

Data Protection

Overview

Protecting customer information is central to the design and operation of AIVA. AIVA implements administrative, technical, and organizational safeguards to protect the confidentiality, integrity, and availability of customer data throughout its lifecycle.

Our data protection program combines encryption, access controls, secure software development, vendor oversight, and documented privacy practices to help customers securely manage their information.

Customer Data Ownership

Customers retain ownership of the information they submit to AIVA.

AIVA processes customer data only to:

- Deliver requested services
- Operate and maintain the AIVA platform
- Improve platform functionality
- Comply with customer instructions
- Meet applicable legal obligations

Customers remain responsible for ensuring they have the necessary rights and permissions for any information submitted to the platform.

Types of Information We Process

The Privacy Policy identifies three primary categories of information processed by AIVA.

Account Data

Information used to create and administer customer accounts, including:

- Name
- Email address
- Organization information

- Account credentials
 - Billing-related information
-

Service Data

Information submitted by customers while using AIVA.

Examples include:

- Documents
- Images
- Audio
- Video
- Workflow data
- AI prompts
- AI-generated responses
- Application content

Service Data is processed only as necessary to provide requested services.

Usage Data

Operational information collected to improve reliability, security, and platform performance.

Examples include:

- IP address
 - Browser information
 - Device information
 - Diagnostic information
 - Log information
 - Usage analytics
-

Encryption

AIVA protects customer information both while it is stored and while it is transmitted.

Data in Transit

Communications with AIVA are encrypted using TLS 1.2+.

This includes supported REST API and WebSocket communications.

Data at Rest

Customer information stored by AIVA is encrypted at rest using symmetric encryption.

Encryption helps protect customer information from unauthorized access throughout the data lifecycle.

Access Controls

Access to customer information is governed by documented access control policies.

Current controls include:

- Least-privilege access
- Role-based authorization
- Multi-Factor Authentication (MFA)
- Administrative approval processes
- Periodic access reviews
- Audit logging

Access is granted only to authorized personnel who require it to perform legitimate business functions.

Data Retention

AIVA retains customer information only for as long as necessary to:

- Deliver requested services
 - Meet contractual obligations
 - Comply with applicable legal requirements
 - Resolve disputes
 - Enforce agreements
-

Customer Data Deletion

Customers may request deletion of their information following termination of services, subject to applicable legal, contractual, and regulatory obligations.

Upon written request, AIVA may:

- Return customer data
- Delete customer data
- Remove customer access

Deletion requests are processed in accordance with the Privacy Policy.

Customer Data Export

Customers maintain access to their information through AIVA's administrative capabilities.

Current capabilities include:

- CRUD APIs
 - Customer administrator access
 - Return of customer data following termination (upon request)
-

Data Sharing

AIVA shares customer information only where necessary to operate AIVA or comply with legal obligations.

Examples include:

- Cloud infrastructure providers
- AI service providers
- Service providers
- Business partners (where authorized)
- Affiliates
- Regulatory authorities where legally required

All sharing is governed by applicable agreements and privacy requirements.

International Data Transfers

Customer information may be processed by cloud providers and subprocessors operating in multiple geographic regions.

Where required by applicable law, AIVA implements appropriate safeguards for international transfers of personal information.

Privacy Rights

Depending on applicable law, individuals may exercise rights relating to their personal information.

Supported rights include:

- Access
- Correction
- Deletion
- Restriction of processing
- Objection to processing
- Data portability
- Withdrawal of consent

Requests are processed in accordance with the Privacy Policy and applicable privacy legislation.

Data Protection by Design

Privacy and security considerations are incorporated throughout the AIVA platform.

Documented practices include:

- Secure Software Development Lifecycle (Secure SDLC)
- DevSecOps
- Threat modeling
- Security testing
- Access controls
- Vendor risk management
- Incident response
- Business continuity planning

These practices help ensure that data protection is considered throughout the software development and operational lifecycle.

Subprocessors

AIVA utilizes carefully selected third-party providers to support cloud infrastructure and AI capabilities.

Current providers identified in the reference documentation include:

Subprocessor	Service	Data Processed
Amazon Web Services (AWS)	Cloud infrastructure, storage, networking, AWS Cognito, AWS Bedrock	Customer Data, Service Data, Usage Data
Microsoft Azure	Cloud infrastructure and Azure AI Services	Customer Data, Service Data
Google Cloud Platform	Cloud infrastructure	Customer Data, Service Data
Nebius	Cloud infrastructure and AI services	Customer Data, Service Data
GitHub	Source code version management	Service Data
Slack	Chat service for employees	Service Data
Discord	Chat service for customers	None

These providers process customer information only as necessary to deliver requested services.