

WHITE PAPER

Flowsana Security and Privacy

How Flowsana protects your data



Last updated: September 2020

Infrastructure

Flowsana utilizes cloud computing service offerings, primarily from Microsoft Azure (Azure), as the core building blocks of the Flowsana platform.

Azure manages the security and compliance of the cloud computing infrastructure, and Flowsana manages the security and compliance of the software and sensitive data residing in the cloud computing infrastructure. Please refer to [the Shared Responsibility Model](#) from Microsoft Azure.

Flowsana has designed its network architecture to be secure, scalable, and easily managed using the networking services and building blocks that Azure provides. Azure Functions comprise the majority of the Flowsana platform and provide a reliable, scalable and secure way to process customer data.

Web Portal

Azure App Services is used to serve Flowsana's public web portal in a scalable way with low latency and high transfer speeds.

Databases

The Flowsana database uses the Azure SQL platform.

Data security

Encryption-in-transit

Connections to flowsana.net are encrypted with 128-bit encryption and support TLS 1.2. Logins and sensitive data transfer are performed over TLS/ SSL only.

Encryption-at-rest

Flowsana guarantees encryption at rest for customer data.

Scalability & reliability

Flowsana uses Azure SQL which grants scalability of the service. The database is replicated synchronously so that we can quickly recover from a database failure.

System availability level

Since Flowsana operates exclusively in conjunction with customers' Asana information, its service availability is dependent on the availability of the Asana service. Service uptime is guaranteed at 99.9% of the time that the Asana service is available.

Operational security

Flowsana information security

Confidential information

Flowsana treats all customer data as confidential, regardless of classification. This policy restricts access to confidential information to those employees who are required to access such confidential information as a part of their job and then only in those circumstances where access to such confidential information is required to provide a specific service to the customer. In such circumstances, the employee is directed to access only the minimum amount of confidential information necessary to perform the task at hand.

Data Center security

Flowsana relies on Microsoft Azure's world-class Physical and Environmental controls.

Risk and vulnerability management

Flowsana maintains a vulnerability scanning process both for external and internal systems in the production environment. Flowsana's Security team performs scans at least monthly and remediates vulnerabilities based on rating.

Software development life cycle

Flowsana uses the git revision control system. Changes to Flowsana's code base are first pushed to a staging server wherein Flowsana employees are able to test changes before an eventual push to production servers and our customer base.

Incident response

Flowsana maintains an Incident Response Plan designed to establish a reasonable and consistent response to security incidents and suspected security incidents involving the accidental or unlawful destruction, loss, theft, alteration, unauthorized disclosure of, or access to, proprietary data or personal data transmitted, stored, or otherwise processed by Flowsana. These incident response procedures detail how Flowsana triages, investigates, remediates, and reports on security incidents.

Disaster recovery and business continuity

Flowsana has prepared a business continuity plan for extended service outages caused by unforeseen or unavoidable disasters in an effort to restore services to the widest extent possible in a reasonable time frame.

Flowsana's primary data center is hosted on Microsoft Azure in Virginia, US. In the event of a single Azure data center loss, recovery procedures would bring up nodes in another data center.

Data retention and disposal

Data retention

We will retain your information for the period necessary to fulfill the purposes outlined in our Privacy Policy. For all customers, we delete their data by request.

Data disposal

Upon request from a customer's authorized representative, customers can request deletion of all customer data.

Sub-processors and vendor management

Flowsana takes reasonable steps to select and retain only third-party service providers that will maintain and implement the security measures consistent with our own policies. Before software is implemented or a software vendor can be used at Flowsana, Flowsana personnel carefully review the vendor's security protocols, data retention policies, privacy policies, and security track record. Flowsana may reject use of any software or software vendor for failure to demonstrate the ability to sufficiently protect Flowsana's data and end users.

Privacy, certifications, and compliance

Privacy Policy

The Flowsana Privacy Policy can be found [on our website Privacy page](#). It includes:

GDPR

The General Data Protection Regulation (“GDPR”) is a European law establishing protections for the personal data of EU residents that came into force on May 25, 2018. Under the GDPR, organizations that collect, maintain, use, or otherwise process EU residents’ personal data (regardless of the organization’s location) must implement certain privacy and security safeguards for that data. Flowsana has established a comprehensive GDPR compliance program and is committed to partnering with its customers and vendors on GDPR compliance efforts. Some significant steps Flowsana has taken to align its practices with the GDPR include:

- Revisions to our policies and contracts with our partners, vendors, and users.
- Enhancements to our security practices and procedures.
- Closely reviewing and mapping the data we collect, use, and share.
- Creating more robust internal privacy and security documentation.
- Carefully evaluating and building a data subject rights’ policy and response process. [Our website Privacy page](#) provides additional details about the core areas of Flowsana’s GDPR compliance program.