Hosting & Deployment

Afi is hosted as a distributed container-based application in Google Cloud Platform (GCP) in the USA, Canada, the EU, the United Kingdom and Australia. These Google facilities hold all major security and data privacy accreditations, including SOC1 – SSAE-16, SOC2, PCI DSS Level 1, ISO 27001, HIPAA, FIPS 140-2.

Users can select the data storage location when they initially sign up in the Afi application. The available locations are:

- Google datacenter `us-central1` (Council Bluffs, Iowa, USA)
- Google datacenter `eu-west2` (London, England)
- Google datacenter `eu-west4` (Eemshaven, Netherlands)
- Google datacenter `northamerica-northeast1` (Montreal, Canada)
- Google datacenter `australia-southeast1` (Sydney, Australia)

The physical access to the servers in the datacenters is restricted to authorized Google and Amazon personnel. Afi employees have no physical access to the servers.

Encryption & Access Control

All customer data is always encrypted: both in transit and at rest. We use TLS 1.3 for all control communications, including data transfer between Afi components, to ensure all traffic is encrypted. When at rest, we use AES 256bit encryption.

Customer administrator and user self-service (if it is allowed by administrators) access to the service is possible only through Okta (SAML), Microsoft or Google identity services that support MFA. Afi employees and contractors don't have access to customer backup data.

We don't host any on-premise infrastructure and we require two-factor authentication for all employees that work with internal systems (code repositories, build systems, cloud providers). We apply the “least privilege” model meaning we assign access to employees based on the absolute least access someone needs to be able to perform their duties.

Backup & Resiliency

Afi services are deployed using Kubernetes Engine. High availability and disaster recovery is built-in into Afi's architecture. In case of a component failure, the platform launches additional container instances and redirects the load.

Afi’s backup policies and procedures outline the critical resources, including the databases, that are backed-up automatically to enable recovery needed to meet our SLAs. All production data is being replicated automatically to a separate infrastructure. Afi tests its data recovery plan continuously.

Sub-processors

We limit the extend of data sharing with our sub-processors to the degree that is minimally necessary to provide our service and make sure that all the technology providers that we use:

- pass regular security reviews and audits;
- comply with data protection and privacy regulations (SOC 2 and/or ISO 27001);
- have good reputation (publicly listed or private companies with reputable backers).

We encrypt (see Encryption & Access Control) all customer data stored in our infrastructure providers' (GCP and AWS) datacenters in transit and at rest. We share only limited information with Stripe, necessary to manage subscriptions, invoice and process payments (including customers' billing addresses, contact details and bank account details). We use customer relations management software, HubSpot and Zendesk, to automate the communication with customers and to store customer contacts in their systems.

Sub-processor	Description	HQ Location
Technology Providers		
Alphabet Inc.	Google Cloud Platform (GCP) offered by Google is a cloud computing service. GCP is compliant with SOC 1/2/3, ISO/IEC 27001, PCI DSS and other major security regulations. Afi uses GCP to host its container-based distributed application using Google Kubernetes engine, as well as to store the backup data using encrypted geo-redundant cloud storage.	Mountain View, CA
Amazon.com, Inc.	Amazon Web Services (AWS) is a subsidiary of Amazon providing an on-demand cloud computing service. AWS is compliant with SOC 1/2/3, ISO/IEC 27001, PCI DSS and other major security regulations. We use Amazon Elastic Kubernetes Service to host our application, and store the backup data using encrypted geo-redundant cloud storage.	Seattle, WA
Stripe, Inc.	Stripe offers payment processing and anti-fraud tools which Afi uses to accept payments from customers, manage subscriptions, and perform transaction reporting. Stripe is certified as a PCI Level 1 Service Provider, which is the most stringent level of certification available in the payments industry.	San Francisco, CA
HubSpot, Inc.	HubSpot provides tools for customer relationship management (CRM), social media marketing, lead generation and web analytics. It has TRUSTe certification for Enterprise Privacy and its IT is audited as part of the Sarbanes Oxley compliance. Afi uses HubSpot CRM and analytics tools to manage and automate our sales processes.	Cambridge, MA
Zendesk	Zendesk is a helpdesk software provider. It is compliant with SOC 2/3, ISO 27001 and other security regulations. Afi uses Zendesk to accept the customer support tickets, manage and automate the technical support services.	San Francisco, CA
Other		
Linford & Company LLP	Linford is an independent auditing firm specializing in third party SOC 1, SOC 2, HIPAA compliance audits, FedRAMP, HITRUST assessments. Afi engages Linford to achieve SOC 2 Type II certification.	Denver, CO

Compliance

Afi complies with major industry regulations and is independently audited as part of the SOC 2 compliance. Reach out at privacy@afi.ai if you need more details or if you have questions about a country- or industry- specific regulation that is not reviewed in this section.

AICPA SOC · CSA cloud security alliance℠ · EU GDPR COMPLIANT · Privacy Shield Certified · Australian Privacy Principles · PIPEDA Compliant Personal Information Protection and Electronic Documents Act · CALIFORNIA CONSUMER PRIVACY ACT · NHS Information Governance

SOC 2 Type II Certification

Service organization control (SOC) 2 is a framework that requires service providers like Afi to establish and follow strict information security policies and procedures, encompassing the security, availability, processing, integrity, and confidentiality of customer data.

Afi is **SOC 2 Type II** compliant. Our auditor is Linford & Company LLP.

SOC 2 is specifically focused on detailed information and assurance about the security, availability, and processing integrity of the systems (unlike SOC 1 that focuses on controls related to clients' financial reporting). A **type II** report details how security controls are implemented over a period of time (unlike type I report that reviews them based on a specified point in time).

Afi SOC 2 Type II report is available upon request after an NDA is signed between Afi and the requesting party (see the NDA form at the bottom of the page).

In addition to SOC 2 Type II report, we have SOC 3 report which details Afi's Trust Services Criteria controls and which you can access without an NDA.

Cloud Security Alliance

Cloud Security Alliance (CSA) operates the most popular cloud security provider certification program, the CSA Security, Trust & Assurance Registry (STAR), helping ensure a secure cloud computing environment.

Afi follows the CSA STAR principles and is included in the CSA STAR registry.

GDPR

The General Data Protection Regulation (GDPR) regulates data protection in the European Union (EU) and the European Economic Area (EEA). Afi is compliant with GDPR. Its major requirements and Afi features that help to address them include:

- Storing and processing data within EU. Afi enables customers to select where their data is stored by specifically setting the predefined destinations.
- Right to erasure. Afi will remove data from the system in a timely manner upon request.
- Security. All the customer data in transit and at rest is encrypted. Afi follows Secure Software Development Cycle and is independently audited as part of SOC 2 Type II certification.
- Records of processing activities. Afi audit log provides visibility on all actions performed in the system and enables customers to retrieve these logs when required.
- We have a Data Protection Officer who can be reached at privacy@afi.ai.

Privacy Shield

The EU-U.S. Privacy Shield is a set of data protection requirements developed by the US and the European Commission in order to regulate transferring personal data from the European Union to the United States. On July 16, 2020, the EU Court of Justice invalidated the EU-US Privacy Shield Framework, while confirming the validity of the European Commission’s standard contractual clauses as a legal mechanism for international transfers of EU personal data.

Despite the invalidation, the U.S. Department of Commerce continues to administer the Privacy Shield program and Afi continues to comply with it.

Afi Data Processing Addendum (see the Documents section) includes the standard contractual clauses that are validated by the EU Court of Justice ruling as a mechanism for international transfers of personal data. We will enter into the DPA if you use Afi to back up personal data of EU residents.

HIPAA

Afi complies with the HIPAA regulations. For customers that process Protected Health Information (PHI) and Personally Identifiable Information (PII) we will sign a Business Associate Agreement (please see the form below).

UK regulations

NHS Information Governance (IG) is a framework developed by NHS Foundation Trust. IG helps organizations to ensure that the information is handled securely and in accordance with relevant legal regulations and industry best practices. Afi is compliant with NHS Information Governance and we work with our customers to assist them with their compliance requirements.

Cyber Essentials is a set of technical controls developed by UK-government and the Information Security Forum. The framework helps organizations protect against cyber threats. Afi earned Cyber Essentials certification through a self-assessment of our systems, and the assessment was verified independently.

NCSC Cloud Security Guidelines is a framework that helps organizations evaluate the security of cloud services before adopting them. Afi services meet the 14 Cloud Security Principles included in the framework, and our compliance with them is independenty tested as part of SOC 2 annual audit.

Canadian regulations

The Personal Information Protection and Electronic Documents Act (PIPEDA) governs how organizations work with personal information. It gives individuals the right to access and request correction of the personal information these organisations collected. Afi is compliant with PIPEDA requirements and uses appropriate security measures to protect personal information.

Personal Health Information Protection Act (PHIPA) establishes principles for collection, use, and disclosure of personal health information (PHI). Afi complies with PHIPA and uses adequate security and privacy practices to protect PHI.