

# Data Protection Agreement

PUBLISHED AT [GLOBALML.COM/DPA-US](https://globalml.com/dpa-us). 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 Delaware, USA 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 information contained in the Vendor’s Assets.

---

## TERMS

### 1. Roles

Each party is an independent controller of the personal information it processes — a “business” under the California Consumer Privacy Act (CCPA/CPRA) and the equivalent under other applicable US state privacy laws — and not the other’s service provider, contractor, or processor. Each determines the purposes and means of its own processing and is separately responsible for its own compliance. Terms such as personal information, business, sell, share, sensitive personal information, and consumer have the meaning given in the CCPA.

### 2. GlobalML’s purpose and use

GlobalML processes the personal information 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 information, and for no other purpose. GlobalML does not sell or share the personal information, does not use it to train or develop AI or ML models, and does not retain, use, or disclose it outside that removal purpose. This restriction concerns the personal information only. It does not limit GlobalML’s rights to use the Assets once personal information 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. No sale or sharing

The Parties intend that the Vendor’s disclosure of personal information to GlobalML, solely so that GlobalML can remove it from the Assets, is neither a “sale” nor a “share” of personal information: GlobalML obtains no value from the personal information itself and uses it only to

delete it.

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

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

#### **5. Each party's responsibilities**

Each party is responsible for its own compliance with applicable US state privacy laws. The Vendor confirms that it is entitled to disclose the Assets and any personal information in them to GlobalML, and that it has given any notices and met any obligations its own compliance requires. Each party handles the requests it receives from consumers about its own processing; neither is required to act on the other's behalf.

#### **6. Confidentiality and security**

GlobalML keeps the personal information confidential and ensures that the people it authorizes to process it are bound by an appropriate duty of confidentiality. GlobalML applies reasonable technical and organizational security measures appropriate to the risk to protect the personal information against unauthorized or unlawful access, use, disclosure, alteration, loss, or destruction. The measures are set out in Annex 2.

#### **7. Service providers**

GlobalML may engage its own service providers or contractors to help with the removal, under a written contract imposing data-protection obligations at least as protective as this DPA, and remains responsible for their compliance.

#### **8. Security incidents**

GlobalML notifies the Vendor without undue delay after becoming aware of a breach of security leading to the unauthorized access to or disclosure of the Vendor's personal information, and provides the information the Vendor reasonably needs. Each party is responsible for meeting its own notification obligations under applicable law.

#### **9. 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 information was received and removed. This replaces, and is not in addition to, any separate data-protection audit right.

## 10. 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 information, this DPA prevails to the extent of the conflict.

## 11. 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-us](https://globalml.com/dpa-us) when that agreement is signed, unless the Parties agree otherwise in writing or a change is required by law.

## 12. Governing law

This DPA is governed by the laws of the State of Delaware, and any dispute falls under the jurisdiction of the court that applies under the Main Agreement.

---

# ANNEX 1. DETAILS OF THE PROCESSING

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

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

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

**Types of personal information:** names, email addresses, usernames, and identifiers embedded in source code, commit history, configuration, documentation, and test data or fixtures, and any other personal information incidentally present. No sensitive personal information is expected, and the Vendor will flag any in advance. In any event, GlobalML's scanning is designed to detect and remove personal information, including sensitive personal information, whether or not the Vendor flags it, so that detection does not depend solely on the Vendor's

notice.

**Categories of consumers:** the Vendor's developers, employees, and contractors, and any individuals whose personal information 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 information in transit and at rest.
- Logging of access to and actions on the personal information.
- No copies beyond what is needed for the removal.
- Secure, irreversible deletion of the personal information on completion.
- Personnel bound by confidentiality and given data-protection training.