

## DATA SHEET

# Planview LeanKit Privacy Information

## DESCRIPTION

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

LeanKit customer data is logically separated from that of other customers in a multi-tenant database, ensuring proper client segregation as well as an easy way to retrieve said data when a client requests their stored data. LeanKit offers a Private Cloud product for customers who need the added assurance of separate data instances.

A customer must appoint one account owner who can administer the Planview LeanKit user accounts. Account owners are entitled to increase the number of user licenses, upgrade editions, and / or close the account.

Elements of personally identifiable information stored and processed by LeanKit include User ID, name, surname, contact information (e-mail, address, phone number, and fax number), and IP address. 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 LeanKit service.

When the customer terminates its contract with Planview, Planview terminates the customer account. The termination process removes any access to the system by that customer and its users. An exiting customer can request to have their data deleted. In this scenario, customer data is deleted within thirty (30) days after the termination of their contract. Prior to contract termination, customers may request their data be provided in a standard format.

## 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 LeanKit production environment is hosted in industry leading, state-of-the-art facilities that provide a redundant, resilient operating infrastructure. Strong access controls are in place to provide physical protection of customer data. Only remote access using VPN with two-factor authentication is allowed for privileged support staff.

All 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. Encryption keys are managed using secure, industry standard methods. Keys are rotated on regular intervals.

The Planview LeanKit 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 are performed annually. Penetration tests are performed in accordance with OWASP testing guidelines.

---

## Hosting location

Data centers are located in Virginia, US.

---

## Retention

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