TDM

Privacy Policy

Privacy Policy

This section describes the measures to ensure personal data security and measures to protect personal data subjects' rights, as implemented in Protelion TDM.

Personal data means any information concerning a natural person that can be used for direct or indirect identification.

Protelion adheres to the principles of respect for rights and freedoms of data subjects with regard to their personal data. To safeguard the rights of subjects, Protelion TDM offers personal data security measures and features that help respect the data subjects' rights.

Key principles of personal data processing

Early at the product development stage, we have already taken measures to implement the personal data processing principles effectively:

- `Principle of transparency, fairness, and lawfulness in the processing and use of personal data` Protelion provides detailed information about the processing of data that can be considered personal. This helps reconcile the interests of the data subject and the product owner.
- `Principle of purpose limitation`. Personal data processing is limited to the specified, explicit, and legitimate purposes. The purposes of personal data processing are explicitly specified (see the section "What are personal data used for?" below). The products process the data within the scope required to achieve these purposes and do not process them otherwise.
- `Principle of data minimization` The products collect and retain the data within a reasonable scope and the limits of the processing purposes.
- `Principle of accuracy` Protelion products allow updating, rectifying, and erasing the personal data if needed, provided that the interests of the data subject and the product owner remain reconciled.
- `Principle of storage limitation` Protelion products provide for a procedure that supports timely and regular erasure of personal data to prevent uncontrolled storage of personal data.
- `Principle of integrity and confidentiality` To ensure adequate security of personal data, the products are developed using the security development. Methods that take into account various aspects, from product design to operation and use, to ensure protection against unauthorized or unlawful use, processing, and accidental loss, as well as negligent destruction or damage to personal data.

What is a personal data breach?

A personal data breach means “a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.”

In the event of a personal data breach, a controller responsible for the data processing shall:

- Immediately report the breach to a competent supervisory authority if the breach can result in a risk to the rights and freedoms of natural persons.
- Immediately inform the data subject about the breach if it can result in a risk to their personal rights and freedoms.
- Each violation must be documented by the supervisory authority, regardless of any reporting obligations, including all the facts related to the personal data breach (number of persons affected, number and categories of data records affected), consequences, and measures taken.

Protelion products, such as Protelion TDA, Protelion NIDS, already contain solutions to support the controller's accountability, assess risks and detect data security breaches.

What personal data does Protelion TDM process?

Protelion TDM does not process confidential personal data (“special categories of personal data”), such as racial and ethnic origin, political opinions, religious or ideological beliefs, trade union membership, genetic data, biometric data to identify a natural person uniquely, data concerning health or data concerning a natural person's sex life or sexual orientation.

Protelion TDM user data.

To control access to various features, the Protelion TDM authentication system processes:

- `User name`
- `User logon`
- `User role`

Protelion TDA user data.

To configure Protelion TDA controls, the Protelion TDM product processes the login of a Protelion TDA user with administrator rights.

Protelion user activity data.

- To audit user actions and ensure Protelion TDM non-repudiation, events related to Protelion TDM user actions are logged in the system.
- To monitor Protelion TDA to detect problems in the product's operation, events related to Protelion TDA user actions are logged in Protelion TDM.
- To monitor Protelion NIDS to detect problems in the product's operation, events related to Protelion NIDS user actions are logged in Protelion TDM.

Events related to user actions are logged in:

- Audit log
- Diagnostic log

Protelion TDM user device data.

For remote operation with Protelion TDM, the device's online ID is processed via Web Access.

What are personal data used for?

Description of reasons for processing your personal data	Categories of personal data used for the processing purposes
Protelion TDM user authentication and authorization	Protelion TDM user data
Managing Protelion TDA	Protelion TDA user data.
Logging of the user actions to audit and ensure non-repudiation	Protelion TDM user activity data
Ensuring the remote connection of the user	Protelion TDM user device data
Monitoring of Protelion TDA, Protelion TDM in order to detect operational issues	Protelion TDA, Protelion NIDS user activity data

Who can access personal data?

As part of information security processes supported by Protelion TDM, personal data can be made available to the following categories of recipients.

Recipient category	Reason for granting access
Protelion TDM Administrator	Secure data exchange between the corporate network user devices Managing the configuration setup of the user devices on the corporate network Monitoring of corporate user devices in order to detect operational issues
Protelion TDM Auditor	Investigating the user activity

How long are personal data stored?

Protelion TDM can automatically delete the data it collects and stores; the data are listed below. If the controller considers that extended storage is required, he or she should arrange suitable storage beyond the period provided by Protelion TDM, outside the product.

Storage	Storage term or conditions
Protelion TDM	Protelion TDM user data and Protelion TDA user data are deleted explicitly or on the product removal. Protelion device activity data: • In the audit log: deleted on the product removal or after 1 to 36 months (set by the Protelion TDM administrator, default value is 36 months). • In the diagnostic log: deleted on the product removal, when the storage exceeds 100 MB fill, or after 10 days. Data about the corporate network users' devices added to Protelion TDM are deleted explicitly or on the product removal.
Protelion TDM user device	Protelion TDM Web Access settings are stored in the web browser storage; these settings are deleted explicitly by the web browser tools or on the web browser removal.

How does Protelion help safeguard the rights of data subjects?

Protelion offers the following tools and documentation to support and facilitate the exercise of data subjects' rights.

Right of access The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

- Processing purposes
- Personal data category
- Recipients or categories of recipients to whom the personal data have been disclosed
- Storage duration

Data subjects may also have the right to obtain a copy of the personal data being the subject matter of the processing.

The information given earlier may be provided to data subjects from this section.

Copy is granted using the following tools:

- Audit log in the `csv` format
- Diagnostic log

a Protelion TDM administrator can obtain data subject details from the downloads to provide a copy to the data subject.

Right to rectification For the user, the right to rectification is exercised as the right to rectify the user email, user name, and email. Other data cannot be changed.

Right to erasure (right to be forgotten). The data subject shall have the right to erasure of the personal data concerning him or her without undue delay if the personal data are no longer necessary in relation to the purposes for which they were collected, as well as if the data subject objects to the processing and there are no overriding legitimate grounds for the processing.

Data erasure occurs as follows:

- Through rotation of data on Protelion product user activity.
- Through explicit deletion of user data and data about the corporate user's device. Explicit deletion of data about the data subject activity is impossible.

Right to data portability The right to data portability may exist in relation to the data subject's data, which the subject provided to a controller and processing of which is based on consent to rectification or an automated procedure. Protelion TDM does not provide for obtaining the consent for data processing operations performed using TDM. In addition, data subjects will not actively provide their personal data. Therefore, the product does not support data portability.

Right to object and right to restriction of processing The right to object and to restrict the processing can be exercised only by deleting a user and device from the system.