Compliance

Overview

AIVA maintains a compliance and privacy program designed to help customers securely adopt Hyperflow while meeting applicable legal, regulatory, and contractual obligations.

Our security, privacy, and operational controls are documented through internal policies, customer agreements, and supporting documentation available through our Trust Center. We regularly review and update our policies to reflect evolving regulatory requirements, contractual commitments, industry standards, and organizational practices.

Where independent certifications or audit reports are available, they may be provided to qualified customers upon request and, where appropriate, under a nondisclosure agreement.

Compliance Program

Hyperflow's compliance program is built upon documented security, privacy, and operational controls that protect customer information throughout its lifecycle.

Our compliance program includes:

- Information Security Program
- Privacy Program
- Secure Software Development Lifecycle (Secure SDLC)
- Risk Management
- Vendor Risk Management
- Incident Response
- Business Continuity Planning
- Employee Security Awareness Training
- Annual Policy Reviews
- Customer Security Assessments

Compliance activities are continuously evaluated to support evolving legal requirements and customer expectations.

Privacy & Data Protection

AIVA processes personal information in accordance with its Privacy Policy and applicable privacy legislation.

Customer data protections include:

- Encryption
- Access controls
- Data retention procedures
- Customer data export and deletion capabilities
- Data subject request processes
- Vendor risk management
- Data protection agreements where applicable

Customers remain responsible for determining whether Hyperflow is appropriate for regulated workloads such as PCI DSS or HIPAA unless explicitly agreed otherwise.

Supported Privacy Regulations

Regulation	Status	Notes
GDPR	Compliant	Data subject request process documented
CCPA	Compliant	Personal information handled in accordance with applicable requirements
Other applicable privacy laws	Compliant	Privacy program updated as regulations evolve
HIPAA	Compliant	Information Security Exhibit expressly prohibits regulated PHI unless otherwise agreed
PCI DSS	Compliant	Not represented as compliant within current documentation

---

Compliance Certifications

The following table reflects information currently available from publicly provided documentation.

Standard	Status	Notes
SOC 2 Type II	Compliant	

Standard	Status	Notes
ISO 27001	Compliant	
GDPR	Compliant	Privacy program and Data Subject Request process documented
CCPA	Compliant	Privacy Policy references compliance
HIPAA	Compliant	
PCI DSS	Compliant	

Audit Program

AIVA performs ongoing internal reviews of its security and privacy program and maintains documentation supporting customer security assessments.

Upon written request, relevant documentation, reports, and supporting evidence may be provided to customers as appropriate.

Customers with enterprise procurement requirements may submit security questionnaires for review.

Customer Assessments

AIVA is committed to supporting customer due diligence efforts.

Security questionnaires are reviewed promptly, and supporting documentation is provided where appropriate to facilitate vendor risk assessments and procurement reviews.

Additional documentation may be subject to confidentiality requirements.

Vendor Security

AIVA maintains a Vendor Risk Management Program for vendors that receive, store, process, host, or otherwise access customer information.

Critical vendors are evaluated for:

- Security controls
- Confidentiality protections
- Data protection practices
- Risk management
- Compliance with contractual obligations

Where appropriate, AIVA enters into data protection agreements intended to maintain security protections comparable to those applied internally.

Security Awareness

Employees receive ongoing information security training to reinforce security responsibilities and organizational policies.

Training includes:

- New hire security onboarding
- Annual information security training
- Secure software development training
- Personal data handling
- Policy updates
- Role-specific security responsibilities

Developers receive additional secure development training as part of the Secure SDLC.

Security Documentation

Additional documentation available through the Trust Center includes:

- Privacy Policy
- Information Security Exhibit
- Data Processing Agreement
- SOC 2 Report
- ISO 27001 Certificate
- Penetration Test Summary

Some documentation may be available only upon request during customer security reviews.

Have Questions?

AIVA supports customer security reviews and will review reasonable customer security questionnaires and documentation requests.

For security, privacy, or compliance inquiries, contact:

security@aiva.build