Data Processing Addendum (DPA)

Published 2026-02-24

Purpose statement: This Data Processing Addendum describes the data protection terms that apply when LatentWorlds AI B.V. processes personal data on behalf of a customer in connection with the DataCore Services.

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/data-processing-addendum
Contact: policy@latentworlds.ai

1. Scope and order of precedence

This Data Processing Addendum ("DPA") applies when LatentWorlds AI B.V. ("Processor") processes personal data on behalf of a customer ("Customer", acting as controller) in connection with the DataCore Services.

This DPA forms part of, and is incorporated into, the agreement governing the Customer's use of the Services (the "Agreement"). In the event of conflict between this DPA and the Agreement regarding data protection, this DPA controls.

2. Definitions

Terms such as **personal data**, **processing**, **controller**, **processor**, and **supervisory authority** have the meanings given in the GDPR.

"**Customer Personal Data**" means personal data contained in Customer Content or otherwise processed by Processor on Customer's behalf through the Services.

"**Subprocessor**" means any processor engaged by Processor to process Customer Personal Data.

3. Processing details

The subject matter, duration, nature, and purpose of the processing, and the types of personal data and categories of data subjects are described in **Appendix A**.

4. Processor obligations

Processor will:

- process Customer Personal Data only on documented instructions from Customer, including with respect to transfers of personal data to a third country, unless required by applicable law;
- ensure that persons authorized to process Customer Personal Data are bound by confidentiality;
- implement appropriate technical and organizational measures to protect Customer Personal Data, as described in **Appendix B**;
- respect the conditions for engaging subprocessors set out in Section 6;
- assist Customer in responding to data subject requests and in meeting Customer's obligations under GDPR Articles 32–36, taking into account the nature of processing and information available to Processor; and
- at Customer's choice, delete or return Customer Personal Data at the end of the provision of Services, as described in Section 10.

5. Security measures

Processor maintains a security program designed to protect Customer Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access. Measures include, as appropriate to the deployment model: access controls, encryption in transit where supported, environment isolation, audit logging, and vulnerability management practices.

Customer is responsible for configuring the Services appropriately, including setting retention rules, managing user access, and maintaining secure credentials for its users.

6. Subprocessing

Customer provides a general authorization for Processor to engage subprocessors to process Customer Personal Data for the purpose of providing the Services.

Processor will:

- impose data protection obligations on subprocessors that are no less protective than those in this DPA; and
- remain responsible for the performance of its subprocessors' obligations.

Processor maintains a current list of subprocessors used for the Services and will make it available to Customer on request. Processor will provide reasonable advance notice of material changes to subprocessors used to process Customer Personal Data, and Customer may object to a new subprocessor on reasonable data protection grounds. If the parties cannot resolve the objection, Customer may terminate the affected Services by providing written notice.

7. Assistance with data subject requests

Taking into account the nature of processing, Processor will provide reasonable assistance to Customer to enable Customer to respond to requests from data subjects to exercise their rights under applicable data protection law. If Processor receives a request directly from a data subject relating to Customer Personal Data, Processor will, to the extent legally permitted, direct the data subject to Customer and notify Customer.

8. Personal data breach notification

Processor will notify Customer without undue delay after becoming aware of a personal data breach affecting Customer Personal Data and will provide information reasonably required to assist Customer in meeting breach notification obligations.

9. Audits and compliance

Processor will make available information reasonably necessary to demonstrate compliance with this DPA and will allow for and contribute to audits conducted by Customer or an auditor mandated by Customer, subject to:

- reasonable advance notice;
- a limit of one audit per 12-month period, unless a personal data breach or substantiated security issue requires more; and
- reasonable confidentiality and security requirements.

Audits must not unreasonably interfere with Processor's business operations. Customer bears its own audit costs and reimburses Processor's reasonable costs for supporting an audit.

10. Deletion and return

Upon termination or expiration of the Agreement, Processor will, at Customer's choice, delete or return Customer Personal Data and delete existing copies, unless applicable law requires retention. Deletion from backups occurs as backups expire, consistent with Processor's backup retention practices.

11. International transfers

If Customer Personal Data is transferred from the EEA to a country that has not been recognized as providing an adequate level of protection, the parties will rely on appropriate safeguards.

Where the European Commission's Standard Contractual Clauses ("SCCs") are required, the parties agree that:

- the SCCs adopted by the European Commission under Implementing Decision (EU) 2021/914 apply and are incorporated by reference; and
- for transfers where Customer is a controller and Processor is a processor, Module Two (Controller to Processor) applies; for transfers where Customer is a processor and Processor is a subprocessor, Module Three (Processor to Processor) applies.

If there is conflict between the SCCs and this DPA, the SCCs prevail for the scope of the transfer.

12. Limitation

Nothing in this DPA reduces Processor's obligations under applicable data protection law. Customer acknowledges that the Services are designed primarily for business use, and Customer is responsible for determining whether and how to ingest personal data into the Services consistent with applicable law.

13. Adoption and signature

By signing this document, top management adopts this Data Processing Addendum for publication and use as a standard addendum to customer agreements.

Adopted on: 2026-02-24

Cristian Meo
Cofounder & CEO, LatentWorlds AI

Signature:

Appendix A — Description of processing

Subject matter: Provision of the DataCore Services, including ingestion, storage, indexing, processing, and retrieval of Customer Content; creation of derived artifacts such as synchronized slices and dataset versions; and operation of access controls, audit logs, and platform administration.

Duration: For the term of the Agreement and any additional period required for deletion and backup expiry.

Nature and purpose of processing: Hosting and processing Customer Content and related metadata to provide the Services, including enabling customers to search, retrieve, export, and manage robotics data and operational workflows.

Categories of data subjects: Customer personnel and contractors; end users authorized by Customer; and individuals whose personal data may be captured in Customer Content (for example, people appearing in video or audio, or identifiers in logs).

Types of personal data: Account identifiers (name, email, user ID); authentication and authorization data; audit logs tied to user actions; and personal data that may be included in Customer Content (which may include images, video, audio, or identifiers depending on Customer's use case).

Special categories of data: Not intended. Customer should avoid ingesting special category data unless appropriate lawful basis and safeguards are in place and agreed.

Appendix B — Technical and organizational measures (summary)

Processor maintains measures appropriate to risk and the deployment model, including:

- access control and authentication for administrative functions;
- logical isolation between customer projects/tenants where applicable;
- encryption in transit where supported;
- logging of administrative and sensitive actions;
- secure software development practices (code review and dependency hygiene);
- vulnerability management and incident response procedures; and
- backup and disaster recovery practices designed for data integrity and availability.