DATA SHEET

Planview Spigit Privacy Information

DESCRIPTION

Customer data is loaded into the Planview Spigit™ databases for the identification and selection of resources for assignment to the work that is managed in the Planview Spigit SaaS service. All data, including personal data of users, is provided by the Customer to Spigit. Categories of personal data, as well as data subjects, are exclusively determined and controlled by the Customer.

A customer must appoint one or more account administrators, who are responsible for the Planview Spigit user accounts.

Each user must provide unique identifiers, i.e. email and first/last name, to be able to log in to the system. Such data is essential for the user to be able to work in the product.

Any other information that account owners, users, and customers provide into the product, in documents, boards, tasks, administration, conversations, plans or about member participants, is solely controlled and administrated by the customer and/or users.

Visibility to a customer's personal data can be controlled by submitting a support request from the account administrator to delete the user's personal information. The request will be resolved in a timely manner.

When the customer terminates its contract with Planview®, Planview terminates the customer product account. The termination process deletes any access to the system by the customer and its users. If applicable, the termination process also destroys all data, processing, and utilization results as well as data sets related to the contract. This destruction process is managed in a data-protection-compliant manner. Customer data in archive storage is deleted thirty (30) days after the termination of a contract.

SECURITY

Technical and organizational measures with regards to risk

- ISO 27001 certification
- SOC 2 reports
- Annual pentests
- Internal policies and instructions
- Internal authorization for access to data
- Security and privacy e-learnings and seminars
- Incident Management Response Plan

The server environment is hosted in facilities that provide redundant electricity /internet, have fire protection, and strong access controls. A limited number of system operation team members have access to the production environment, including databases, through VPN access with two-factor authentication.

For the Planview Spigit service, operational access controls are implemented at the object level to prevent unauthorized users from accessing data. Data in transit is encrypted. All data is automatically encrypted using the AES-256 encryption algorithm. User passwords are stored in a one-way hash using a SHA-256-bit cipher. Encryption keys are stored separately, with precautions taken to prevent unauthorized access both to encrypted data and the corresponding encryption keys.

Planview retains user data for as long as a client remains an active subscriber of the service.

The Planview Spigit services are constructed on a multi-tier architecture, consisting of web servers, application servers and database storage. There are established coding standards and a software-development life cycle, with security incorporated from the very outset. Industry guidelines, such as The Open Web Application Security Project ("OWASP"), Secure Coding Guide, SANS CWE Top 25, and CERT Secure Coding are followed by the product development team. Security is tested by web application vulnerability scans quarterly and penetration tests an?nually. These tests are performed in accordance with OWASP testing guidelines.

The Planview Spigit production environment is protected by a robust network infrastructure that provides a secure environment for all customer data. The Spigit service is on a physically segregated network that requires VPN access and two-factor authentication for administrative access. Planview also monitors and analyzes system logs to identify unusual traffic patterns, potential intrusion attempts and other security threats.

User data is not stored on removable backup media (i.e. tapes). The backups serve the sole purpose of restoring the whole production system in the unlikely event of multiple server failure.

Hosting location

Customer instances, including data, are hosted in geographically disparate data centers. Customers may choose the location to host their data in based on corporate location or user base location in an effort to minimize latency.

Retention

Data is explicitly managed by the customer through the users that are the Spigit administrator. All information, including challenge and community, is retained for the duration of the project. Once a user initiates deletion of project data – for example, deleting a challenge – objects and files are deleted from the system.

Sub processors

Sub processors for parts of administration of the services are used.

Planview uses sub processors located in Australia, Canada, Europe, and the United States. The sub processors are processing personal data to provide the contracted services and identify events and activities between computers and agents (such as browsers) on the Internet (e.g. determining whether an action on a website is being performed by a human or a bot) or other identify patterns that may indicate malicious or fraudulent activity. Sub processors also provide services for security and operational information and event management system that aggregates system, infrastructure, and application log data for use in security, provide operational monitoring for activities performed by Planview staff. Information about sub processors is provided on Plainview's website and updated regularly.

Data Transfers

All data transfers must be subject to adequate transfer mechanisms, such as approved adequate level of protection by reason of its domestic law or of the EU Commission/ International commitments it has entered into, or the provisions in the European Commission Standard Contractual Clauses for the Transfer of Personal Data to Processors Established in Third Countries (2010/87/EU) ("Model Processor Contract").

Personal Data Breaches

Planview has an established security and privacy incident response plan and escalation procedures that ensure timely and effective handling of critical suspicious activities and situations. All affected customers are informed in the event of a confirmed data breach that may potentially expose their data or cause a major disruption to the service. Planview is in close contact with CERT, the police, and supervisory legal authorities to handle such cases in the event of a breach.

Data Processing Agreement

Planview has specific and tailored Data Privacy Agreements in place to ensure all requirements that Planview as a data processor is subject to, are fulfilled and compliant with the instructions given by the customer as a data controller, and the GDPR.

Compliance

Planview has appointed a Director of Information Security and a Data Privacy Officer to ensure compliance with the privacy regulations and security standards it is subject to.