (Section 2.7 — Deletion or return of Personal Data); and
- The Remote-I **Information Security Policy** (Section 6 — Asset Management and Data Classification).

2. Scope

Applies to Customer Data and Remote-I business records, including platform records, uploaded compliance documentation, audit logs, notification metadata, support tickets, and backups.

3. Principles

Remote-I follows: storage limitation, minimisation, secure disposal, and auditability. Retention may be extended for legal holds or investigations.

4. Responsibilities

Customer (Controller) defines retention requirements for Customer Data within the configurable ranges below.

Remote-I (Processor) implements automated retention and deletion processes where technically feasible, supports Customer requests per the DPA, and provides evidence of retention enforcement on reasonable request.

5. Implementation status (transparency notice)

Retention is enforced through a combination of automated cron jobs and manual deletion processes. As of v1.1 effective date, the implementation status of automated retention is:

Category	Automated retention	Implementation status
Audit logs	Yes — daily cron, configurable via environment variable	`Active (deployed 7 May 2026)`
Password reset tokens	Yes — daily cron	`Active`
Email verification tokens	Yes — daily cron	`Active`
MFA codes	Yes — daily cron	`Active`
Hospital invitations	Yes — daily cron	`Active`
Backups	Yes — hosting rotation	`Active (30-day rotation)`
Other categories	Manual deletion on request, or scheduled implementation	`In progress`

For categories marked "in progress", Customers may request deletion of specific data at any time via compliance@remote-i.com. Automated retention for these categories is being developed and deployed progressively. Customers will be notified when full automation is achieved.

6. Retention Schedule

Retention periods are baseline; Customers may configure tighter or longer retention within the configurable ranges, subject to Platform capability and contract terms.

Data category	Examples	Baseline retention	Disposal method	Notes
Account & identity data	User name, email, role, MFA status	Active subscription term + 12 months	Logical deletion / anonymisation	Security investigations, dispute resolution. Customer may request earlier deletion on user request.
Job lifecycle records	Job posts, assignments, timestamps, handover notes	12–24 months (configurable)	Logical deletion after expiry; backups rotate within 30 days	Operational review and governance reporting. Default: 24 months.
SOP acknowledgements	Sign-off records, SOP versions	7 years (clinical governance baseline)	Logical deletion after expiry; backups rotate	`V1.1 UPDATE` extended from 24 months to 7 years for clinical governance and CQC inspection alignment. Customer may apply shorter retention only with documented risk acceptance.
Compliance — Right-to-Work evidence	RtW documentation	2 years post-engagement (UK Home Office statutory)	Secure deletion; backups rotate	`V1.1 UPDATE` specified separately to reflect statutory requirement.
Compliance — DBS evidence	DBS / criminal record check confirmations	12 months post-engagement	Secure deletion; backups rotate	Reduce to absolute minimum where practical.

Data category	Examples	Baseline retention	Disposal method	Notes
Compliance — Training & insurance	Training certificates, insurance evidence	6 years (clinical governance baseline)	Secure deletion; backups rotate	`V1.1 UPDATE` extended for clinical governance alignment.
Incident records & reflections	Incident entries, reflections, metadata	24 months (configurable, may extend to 7 years for clinical incidents)	Logical deletion after expiry; backups rotate	Supports investigations and learning. Customer may extend for clinical governance.
Audit / security logs	Auth events, admin actions, exports	12 months (default, configurable up to 24 months)	Automated daily deletion via `cron_retention.php`	Configurable via `RETENTION_AUDIT_DAYS` environment variable. NHS DSPT customers typically require 24 months minimum.
Authentication tokens	Password reset, email verification, MFA codes	2 days past expiry	Automated daily deletion via `cron_retention.php`	Configurable via `RETENTION_RESETTOKENS_DAYS`.
Notification metadata	Delivery attempts, timestamps, recipient identifiers	6–12 months	Logical deletion (manual or scheduled)	`V1.1 UPDATE` body content not retained beyond delivery; only metadata.
Free-text fields in incidents/notes	Inline text within incident/ reflection records	Same as parent record (24 months / 7 years)	Deletes with parent record	Customer responsible for minimisation.
Login attempt records	Failed login attempts, account lockout events	90 days	Logical deletion	`V1.1 ADDITION` distinct from general audit logs; tighter retention.
Session data	Session tokens, "remember me" tokens	Until expiry plus 7 days for forensic continuity	Automated session expiry	`V1.1 ADDITION` previously implicit.
Backups	DB / file / app archives	30 days (default)	Rotation and deletion via hosting backup cycle	Extended retention may be agreed for legal holds.
Support records	Support emails and tickets	24 months	Manual deletion / archive	`V1.1 UPDATE` held in Processor email system, not Platform; retention applies to Processor's email archive.

Data category	Examples	Baseline retention	Disposal method	Notes
Billing & legal records	Invoices, contracts, procurement docs	6 years	Secure archive then deletion	UK statutory requirement (Companies Act, HMRC).

Notes on the schedule

"Active subscription term" means the period during which Customer holds an active Order Form with Processor. On termination, the post-termination retention period begins.

"Active engagement" for compliance documents means the period during which the radiographer is actively contracted to or working through a Customer's hospital. On de-engagement, the post-engagement retention period begins.

"Logical deletion" means removal from the production database query path. Physical purge occurs on the next backup rotation cycle (30 days), so "logical deletion + backup rotation" represents the full purge timeline.

"Secure deletion" for sensitive categories means logical deletion with restricted-permission access during the rotation window, followed by physical purge on backup cycle. Backup archives are stored outside the public web root with restrictive file permissions.

7. Disposal procedures

7.1 Database records

Records subject to retention are removed via parameterised SQL DELETE statements run by `cron_retention.php` daily at 02:15 UTC. The script:

- Validates table existence and column structure before deletion;
- Uses configurable retention windows via environment variables;
- Records every run as a `RETENTION_RUN` audit event with row counts and any errors;
- Operates within database transactions where supported.

7.2 Uploaded files

Files associated with deleted records (compliance documents, attachments) are removed from the file storage directory at the point of record deletion. Backup archives retain a copy for 30 days per backup rotation policy.

7.3 Backups

Backups follow a 30-day rotation: each daily backup is retained for 30 days, after which it is securely deleted from the backup storage location. Extended retention is applied only by documented exception (e.g., legal hold, active investigation).

7.4 Logs and operational records

Application logs are rotated by `cron_rotate_logs.sh` daily at 02:05 UTC. Rotated logs are compressed and retained for the period defined in the Logging & Monitoring Policy.

8. Customer requests

Customers may request:

- **Earlier deletion** of specific Customer Data (e.g., to honour a Data Subject erasure request)
- **Extended retention** of specific Customer Data (e.g., for legal hold, regulatory investigation)
- **Verification** that retention is being enforced as documented
- **Bulk export** of Customer Data prior to deletion

Requests should be sent to **compliance@remote-i.com**. Standard response time: within statutory windows for Data Subject Rights requests (1 calendar month under UK GDPR), or within 10 business days for general retention queries.

9. Legal holds

Where Processor or Controller is subject to a legal hold (e.g., active litigation, regulatory investigation, criminal proceedings), the affected categories are exempted from automated deletion until the hold is lifted. Holds are documented with:

- Scope of data subject to the hold;
- Reason and authority requiring the hold;
- Expected duration or trigger for release;
- Periodic review to confirm continued necessity.

10. Document Changelog

Version	Date	Changes
1.1	7 May 2026	Aligned retention schedule with Privacy Policy v1.1 (web-published 7 May 2026) and platform implementation reality. Added "Implementation status" transparency section (Section 5). Extended SOP acknowledgements to 7 years for clinical governance. Split compliance documents by sub-category (Right-to-Work, DBS, training/insurance) reflecting statutory differences. Added missing categories (login attempts, session data, free-text fields). Added explicit disposal procedures (Section 7) with reference to actual cron implementation. Added Customer requests procedure (Section 8) and Legal holds (Section 9). Added cross-references to Privacy Policy, DPA, and ISP.
1.0	12 December 2025	Initial version. Baseline retention schedule established.

Changes pending in future revisions

- **Automation roll-out for "in progress" categories:** As cron-based retention is extended to cover job lifecycle records, SOP acknowledgements, incident records, notification metadata, and account data, the implementation status table in Section 5 will be updated.
- **Soft-delete pattern:** For sensitive categories (account data, compliance documents), logical deletion will transition to a `deleted_at` soft-delete pattern, with physical purge on a separate schedule. This change will be reflected in v1.2.

End of Data Retention & Disposal Policy v1.1. For enquiries, contact compliance@remote-i.com.

REMOTE-I LTD · COMPANY NO. 15293974 · COMPLIANCE@REMOTE-I.COM