Privacy Notice

Published 2026-02-24

Purpose statement: This Privacy Notice explains how LatentWorlds AI B.V. collects and uses personal data through our website, our communications, and our products and services (including DataCore).

Document status: Public
Version: 1.0
Effective date: 2026-02-24
Owner (top management): Cristian Meo, Cofounder & CEO
Website publication location: https://www.latentworlds.ai/policies/privacy-notice
Contact: policy@latentworlds.ai

1. Controller and scope

This Privacy Notice applies to personal data processed by **LatentWorlds AI B.V.** (“LatentWorlds”, “we”, “us”) through:

- our website at https://www.latentworlds.ai and associated pages;
- our communications with customers, partners, and prospective customers (including pilot requests);
- recruiting activities; and
- the DataCore platform and related services (the “Services”).

Controller details. LatentWorlds AI B.V., Molengraaffsingel 12, 2629JD Delft, the Netherlands. KvK: 97470163.

How this notice interacts with customer deployments. When we provide the Services to a business customer and process personal data on the customer’s behalf, that customer is typically the **controller** and LatentWorlds is a **processor**. In those cases, the customer’s privacy notice governs the collection of personal data, and our processing is governed by our Data Processing Addendum and the customer contract.

2. Categories of personal data we process

2.1 Website and communications

Depending on how you interact with us, we process:

- **Contact details:** name, work email, company, job title, phone number (if provided).
- **Inquiry content:** information you include in messages, pilot notes, or forms.
- **Technical and usage data:** IP address, device and browser information, approximate location derived from IP address, pages viewed, and general interaction logs.

2.2 Recruiting

If you apply for a role, we process:

- CV/resume, employment and education history, links to public work (e.g., GitHub), and application correspondence;
- interview notes and evaluation feedback; and
- reference details if you choose to provide them or if we request them with your consent.

2.3 DataCore Services

When we operate DataCore for a customer, we may process:

- **Account and access data:** names, work emails, user IDs, authentication and authorization data, and audit logs tied to user actions.
- **Customer Content:** data that customers ingest into the Services, which may include sensor streams, logs, images, video, audio, and annotations. Customer Content can include personal data depending on the customer’s use case (for example, voices, faces, or identifiers in logs).

We do not intentionally collect special category data (such as health data) through our website. For the Services, customers control what they ingest; customers should avoid ingesting special category data unless they have a lawful basis and have agreed appropriate safeguards with us.

3. Purposes and legal bases

We process personal data for the following purposes and legal bases (under GDPR where applicable):

- **Operate and secure the website and Services** (legitimate interests in running a secure business and providing a stable product; and performance of a contract for customer users).
- **Respond to inquiries and pilot requests** (legitimate interests; and steps prior to entering a contract).
- **Provide the Services to customers** (performance of a contract; and processor obligations under customer instructions).
- **Improve our product and operations** (legitimate interests). This includes reliability metrics, usage patterns, and aggregated performance data. Where feasible, we use aggregated or de-identified data for analytics and product improvement.
- **Recruiting and hiring** (legitimate interests; and steps prior to entering an employment contract).
- **Compliance and legal protection** (compliance with legal obligations; legitimate interests in enforcing agreements and protecting our rights).

If we rely on consent for any specific processing activity (for example, optional marketing emails where required), you can withdraw consent at any time by contacting us or using the unsubscribe mechanism in the message.

4. How we share personal data

We share personal data only as needed for the purposes above:

- **Service providers.** We use trusted third parties for infrastructure hosting, email and collaboration, customer relationship management, security monitoring, and other business operations. They are bound by confidentiality and data protection obligations.
- **Customers and end users.** If you are an authorized user of a customer deployment, we may share account and audit information with the customer administrators as part of normal operation.
- **Legal and safety.** We may disclose information if required by law or to protect rights, safety, and security, including to respond to lawful requests.

We do not sell personal data. We do not share personal data for cross-context behavioral advertising.

5. International data transfers

We are based in the Netherlands and may process data in other countries where we or our service providers operate. Where personal data is transferred outside the European Economic Area, we use appropriate safeguards such as the European Commission’s Standard Contractual Clauses and, where required, additional measures.

6. Security

We implement technical and organizational measures designed to protect personal data, including access controls, encryption in transit where supported, least-privilege practices, and audit logging for sensitive operations. No method of transmission or storage is completely secure; however, we work continuously to improve our security posture.

7. Data retention

We retain personal data only as long as necessary for the purposes described in this notice:

- **Website inquiries and pilot communications:** typically up to 24 months after our last interaction, unless a longer retention is needed for contracting or legal reasons.
- **Recruiting:** typically up to 12 months after a role is closed, unless you consent to a longer retention.
- **Customer Services:** retention of Customer Content is controlled by the customer configuration and contract. After termination or a deletion request, we delete Customer Content and associated personal data in accordance with the contract and our deletion procedures, subject to limited backup retention.

We may retain certain records longer where required by law (for example, accounting records) or where necessary to establish, exercise, or defend legal claims.

8. Your rights

Where GDPR (or other applicable law) applies, you may have rights to:

- access your personal data;
- correct inaccurate data;
- delete data;
- restrict or object to certain processing;
- receive a copy of your data (data portability) where applicable; and
- lodge a complaint with a supervisory authority.

If we process your personal data as a processor for a customer, please direct requests to the customer (the controller). We will support the customer in responding to requests as required by our contracts and applicable law.

9. Children

Our website and Services are not directed to children, and we do not knowingly collect personal data from children.

10. Changes to this notice

We may update this Privacy Notice from time to time. We will publish the updated version on our website and update the effective date.

11. Adoption and signature

By signing this document, top management adopts this Privacy Notice for publication and use.

Adopted on: 2026-02-24

Cristian Meo
Cofounder & CEO, LatentWorlds AI

Signature: