



Code Intelligence Platform

## **DATA PROCESSING AGREEMENT**

*GDPR & Privacy Law Compliance*

**Silicon Harbor Technologies, LLC**

Charleston, South Carolina

*Effective Date:* \_\_\_\_\_

# DATA PROCESSING AGREEMENT

*Last Updated: March 16, 2026*

This Data Processing Agreement ("DPA") governs the processing of personal data by Silicon Harbor Technologies, LLC ("Processor") on behalf of Customer ("Controller") in connection with Enovari services. This DPA is designed to ensure compliance with GDPR, CCPA, and other applicable privacy laws.

## 1. Definitions

---

- **"Controller"** means Customer, who determines the purposes and means of processing personal data.
- **"Processor"** means Silicon Harbor Technologies, LLC, which processes personal data on behalf of Controller.
- **"Personal Data"** means any information relating to an identified or identifiable natural person that may appear in code, comments, or logs uploaded to Enovari.
- **"Sub-processor"** means third-party service providers engaged by Processor to assist in processing (e.g., cloud hosting, AI providers).

## 2. Scope of Processing

---

### 2.1 Subject Matter & Duration

- **Subject Matter:** Real-time code intelligence and security analysis
- **Duration:** Duration of Master Services Agreement plus 30-day post-termination retention
- **Nature & Purpose:** Processing Customer-uploaded code for real-time analysis only (NO RETENTION)

### 2.2 Categories of Data Subjects

- Customer employees and contractors whose information may appear in code/comments
- End users whose data may be referenced in sample code or test data
- Third-party developers contributing to open-source projects

### 2.3 Types of Personal Data

- Developer names, email addresses, and usernames in code commits/comments
- IP addresses, session IDs, or identifiers in log files or test data
- Any PII inadvertently included in code strings, comments, or configuration files



### 3. Processor Obligations

---

Silicon Harbor agrees to:

- Process personal data only on documented instructions from Controller
- Ensure all personnel are bound by confidentiality obligations
- Implement appropriate technical and organizational security measures (Section 4)
- Process data in real-time only with NO retention beyond service delivery
- Assist Controller with data subject rights requests (access, deletion, portability)
- Notify Controller of data breaches within 24 hours of discovery
- Delete all personal data upon termination (unless legally required to retain)

### 4. Security Measures

---

#### 4.1 Technical Measures

- **Encryption:** TLS 1.3 in transit for all data transmission
- **Access Control:** Role-based access control (RBAC), multi-factor authentication (MFA)
- **Network Security:** Firewall protection, intrusion detection/prevention systems
- **Logging & Monitoring:** Comprehensive audit logs, anomaly detection, 24/7 monitoring
- **Zero Retention:** In-memory processing only, immediate purge after analysis

#### 4.2 Organizational Measures

- **Security Training:** Annual security awareness training for all personnel
- **Incident Response:** Documented incident response plan, 24-hour breach notification
- **Vendor Management:** Security assessments of all sub-processors

## 5. Sub-processors

---

Controller authorizes Processor to engage the following categories of sub-processors:

- **Cloud Infrastructure:** AWS, Google Cloud Platform, Microsoft Azure (as needed)
- **AI Service Providers:** Anthropic, OpenAI, or other AI providers (with zero-retention agreements)
- **Analytics & Monitoring:** Performance monitoring services (anonymized data only)

*Processor will provide 30 days' notice before engaging new sub-processors. Controller may object within 15 days on reasonable privacy grounds.*

## 6. International Data Transfers

---

Silicon Harbor may transfer personal data outside the European Economic Area (EEA). For such transfers, Processor implements appropriate safeguards:

- Standard Contractual Clauses (SCCs) approved by the European Commission
- Adequacy decisions where applicable (e.g., EU-US Data Privacy Framework)
- Binding Corporate Rules (BCRs) for internal transfers

## 7. Data Subject Rights Support

---

Silicon Harbor will assist Controller in responding to data subject requests within 10 business days:

- **Right of Access:** Provide export of analysis results in JSON/CSV format
- **Right to Deletion:** Delete all persona memory data within 72 hours
- **Right to Portability:** Provide data in machine-readable format for transfer

*NOTE: Source code is processed in real-time and NOT retained, so data subject requests primarily apply to analysis results and persona memory only.*

---

## EXECUTION PAGE

### DATA PROCESSING AGREEMENT

IN WITNESS WHEREOF, the parties hereto have caused this Data Processing Agreement to be executed by their duly authorized representatives as of the date last signed below.

#### **CONTROLLER (CUSTOMER):**

Company Name: \_\_\_\_\_

Signature: \_\_\_\_\_

Printed Name: \_\_\_\_\_

Title: \_\_\_\_\_

Date: \_\_\_\_\_

Email: \_\_\_\_\_

Address: \_\_\_\_\_

#### **PROCESSOR (SILICON HARBOR TECHNOLOGIES, LLC):**

Signature: \_\_\_\_\_

Printed Name: Kenny Alge

Title: Co-Founder & Chief Technology Officer

Date: \_\_\_\_\_

Email: kenny@siliconharbor.tech

Address: [Insert Silicon Harbor Registered Address]