

# Data Protection Agreement — France / EU

PUBLISHED AT [GLOBALML.COM/DPA-EU](https://globalml.com/dpa-eu). VERSION 2.0.

This Data Protection Agreement (the “DPA”) is published by GlobalML and forms part of the Software License & Acquisition Agreement between GlobalML and the Vendor (the “Main Agreement”) through the reference to it in that agreement. It applies where the Main Agreement selects France (Paris) as the governing law. By entering into the Main Agreement, the Vendor and GlobalML agree to this DPA; it is not separately negotiated or signed. The parties, the effective date, and the governing law and competent court are those of the Main Agreement. This DPA governs GlobalML’s processing of personal data contained in the Vendor’s Assets.

---

## TERMS

### 1. Roles

For the personal data in the Assets, the Vendor and GlobalML are separate, independent controllers under the GDPR — not controller and processor, and not joint controllers. Each determines the purposes and means of its own processing and is separately responsible for its own compliance. Words defined in the GDPR — such as controller, personal data, processing, special categories of personal data, and personal data breach — have the same meaning here.

### 2. GlobalML’s purpose

GlobalML processes the personal data only to remove or redact it from the Assets, using a documented process designed to detect and remove it so that the Assets it delivers are not intended to contain personal data, and for no other purpose. GlobalML does not use the personal data to train or develop AI or ML models, and does not disclose or use it outside that removal purpose. This restriction concerns the personal data only. It does not limit GlobalML’s rights to use the Assets once personal data has been removed — including to host, modify, train, develop, sell, or sublicense AI or ML models, environments, weights, and outputs from the cleared Assets — as set out in the Main Agreement.

### 3. Lawful basis and responsibilities

Each party is responsible for its own compliance with the GDPR and applicable data-protection law. The Vendor confirms that it is entitled to disclose the Assets and any personal data in them to GlobalML, and that it has a lawful basis and has met its own information obligations for that

disclosure. GlobalML is responsible for having a lawful basis for its own processing, which is limited to removing the personal data. Each party handles the data-subject requests it receives about its own processing; neither acts on the other's behalf.

#### **4. Duration and deletion**

GlobalML processes the personal data only for as long as needed to carry out the removal. It keeps the data in an isolated, access-controlled environment, accesses it only as far as needed, and deletes it as soon as the removal is complete, or returns it if the Vendor asks, confirming deletion in writing.

Deletion concerns the personal data itself. GlobalML may retain its records of processing and provenance logs evidencing how the personal data was received, handled, and removed, provided those records themselves contain no personal data. This preserves the auditable chain of provenance described in the Main Agreement while irreversibly destroying the underlying personal data.

#### **5. Confidentiality**

GlobalML ensures that the people it authorizes to process the personal data are bound by an appropriate duty of confidentiality.

#### **6. Security**

GlobalML applies appropriate technical and organizational measures to protect the personal data against accidental or unlawful destruction, loss, alteration, or unauthorized disclosure or access, taking into account the risk. The measures are set out in Annex 2.

#### **7. Other processors**

GlobalML may engage its own processors to help with the removal, under a written contract imposing data-protection obligations at least as protective as this DPA, and remains responsible for them under Article 28 of the GDPR.

#### **8. Personal data breach**

Each party meets its own obligations under Articles 33 and 34 of the GDPR. GlobalML notifies the Vendor without undue delay after becoming aware of a personal data breach affecting the Vendor's personal data, and gives the Vendor the information and cooperation it reasonably needs.

#### **9. International transfers**

Where the Vendor's personal data is transferred from the EU or EEA to GlobalML in the United States, GlobalML relies on the EU-US Data Privacy Framework where it applies, or otherwise on the European Commission's Standard Contractual Clauses (controller-to-controller module —

Module One), which the Parties enter into and which are incorporated into this DPA, supported by a transfer impact assessment.

## 10. Records and provenance

On the Vendor's reasonable request, GlobalML makes available the provenance records described in the Main Agreement, giving the Vendor an auditable record of how the personal data was received and removed. This replaces, and is not in addition to, any separate data-protection audit right.

## 11. Liability and conflict

Liability under this DPA is subject to the limitations and exclusions in the Main Agreement, including its liability cap. The Main Agreement no longer carves the data-protection obligations out of that cap, so liability under this DPA is capped at the total amounts paid or payable to the Vendor under the Main Agreement. This cap does not limit either party's statutory liability to regulators or data subjects, which no agreement can cap. If this DPA and the Main Agreement conflict on the processing of personal data, this DPA prevails to the extent of the conflict.

## 12. Updates to this DPA

GlobalML may update this DPA from time to time. The version that applies to a Main Agreement is the one published at [globalml.com/dpa-eu](https://globalml.com/dpa-eu) when that agreement is signed, unless the Parties agree otherwise in writing or a change is required by law.

## 13. Governing law

This DPA is governed by French law, and any dispute falls under the jurisdiction of the court that applies under the Main Agreement (Paris).

---

# ANNEX 1. DETAILS OF THE PROCESSING

**Subject matter:** the removal or redaction of personal data from the Vendor's Assets under the Main Agreement.

**Duration:** from first access to the Assets until the personal data is deleted on completion of the removal.

**Nature and purpose:** accessing, scanning, redacting or removing, and then deleting personal data through a documented process, so the delivered Assets are not intended to contain personal data; no other use, and no use of the personal data to train AI.

**Types of personal data:** names, email addresses, usernames, and identifiers embedded in source code, commit history, configuration, documentation, and test data or fixtures, and any other personal data incidentally present. No special-category data is expected, and the Vendor

will flag any in advance. In any event, GlobalML's scanning is designed to detect and remove personal data, including special-category data, whether or not the Vendor flags it, so that detection does not depend solely on the Vendor's notice.

**Categories of data subjects:** the Vendor's developers, employees, and contractors, and any individuals whose personal data is incidentally embedded in the materials.

---

## **ANNEX 2. SECURITY MEASURES**

- Processing only in an isolated, access-controlled environment.
- Access on a least-privilege, need-to-know basis, with authentication.
- Encryption of personal data in transit and at rest.
- Logging of access to and actions on the personal data.
- No copies beyond what is needed for the removal.
- Secure, irreversible deletion of the personal data on completion.
- Personnel bound by confidentiality and given data-protection training.