DATA RETENTION POLICY

V1.1

The owner of this policy is the Chief Legal and Compliance Officer

VERSION	STAKEHOLDER	NAME	DATE	CONTENT
1.0	Author	V. Laffite	Nov. 15, 2025	
	Validation	D. Masson	Nov. 16, 2025	
1.1	Author	V. Laffite	May 21, 2026	
	Validation	D. Masson		

1. Introduction

Purpose

This data retention policy (the "Policy") sets out the required retention periods for specific categories of Personal Data and determines when certain data must be deleted within Goodweek.

Goodweek is responsible for this policy and the owner of that policy is David Masson, Chief Legal Officer (CLO).

Goodweek only uses Personal Data in strict compliance with privacy legislation and in particular Regulation 2016/679 (General Data Protection Regulation or abbreviated: "**GDPR**"), which entered into force on 25 May 2018.

Scope

This policy covers all personal data collected by Goodweek and stored in Goodweek technical platform, regardless of location. It applies to both data collected and held electronically (including photographs, video and audio recordings) and data that is collected and held as hard copy or paper files. The need to retain certain information may be mandated by federal or local law, federal regulations and legitimate business purposes, as well as the GDPR.

2. Defintions

For the purposes of this Policy, the following terms shall have the meanings set out below. Where not defined herein, terms shall have the meaning ascribed to them in Goodweek's Terms of Use, the applicable Data Processing Agreement, or applicable Data Protection Laws.

"Client Entity" means any organization that has entered into an agreement with Goodweek for the provision of the Solution, as further defined in Goodweek's Terms of Use.

"Data Controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data, as defined under applicable Data Protection Laws.

"Data Processor" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the Data Controller, as defined under applicable Data Protection Laws.

"Data Protection Laws" means all applicable laws and regulations relating to the processing of personal data, including without limitation the GDPR and any corresponding national implementing legislation, and applicable US federal and state privacy laws.

"End User" means any individual who accesses and uses the Solution under the authorization of a Client Entity, including administrators, managers, and other designated users.

"Personal Data" has the meaning given to that term under applicable Data Protection Laws.

"Solution" means the multimodal AI management platform developed and operated by Goodweek, as described in Goodweek's Terms of Use and further detailed at www.goodweek.com.

"Retention Period" means the period during which Goodweek retains a specific category of data, as set out in the Reference Table of this Policy.

3. Data Retention Regulations

Retention periods

Goodweek determines the retention periods of documents and data in accordance with applicable laws.

If a certain category of documents is not specifically mentioned in the “Reference table” below, the retention period for such category of documents shall be 1 year from the date of creation/receipt of this document, unless a longer period is required due to applicable legislation.

The retention periods in the “Reference table” may exceptionally be extended in the following cases:

- Ongoing audit by the Data Protection Authority if there is a chance that the personal data is necessary to demonstrate that Goodweek is acting in accordance with legal requirements,
- In case of court proceedings or similar procedures.

In such cases, written consent by the CLO is required.

Data retention safeguards

Goodweek ensures the following guarantees during data retention periods:

- Data will be retained in accordance with applicable legal principles and retention periods
- Only the necessary data will be kept
- The retained data will be regularly and systematically deleted in accordance with this Policy
- Data will be retained securely and the retained data is easy to identify
- Data will only be retained after the retention period specified in the section “Reference table” if this is justified.

Data destruction/deletion

Data will not be retained longer than necessary and shall be deleted in accordance with the periods specified in the section “Reference table”.

This Policy protects Goodweek and minimizes the risk of a breach of applicable data protection legislation. Goodweek will therefore regularly review all data, both electronic data and original documents to decide whether this data will be destroyed or deleted once the purpose for which these data/documents have been created or received is no longer relevant.

The deletion of data before or after the retention period has expired is subject to prior written consent of the CLO.

Goodweek applies the following approach to data:

- The original data is destroyed by fragmentation; and/or
- Electronic data is destroyed by permanent deletion of such data in electronic form.

Goodweek will execute this destruction and will assume the responsibilities in relation to the appropriate destruction of data. All applicable general provisions of GDPR and local law must be observed.

Interaction with data subject rights requests

The retention periods set out in this Policy do not affect Goodweek's obligations to respond to requests from data subjects exercising their rights under applicable Data Protection Laws, including the right to erasure (GDPR, Art. 17), the right to restriction of processing (GDPR, Art. 18), and the right to data portability (GDPR, Art. 20).

Where a data subject submits a valid erasure request in respect of data that is still within its applicable retention period, Goodweek shall assess whether a legal ground for continued retention applies (including compliance with a legal obligation or the establishment, exercise or defence of legal claims). Where no such ground applies, Goodweek shall proceed with early deletion, subject to the prior written consent of the CLO as required under this Policy.

Goodweek

Data subject rights requests shall be handled in accordance with the workflows maintained by the Legal & Compliance team, as further described in Goodweek's Privacy Policy and the applicable Data Processing Agreement

Operational responsibilities for deletion

To ensure that data is deleted in accordance with the retention periods set out in this Policy, the following responsibilities are assigned:

Category of Data	Responsible Owner	Deletion Mechanism
Platform & user account data	Engineering team, on instruction from Legal & Compliance	Automated deletion triggered upon contract termination or account deactivation; manual review where automated process is not available
Content & AI interaction data (prompts, outputs, uploaded documents)	Engineering team, on instruction from the Client Entity or Legal & Compliance	Automated deletion upon contract termination; manual deletion upon written request from the Client Entity
Activity logs and authentication data	Engineering team	Automated deletion after the applicable retention period
HR and payroll data	HR team	Manual review and deletion, documented in the HR system
Commercial and contractual data	Legal & Compliance team	Manual review and deletion, documented in the contract management system
Billing and accounting data	Finance team	Manual review and deletion, in accordance with applicable statutory obligations

The deletion of any data must be documented. The responsible owner shall maintain a record of deletions carried out, including the date, category of data, and method of destruction, and shall make such records available to the CLO upon request.

Any deletion carried out before or after the applicable retention period has expired requires the prior written consent of the CLO.

Infringement

Any breach of this Policy must be reported to the CLO.

4. Reference Table for Data Retention Policy

In this section, Goodweek determines the retention periods of the documents and electronic data in accordance with the applicable legislation.

4.1. Client / End-User Data of the Solution

Preliminary note on Goodweek's role

In connection with the provision of the Solution to Client Entities, Goodweek acts exclusively as a data processor within the meaning of applicable Data Protection Laws, including the GDPR. The Client Entity, as data controller, determines the purposes and means of processing of all personal data processed through the Solution, including user account data, activity logs, and content data. Goodweek processes such data solely on the documented instructions of the Client Entity, in accordance with the applicable Data Processing Agreement (DPA).

The retention periods set out below therefore represent maximum default periods applicable in the absence of specific instructions from the Client Entity. Where the Client Entity provides specific retention instructions under the DPA, those instructions shall prevail, provided they are consistent with applicable law.

Goodweek shall delete or return all personal data processed on behalf of a Client Entity upon termination or expiration of the applicable agreement, in accordance with the Client DPA.

Category 1 — Platform & User Account Data

(*Personal data of end users accessing the Solution — processed by Goodweek as data processor on behalf of the Client Entity)*

This data relates to the individuals who access the platform (administrators, managers, and end users) as designated and provisioned by the Client Entity.

Category of Data	Practical Examples	Default Retention Period
User account identification data	First name, last name, professional email address, login identifier	Duration of the contractual relationship with the Client Entity. Deletion within 30 days following the end of the contract or deactivation of the account, upon the Client's written request
Role and permission data	User role profile (admin, user, reader), assigned access rights	Duration of the contractual relationship with the Client Entity. Deletion within 30 days following termination
Login and authentication data	Login events, MFA authentication records, failed access attempts	1 year from the date of collection
Application activity logs (platform usage)	API calls, user actions within the Solution, feature usage events	1 year from the date of collection
Support and communication dat	Support tickets and exchanges with the Goodweek support team relating to the Client's use of the Solution	3 years from the date of last contact, or until the end of the contract if earlier
Billing and subscription data	Payment information, subscription history, invoices	10 years from the end of the contract (processed by Goodweek as data controller for its own billing purposes — statutory accounting obligation)

Note on billing data: to the extent that billing and subscription data is processed by Goodweek for its own contractual and accounting purposes (and not solely on the Client Entity's instructions), Goodweek acts as an independent data

controller for that specific processing activity, in accordance with relevant DPAs in place and applicable law.

Category 2 — Solution Usage Data — Content & AI Interactions

(Data generated by end users in the course of using the Solution — processed by Goodweek exclusively as data processor on behalf of the Client Entity)

This data is generated by end users in the course of their active use of the platform. It may contain personal data but does not necessarily do so. The Client Entity, as data controller, is responsible for determining the lawfulness of the processing and for providing end users with appropriate information (in addition to Goodweek's privacy policy approved upon onboarding).

Goodweek has no visibility over the nature or sensitivity of the content processed through the Solution. It is the Client Entity's responsibility to ensure that end users do not submit special category data or data whose processing would require specific safeguards, unless expressly agreed in the applicable Client DPA.

Category of Data	Practical Examples	Default Retention Period
Prompt content and user requests	Text entered by users in the Solution interfaces, instructions submitted to AI models through the Solution	Duration of the contract with the Client Entity. Deletion within 30 days following the end of the contract or upon the Client's written request, unless otherwise required by applicable law
Documents uploaded by users	PDF, Word, image or other files imported into the Solution for processing purposes	Duration of the contract with the Client Entity. Deletion within 30 days following the end of the contract or upon the Client's written request
Solution-generated content (AI outputs)	Responses, summaries, documents produced by AI models from user requests	Duration of the contract with the Client Entity. Deletion within 30 days following the end of the contract or upon the Client's written request
Conversation histories and work threads	Discussion threads, interaction histories with AI agents	Duration of the contract with the Client Entity. Deletion within 30 days following the end of the contract or upon the Client's written request
Solution configuration data	Deployment settings, agent configuration, integrations activated by the Client	Duration of the contract + 1 year to allow for potential post-contractual claims, unless the Client requests earlier deletion

Category 3 — Aggregated and Anonymized Usage Data

(Data processed by Goodweek as data controller for platform improvement purposes — no longer constitutes personal data)

Where Goodweek generates usage statistics or performance metrics that are irreversibly anonymized and cannot be re-linked to any individual or Client Entity, such data is no longer subject to Data Protection Laws and may be retained by Goodweek for its own purposes.

Category of Data	Practical Examples	Retention Period
Aggregated and anonymised usage data	Feature usage statistics, request volumes, performance metrics — provided they are irreversibly anonymised	No limitation — retained for as long as necessary for Goodweek's legitimate business, product improvement, and analytics purposes

Goodweek commits not to attempt to re-identify anonymised data. Any data that cannot be confirmed as irreversibly anonymised shall be treated as personal data and subject to the retention rules applicable to Category 2 above.

Residual rule

In the absence of instructions from the Client Entity and in the absence of any activity for 12 consecutive months, Goodweek will proceed with the deletion of all content and user data in accordance with Article 11 of the Client DPA, unless retention is required by applicable law.

Any exception to the above retention periods requires the prior written consent of the CLO/COO**.**

4.2. Technical Data & Logs

Category of Data	Practical Examples	Retention Period
Authentication and authorisation logs	Login events, MFA authentication records, failed access attempts, session tokens	90 days in readily accessible storage + up to 12 months in archived storage
Privileged and administrative activity logs	Admin actions, configuration changes, access rights modifications, cloud console activity	90 days in readily accessible storage + up to 12 months in archived storage
Security and incident logs	Alerts, anomalous activity events, security configuration changes	90 days in readily accessible storage + up to 12 months in archived storage; may be extended in the event of an ongoing security incident or regulatory investigation, subject to prior written consent of the CLO
Application activity logs (platform usage)	API calls, user actions within the Solution, feature usage events	1 year from the date of collection
IP addresses	IP addresses collected in connection with platform access and usage	1 year from the date of last collection
Error and performance logs	System errors, performance monitoring events, crash reports	90 days, unless retention beyond this period is required for an ongoing incident investigation

4.3. Goodweek Human resource administration

Category of Data	Retention Period
General: Reports and records containing personal data supporting the HR function	5 years after termination of the employment agreement
Employment agreements (general)	5 years after the termination of employment agreements
Student employment agreements	5 years after the termination of the student employment agreement
Health and Safety: Forms work accidents / Work accident card	10 years
Files following a request for formal intervention in relation to psychosocial risks	20 years from the date of the submission of the application
Payroll: Records related to employee salary, compensation, timekeeping, overtime, bonuses, expenses, tax records	5 years from the annual closing of the employee's individual account
Pay slips	5 years from the annual closing of the employee's individual account
Personnel files for interns	5 years from the annual closing of the employee's individual account
Recruitment records	5 years after recruitment
Training records	5 years from the annual closing of the employee's individual account
HR Database	5 years after termination of the employment agreement
Register with deviations for part-time workers	5 years from the date of the last entry until the end of the month following the quarter
Follow-up in the case of variable work schedules	5 years after the end of the date to which the data relate
Records regarding supplementary pensions	Up to 5 years after the employee's retirement
Legal benefits (long-term illness, maternity, insurance, sickness & disability)	5 years from the annual closing of the employee's individual account

4.4. Marketing and customer relations

Category of Data	Retention Period
Direct marketing: Personal data with explicit opt-in consent	During the period direct marketing is carried out. Immediate deletion upon consent withdrawal.
Customer survey data	For the duration of the customer relationship
Customer profiling	For the duration of the customer relationship, with express consent
Recording of electronic communications in the context of business transactions	10 years after the collection of the data

Contract management with customers (contractual documents, invoices, etc.)	10 years after the contract termination
IP address	1 year from the last collection of the data
Phone number	5 years from the last collection of data
Cookie _ga (Google Analytics - user distinction)	2 years
Cookie _ga_Q892VY5ZCZ (Google Analytics - session tracking GA4)	2 years

4.5. Administrative documents

Category of Data	Retention Period
Archives: Records of fiscal, administrative, legal or historical value	5 years after creation of the record
Tax related documents	7 years after creation of the record
Correspondence – General	10 years after the correspondence
Regulatory compliance documents	10 years
Documents relating to customs	3 years
Register of waste	5 years
Documents relating to anti-money laundering duties	10 years

4.6. Commercial

Category of Data	Retention Period
Contracts and agreements (general business purposes)	5 years after the termination of the contract
Contracts and agreements regarding the sale and acquisition of products	7 years after the effective date of the sale/purchase

4.7. Insurance

Category of Data	Retention Period
Company insurance (employer's liability, accident policies, professional indemnity, claims files)	10 years after termination of the contract
Group health policies	10 years
Group personal accident policies	10 years
Claims correspondence	10 years after settlement

4.8. Litigation records

Category of Data	Retention Period
Litigation case records	As long as the proceedings are ongoing, including possible periods for Appeals
Litigation regarding real estate	30 years

4.9. Banking / Accounting records

Category of Data	Retention Period
Annual reports and accounts	Permanently
Accounts and payroll (invoices, cash receipts, cheques, etc.)	7 years from 1 January after the end of the financial year
VAT records	10 years from 1 January after the end of the financial year
VAT on immovable property / rights in rem	15 years from 1 January after the end of the financial year
Banking records (statements, instructions, etc.)	7 years

4.10. Property records

Category of Data	Retention Period
Contracts regarding acquisition or transfer of real estate and land	30 years after the contract was concluded
Deeds of title	Until sold/transferred and at least 5 years after the closing of the liquidation of the company
Leases	5–10 years
Agreements relating to premises	10 years