

Leesman Data Retention policy

Company	Leesman Ltd, an HqO company
Scope of Policy	This data retention policy is a formal framework that guides Leesman in managing its data. It specifies how long data should be kept, how it should be securely disposed of when no longer needed, ensuring legal compliance and responsible data management. This data retention policy primarily addresses external data, as Leesman maintains a separate internal data retention policy specifically tailored for employee data. For any further details, please refer to our privacy policy.
Data Category Subject of this Policy	This essential policy applies to all Leesman surveys, website visitors, recipients of emails, job applicants, Leesman employees (for good understanding), and third-party entities handling Leesman's data.
Policy Review Date	22nd September 2023, yearly update. 2nd October 2024, yearly update. 19th March 2025, yearly update. 20th March 2026, yearly updated.

1. OVERVIEW

A data retention policy is a formal framework that guides an organisation in managing its data. It specifies how long data should be kept, how it should be securely disposed of when no longer needed, ensuring legal compliance and responsible data management.

This data retention policy primarily addresses external data, as Leesman maintains a separate internal data retention policy specifically tailored for employee data.

Leesman follows ICO guidance and aligns its data retention practices with international data protection laws, mainly including GDPR (EU & UK).

Additionally, where artificial intelligence or automated decision-making processes are involved in data processing, Leesman ensures compliance with the transparency and accountability provisions of the EU AI Act.

2. PURPOSE

The purpose of this policy is to mitigate threats of non-compliance with regulatory, legal, and contractual requirements regarding data retention and disposal policies.

3. ROLES AND RESPONSIBILITIES

Role/Service	Responsibilities
Leesman Ltd (Data Processor)	Ensures compliance with GDPR and UK GDPR.
Client (Data Controller)	Manages data in accordance with contract terms and privacy laws
Director of Productions & IT	Ensure security configurations, encryption, backups, and proper data disposal
Data Protection Officer	Oversees policy enforcement and data privacy compliance
Chief Technology Officer	Aligns policies with technology strategies and ensures secure data management
Leesman Employees	Receive training on this policy and handle data securely

4. DATA RETENTION

Each of these data categories may have different retention requirements based on legal, regulatory, and business considerations.

4.1 Respondent Data

Leesman prioritises the anonymisation of survey data before retention. All data is anonymised, and confidential data is removed upon survey closure. The anonymised data forms part of the Leesman Benchmark database for long-term use in identifying global trends.

Personal data such as respondents' email addresses is retained only for login purposes and erased after survey closure. Alternative login methods, such as unique random reference IDs, are used when possible.

Leesman ensures compliance with ISO 27001/27701 security frameworks by applying rigorous access controls, encryption, and secure deletion mechanisms to all respondent data. Under GDPR (Article 6), all data collection and processing activities have a lawful basis, and individuals have rights to access, correction, and deletion.

5. DATA MINIMISATION

Leesman follows GDPR by ensuring that only necessary data is retained, and unnecessary records are securely deleted in a timely manner.

More information can be found in the Information Security Policy.

6. DISPOSAL

Leesman implements cross-border data transfer safeguards as per GDPR Articles 44-49, ensuring that any international data processing complies with Standard Contractual Clauses or UK International Data Transfer Agreements.

6.1. Disposable Schedule

Following ICO guidance, the rules of a disposal schedule identify:

- Classes of records
- The retention period for each class of record
- What should happen at the end of the retention period

6.2. Customer Data Disposal

Disposal of non-anonymised and non-aggregated customer data is carried out per contractual agreements with clients. If no agreement is in place, the client must submit a written request for data deletion.

A certificate of destruction is provided upon completion of data disposal.

7. AUDIT CONTROLS AND MANAGEMENT

Leesman maintains a documented audit log of all data subject access requests, rectifications, and erasures in compliance with GDPR, CCPA, and PIPEDA. Audit controls ensure privacy impact assessments are conducted where required, particularly in AI-driven decision-making.

On-demand documented procedures and evidence of compliance include:

- Policy records and updates
- Anecdotal and archival communications demonstrating policy implementation
- Training evidence
- Certification of destruction (if non-confidential)

8. ENFORCEMENT AND EXCEPTIONS

- **Non-Compliance**
Any staff, contractors, or affiliates found violating this policy may be subject to disciplinary action.
- **Exceptions**
All exceptions must be fully documented, with justifications. There are no exceptions listed as of today.
- **Review**
The policy is reviewed at least yearly or as necessary to maintain its relevance and effectiveness.

9. FURTHER QUESTIONS

For any concerns regarding data retention and compliance, please contact Leesman's Data Protection Officer at dataprotection@leesmanindex.com.