Halo Benefits

POLICY

Data Protection, Retention and Deletion Policy

How we protect, keep and delete personal data.

UPDATED	VERSION	NEXT REVIEW
23 November 2026	2.0	November 2027

Halo Benefits Ltd · Owner: Alexander Dick, Head of Security & Operations · Classification: Internal & Public

Document control

Policy owner	Alexander Dick, Head of Security & Operations
Approved by	Board of Directors
Date approved	23rd November 2026
Next Review Date	23th November 2027
Review frequency	Annually
Applies to	All directors, employees and contractors who handle personal data for Halo Benefits Ltd
Related policies	Supplier Security Policy, Incident Response Plan, Information Security Policy

Version history

Version	Date	Summary of changes	Author
1.0	30 Oct 2026	First issue	Alexander Dick
2.0	23 Nov 2026	Rebranded and restructured for clarity and readability	Dionne Clarke

Contents

1. Purpose of the policy 3
2. Scope 3
3. Our role and approach 3
4. Requests from individuals 3
5. How long we keep data 4
6. Deletion and contract end 4
7. Where data is stored 5
8. Personal data breaches 5
9. Roles and responsibilities 5
10. Compliance and exceptions 5
11. Review 6

1. Purpose of the policy

This policy sets out how Halo Benefits Ltd complies with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. It covers our role, how we handle requests from individuals, how long we keep data, how we delete it and how we protect data transferred outside the UK.

2. Scope

This policy applies to **Halo Benefits Ltd** (company number 17577358) and covers all personal data we process, both on behalf of our customers through the Halo Benefits platform and for our own purposes, such as our staff, recruitment, sales and supplier records.

3. Our role and approach

- **Processor:** for the Halo Benefits platform, the employer normally decides why and how employee and benefits data is processed, and we process it on the employer's instructions under a data processing agreement. The employer is responsible for its lawful basis, including any condition for special category data such as health information.
- **Controller:** we are the controller for our own staff, recruitment, sales and marketing, and supplier records, and for the security operation of our platform.
- **Principles:** we only process personal data for agreed purposes, collect no more than we need, keep it secure and apply clear retention rules.
- **Records:** we keep records of our processing activities, both as a processor and as a controller.
- **Impact assessments:** new or significantly changed processing, new uses of AI, new international transfers and anything involving children's data are assessed for a data protection impact assessment before going live. Where the employer is the controller, we give them the information they need for their own assessment.

4. Requests from individuals

- **Where we are the processor:** requests we receive directly are passed to the employer, normally within two working days. We help the employer find, export, correct, restrict or delete the data in time to meet its one-month deadline.

- **Where we are the controller:** we respond within one month, which can be extended by up to two further months for complex requests. We tell the person about any extension within the first month.
- We check the identity of anyone making a request before sharing any data, and every request is logged.
- Access to pay, health and benefit information is limited to authorised roles.

5. How long we keep data

Our standard retention periods for the Halo Benefits platform are set out below. Employers can set their own retention rules where these differ.

Data	How long we keep it
Employee, pay and dependant records	6 years after employment ends, then anonymised
Benefit elections and payroll history	6 years
Supporting evidence documents	6 years after the employee leaves, then deleted
Personal wellbeing and money areas	Deleted on request, or 90 days after the employee leaves
Sign-in security records	24 months
Audit history	For the life of the employer account, with personal details anonymised after erasure
System logs	30 days
Backups	Expire automatically within 37 days

6. Deletion and contract end

- Deletion and anonymisation requests are recorded and carried out through the platform. Where data must be kept for legal reasons, such as tax records or a legal claim, this is recorded explicitly.
- Backup copies expire within 37 days. If we ever restore from a backup, earlier deletion requests are reapplied before the service goes live.
- When a contract ends, customers have 30 days to export their data, and it is then returned or deleted within 90 days, unless otherwise agreed in the customer contract.

- Our suppliers must follow the deletion terms we agree with them.

7. Where data is stored

Our main customer records and files are stored in the EU (Frankfurt), and our application servers and backups are in the UK (London). Some services, such as website delivery, notifications and certain AI and voice features, may involve processing in other locations.

Any transfer of personal data outside the UK must be assessed, covered by an approved legal safeguard (such as UK adequacy regulations, the UK International Data Transfer Agreement or the UK Addendum to the EU Standard Contractual Clauses) and shown in our sub-processor list, which is available on request. Customers are given notice of new transfers.

8. Personal data breaches

Personal data breaches are handled under our Incident Response Plan:

- Where we are the processor, we tell the affected employer without undue delay.
- Where we are the controller, we tell the Information Commissioner's Office (ICO) within 72 hours of becoming aware of a reportable breach, and tell affected individuals without undue delay where there is a high risk to them.

9. Roles and responsibilities

- **Board of Directors:** is accountable for data protection compliance.
- **Head of Security & Operations:** owns this policy, our records of processing, the retention schedule and the sub-processor list, and is the contact for data protection requests and impact assessments.
- **External advisers:** we take legal or data protection advice where needed. Whether we need a formal Data Protection Officer is kept under review.
- **Everyone:** handles personal data only as their role requires, and passes on requests and suspected breaches immediately.

10. Compliance and exceptions

Compliance is shown through our records of processing, impact assessments, request log, deletion records and sub-processor list. Any breach of this policy may lead to disciplinary action or termination of contract.

Any departure from the retention schedule, such as a legal hold, must be approved by the Head of Security & Operations with a documented reason.

11. Review

This policy is reviewed annually, and sooner after any significant change, including changes in the law, ICO guidance, our suppliers or where data is stored. The Head of Security & Operations proposes changes and the Board of Directors approves them.

> QUESTIONS ABOUT THIS POLICY?
> Contact Alexander Dick, Head of Security & Operations, at security@halobenefits.co.uk.