Planview Enterprise One™

DATA SHEET

Planview Enterprise One Privacy Information

DESCRIPTION

Customer data is owned by the customer. In the context of data subject rights, the customer is the controller, and Planview® is the processor. The customer has responsibility for all data subject requests made by the customer's employees regarding data stored in the Planview Enterprise One™ service.

Planview Enterprise One enables the local administrator to define roles and permissions within the application. To support role-based access control, Planview Enterprise One user types indicate a grouping of user roles that define access rights.

When the customer terminates its contract with Planview, Planview terminates the customer product account. The termination process deletes any access to the system by that customer and its users, and if applicable, destroys all data, processing and utilization results, and data sets related to the contract that have come into its possession, in a data-protection compliant manner. Customer data in primary storage is deleted thirty (30) days after the termination of a contract. Backups of content are retained for thirty (30) days.

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

The server environment is hosted in separate 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.

Planview grants access on a least-privilege, need-to-know basis to ensure only those employees with a business need to access customer data have it. Access is reviewed regularly and removed promptly upon an employee's departure. Access to production environments is granted using multi-factor authentication and is logged / monitored by a dedicated security team.

All customer data in transit is encrypted using the AES- 256 encryption algorithm. Encryption keys are stored separately, with precautions taken to prevent unauthorized access both to encrypted data and the corresponding encryption keys.

Planview manages, processes, and stores customer data in accordance with relevant data protection regulations with specific requirements formally established in customer contracts. All user-generated content in the Planview Enterprise One environment is owned solely by the user.

The Planview Enterprise One 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 annually. These tests are performed in accordance with OWASP testing guidelines.

The Planview Enterprise One production environment is protected by a robust network infrastructure that provides a secure environment for all customer data. The Enterprise One service is on a physically segregated network that requires VPN access and twofactor 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

Data centers are located in different areas depending on customer location. For US customers, the data center is located in Texas, US. For European customers, we have data centers located in the United Kingdom or Germany. For APAC customers, the data center is located in Australia.

Retention

Data is explicitly managed by the customer. All information, including personal data and all project information, is retained for the duration of the project. Once a user initiates deletion of project data – for example, terminating a project – 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, Germany, 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.