PRIVACY

Data Processing Agreement

With annexes: the processing, sub-processors and security

Lean AI Coach B.V. · November 2026
Version 1.0



This data processing agreement applies to every subscription to leanaicoach.com and forms part of the terms and conditions. It sets out how Lean AI Coach B.V. processes your organisation's personal data, as required by Article 28 of the GDPR.

Parties

1. The organisation that takes out a subscription to Lean AI Coach, hereinafter: **Controller**;
2. Lean AI Coach B.V., Rauwbrakenweg 7, 5056 EJ Berkel-Enschot, the Netherlands, registered with the Chamber of Commerce under number 42193574, hereinafter: **Processor**;

together: **Parties**.

Recitals

- Controller uses the product leanaicoach.com (hereinafter: Lean AI Coach or the Service) under a subscription (hereinafter: the Main Agreement).
- In providing the Service, Processor processes personal data on behalf of Controller.
- In this agreement the Parties record their arrangements on this, as required by Article 28(3) of the General Data Protection Regulation (GDPR).

1 Definitions

Terms such as personal data, processing, data subject, controller, processor and personal data breach have the meaning given to them in the GDPR. A **Sub-processor** is a third party engaged by Processor to process personal data on behalf of Controller.

2 Subject matter and instructions

1. Processor processes personal data only to provide the Service, as described in Annex 1, and in accordance with Controller's written instructions. The Main Agreement, this agreement and the settings Controller chooses in the Service count as instructions.
2. Processor does not use the personal data for its own purposes. Processor does not use the data to train AI models and does not let Sub-processors do so.
3. If Processor considers that an instruction infringes the GDPR or other legislation, it informs Controller immediately.
4. Controller warrants that it processes the personal data lawfully and is entitled to provide it to Processor.

3 Confidentiality

Processor keeps the personal data confidential. Only persons who need the data to provide the Service have access, and they are bound by confidentiality.

4 Security

1. Processor takes appropriate technical and organisational measures to protect the personal data. The measures are set out in Annex 3.
2. Processor may adjust the measures, provided the level of security does not decrease.

5 Sub-processors

1. Controller gives general authorisation for the engagement of Sub-processors. The Sub-processors at the time this agreement is entered into are listed in Annex 2.
2. Processor notifies a new or replacement Sub-processor at least 30 days in advance. Within that period Controller may object in writing, stating its reasons. If the Parties cannot reach agreement, Controller may terminate the Main Agreement as of the date the change takes effect.
3. Processor imposes obligations on each Sub-processor that are at least equivalent to those in this agreement, and remains responsible towards Controller for its Sub-processors.

6 Processing within the European Economic Area

1. Processor processes the personal data within the European Economic Area (EEA).
2. Transfers to a country outside the EEA only take place if a valid basis under Chapter V of the GDPR exists, and after notification in accordance with Article 5(2). Sub-processors with a parent company outside the EEA are bound by the standard contractual clauses of the European Commission.

7 Assistance

1. Processor assists Controller, as far as reasonable, with requests from data subjects (access, rectification, erasure, portability, objection). If Processor receives such a request itself, it forwards it and does not respond to its substance.
2. Processor assists Controller, as far as reasonable, with a data protection impact assessment and with prior consultation of the supervisory authority.
3. Controller can handle most requests itself using the functions of the Service, including the export.

8 Personal data breach

1. Processor notifies Controller of a breach without undue delay, and no later than 48 hours after discovering it.
2. The notification contains, as far as known: what happened, which data and how many data subjects are involved, the likely consequences and the measures taken or to be taken. Missing information follows as soon as it is available.
3. Controller assesses whether to notify the supervisory authority and the data subjects. Processor does not make those notifications itself.
4. Processor sends the notification to the contact person Controller has specified in the Service.

9 Audit

1. On request, Processor provides the information needed to demonstrate that it complies with this agreement.
2. Controller may have compliance audited by an independent expert bound by confidentiality no more than once a year, and more often in case of a concrete suspicion of a breach. It announces the audit at least 30 days in advance. The audit disrupts the service as little as possible and gives no access to data of other customers.

3 Each party bears its own costs of an audit. If the audit reveals a material shortcoming on the part of Processor, Processor bears the reasonable costs of the expert.

10 Duration, return and deletion

1 This agreement applies for as long as Processor processes personal data on behalf of Controller.

2 Controller can export its data at any time, and up to 30 days after the end of the Main Agreement.

3 90 days after the end of the Main Agreement, Processor deletes the personal data. Until then, Processor keeps it restricted and does not use it.

4 At Controller's written request, Processor deletes the personal data sooner, within 30 days of the request.

5 Backups are deleted no later than 30 days after they are made. Data removed from the Service has therefore also disappeared from the backups no later than 30 days later.

6 The above does not apply to data Processor is required by law to keep longer, such as payment records.

11 Liability

The limitation of liability in the Main Agreement (article 13 of the terms and conditions) also applies to this agreement. This does not affect the rights of data subjects under Article 82 GDPR.

12 Final provisions

1 In case of conflict between this agreement and the Main Agreement, this agreement prevails as far as the processing of personal data is concerned.

2 Processor may transfer this agreement to a legal successor or group company that continues the Service, and notifies this in advance.

3 Processor may adjust the annexes if the Service changes. Article 5 applies to Sub-processors.

4 This agreement is governed by Dutch law. Disputes are submitted to the court designated in the Main Agreement.

5 This agreement is drawn up in English. A translation is provided for information only; in case of differences the English text prevails.

Annex 1 The processing

Item	Description
Subject matter and purpose	Providing Lean AI Coach: a platform for continuous improvement (A3, Kaizen, 5S, VSM, Gemba walks, goals and dashboards) with an AI coach that supports users
Nature of the processing	Storing, organising, displaying, translating, processing by the AI, backing up, exporting and deleting
Duration	The term of the Main Agreement, plus the periods in Article 10
Data subjects	Controller's users (power users, practitioners, viewers); employees and other persons named or visible in projects, documents or photos
Categories of personal data	Name, business email address, role, location and department, language preference; login and usage data; what users enter themselves in projects, chats with the AI coach, uploaded documents and photos
Special categories of personal data	The Service is not intended for them. Controller ensures that users do not enter special categories of personal data (such as health data) or criminal data
Processor contact	privacy: info@leanaicoach.com

Annex 2 Sub-processors

Sub-processor	What	Where	Safeguard
Amazon Web Services EMEA SARL (Luxembourg)	Storage of uploaded documents and backups (S3); sending email (SES)	EU, Stockholm region (eu-north-1)	AWS data processing agreement (GDPR Data Processing Addendum), part of the AWS Service Terms
Microsoft Ireland Operations Limited (Ireland)	AI models via Azure OpenAI	EU Data Zone	Microsoft data processing agreement (DPA); input is not sent to OpenAI and is not used for training

Only if the user chooses to

Party	What	Data
Google or Microsoft (sign-in)	Signing in with an existing Google or Microsoft account	Name and email address of the person signing in
Microsoft Bookings	Scheduling an appointment after subscribing	What the user enters in the booking window

No sub-processing

- The database, the privacy filter and the log files run on a dedicated server of Processor in the Netherlands. Only Processor's management has access.
- The payment provider Stripe processes the order and invoice data (email address of the purchaser, chosen plan, number of seats) for Processor's administration. Processor is the controller for this. User names are not sent to Stripe.
- Visitor statistics (Google Analytics) run only on the public website, after consent, and not in the Service.

Annex 3 Security measures

Access and separation

- Each organisation's data is separated from that of other customers: every query is filtered by organisation, and this is checked with automated tests.
- Within an organisation, the customer sets each user's role, location and department.
- Users can sign in with a Google or Microsoft account; the two-step verification of their own organisation then also applies to the Service. An organisation can require one sign-in method for all its users.
- Passwords have at least 12 characters; the number of sign-in attempts is limited. Sign-in attempts and administrative actions are logged in the Service.
- Access to the server: only Processor's management, through an encrypted connection with a key. Access to storage at AWS: only Processor's account, with two-step verification.

Connections and storage

- All traffic between user and Service is encrypted (HTTPS, TLS 1.2 or higher).
- The database cannot be reached from outside the server.
- Uploaded documents and backups are stored encrypted at AWS (AES-256) and are not publicly accessible.

AI

- Every AI request first passes through a privacy filter that removes names, phone numbers and email addresses. If the filter is unavailable, the request is blocked.
- Documents pass through the same filter as text. Photos are not sent to the AI.

Backup and recovery

- Backups four times a day, kept locally for 7 days and stored encrypted at AWS, where they are deleted after 30 days.
- Each new version is tested before release in a production acceptance environment with a copy of the production data; this also tests recovery from backup. That environment runs on the same server and is subject to the same measures and the same access restrictions.

Retention periods in the Service

- Conversations with the AI coach: 180 days. AI usage log and privacy filter log: 365 days. Administrative actions log: 90 days.