DATA SHEET

Planview Projectplace Privacy Information

DESCRIPTION

Customer login user data is loaded into the Planview Projectplace™ databases as metadata for the identification and selection of resources for assignment to the work that is managed in the Planview Projectplace SaaS service. Processing activities comprises hosting in the SaaS product. All data, including personal data of users, is provided by the Customer to Projectplace. 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 owners, who are administrators of the Planview Projectplace user accounts. Account owners, or their delegates, are entitled to invite users to the service.

Each user must provide unique identifiers, i.e. mail 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 customer 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.

A user can delete its own user account at any time. An account owner can control account visibility or delete accounts, and thereby delete all information in the accounts, including user personal data.

When the customer terminates its contract with Planview®, Planview terminates the customer product account and deletes any access to the system by that customer and its users, and if applicable, destroys all documents, processing and utilization results, and data sets related to the contract that have come into its possession, in a data-protection compliant manner. The same applies to any and all connected test, waste, redundant and discarded material. All customer data is deleted at the most thirty (30) days after the termination of a contract. Back-ups of content is deleted after ninety (90) days.

SECURITY

Technical and organizational measures with regards to risk

- ISO 27001 certification
- SOC 2 reports
- Annual Pen-tests
- 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 separate facilities that provide redundant electricity/internet, have fire protection, and strong access controls. A limited number of system operation team members (fewer than ten) have access to the production environment, including databases, through two-factor authentication. The services are located on a physically segregated network that requires two-factor authentication.

For the Planview Projectplace service, operational access controls are implemented at the object level to prevent unauthorized users from accessing data.

Data in transit is encrypted, including User data. All documents stored are automatically encrypted with a unique key, using the AES- 256 encryption algorithm. User passwords are hashed with Scrypt. Documents are saved anonymously, rendering identification impossible. Encryption keys are stored separately, with precautions taken to prevent unauthorized access both to encrypted documents and their corresponding encryption keys. Planview employees are unable to restore individual projects or documents from backups.

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

The Planview Projectplace 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 whenever any significant change is made in the system and penetration tests annually. These tests are performed in accordance with OWASP testing guidelines.

The network containing the production servers (i.e. the service) is protected by redundant firewalls and load balancers. Planview proactively monitors and analyses firewall and systems, using its internal system for security information and event management, 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. Planview can retain user data indefinitely for active project members, and the data is downloadable for offline retention.

Hosting location

Data centers are located in different areas depending on customer location. For US customers, the data center is located in US. For European customers, the data center is located in Sweden.

Retention

Data is explicitly managed by the project user. 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, by emptying a project's waste paper bin or terminating a project – objects and files and their associated encryption keys are deleted from the databases.

Sub processors

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

Planview uses Sub processors located in the EU and US. The sub processors, some of which may be Privacy Shield certified, 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, and provide email SMTP relay. Information about Sub processors are 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 Security and a Data Privacy Officer to ensure compliance with the privacy regulations and security standards it is subject to.