Record Retention & DSAR Policy

Growthack Ltd

Issue date:	9th October 2025	**Review date:**	Up to 12 months after issue date

Version: 1	**Issued by:** Kevin Kapezi

Purpose:	This policy defines how Growthack Ltd retains and deletes personal and business data in line with UK GDPR Article 5(1)(e) and IASME Cyber Assurance controls for storage limitation. Our DSAR procedure ensures that Growthack Ltd can respond lawfully and efficiently to data subject rights requests in line with UK GDPR. This policy applies to all personal and business data processed by Growthack Ltd as a data controller, and supports IASME Cyber Assurance control areas A7.6 (Data Management) and A7.7 (Data Subject Rights).

Scope:	Applies to all records created, received, or maintained by Growthack Ltd in the course of business, including operational, financial, legal, personnel, and project documentation, regardless of medium or storage location. Records are stored securely within authorised systems, including Google Workspace, HubSpot, ClickUp, QuickBooks Online and other approved platforms.

Associated documentation:	• Security Policy • Business Continuity & Disaster Recovery Policy • Employee Handbook
Approved by:	The Director(s): Kevin Kapezi
Date:	9th October 2025

Review and consultation process:	Annually from the review date above. If applicable, the Cyber Security consultant will advise.
Responsibility for Implementation & Training:	Day-to-day responsibility for implementation: Kevin Kapezi, director Day-to-day responsibility for training: Kevin Kapezi, director
Distribution	Email attachment or shareable link

Contents

Record Retention Policy

1. Principles

Growthack Ltd will:

- Retain data only for the minimum time necessary.
- Delete or anonymise data once the purpose is fulfilled.
- Keep evidence of deletion or destruction for audit purposes.
- Review all retention periods annually.

2. Retention Schedule

Record Type	Retention Period	Basis	Disposal
Accounting and tax records	6 years after financial year end	HMRC requirement	Secure deletion
HR and payroll records	6 years after employment ends	Statutory	Secure deletion
Insurance and claims	7 years after expiry	Audit and compliance	Secure deletion
Contracts and project files	6 years after completion (12 if deed)	Legal limitation period	Secure deletion
Marketing lists (opt-in)	Until consent is withdrawn or after 3 years of inactivity	Consent / legitimate interest	Secure deletion
Website enquiries	12 months	Operational	Secure deletion
Backups	Rolling 30-day encrypted cycle	BCDR plan	Automatic overwrite
Security logs	12 months	IASME requirement	Automated deletion

3. Deletion Methods

Where data is held within cloud platforms, Growthack ensures that secure deletion requests follow platform-specific certified processes (e.g., ISO 27001, SOC 2).

- Electronic records will be securely erased from active and backup systems.
- Physical records will be shredded or destroyed through a secure disposal service.
- Cloud providers used by Growthack apply ISO 27001-aligned deletion standards.

4. Review and Audit

Internal spot checks are conducted at least once per year to confirm adherence.

Retention periods are reviewed annually and updated if regulations change.

Data Subject Access Request (DSAR) Procedure

1. Request Submission

Requests should be sent to **hello@growthack.io** or to Growthack's registered office.

All requests must include enough detail to locate the data.

2. Verification

The requester's identity will be verified before any data is shared.
Verification may require proof of ID or verification through known company systems.

3. Logging and Tracking

All DSARs are recorded in a central DSAR log that includes:

- Date received
- Request type
- Responsible officer
- Status and completion date

4. Response Times

Growthack will respond within 30 calendar days of verification.
If the request is complex, the response time may be extended by up to two months.
The requester will be informed of any extension.

5. Format of Response

Information will be provided securely in a structured, machine-readable format such as PDF or CSV.

6. Refusal or Exemptions

Requests may be refused where legal exemptions apply.
All refusals will include reasons and information on the right to complain to the ICO.

7. Record Retention

A record of the DSAR and correspondence will be kept for six years.