Protelion TDA

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 TDA.

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 TDA offers personal data security measures and features that help respect the data subjects' rights.

1. 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 para 3.7 "What are personal data used for?"). 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, Protelion develops secure products using the 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.

2. 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.

3. What personal data does Protelion TDA process?

Protelion TDA 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.

3.1 Protelion TDA user data

Protelion TDA controls access to various features through authentication with user name and a password.

Notifications about incidents and incident investigation progress employ the user email address.

The following features facilitate the user experience with Protelion TDA UI:

- Sorting by one of the columns
- Filters to search for information
- Customizations of columns and their order.

3.2 Data about the Protelion TDA user activity

User actions related to configuring Protelion TDA are logged.

3.3 Data about the Protelion TDA user's device

Online device ID is used for remote user connection to Protelion TDA.

3.4 Data about the network activity of the corporate user's device

To analyze the network activity of a corporate network user device, Protelion NIDS sends copies of device packets the analysis of which resulted in security events being captured on Protelion NIDS to Protelion TDA in the PCAP format.

3.5 Data about the corporate user's device

For a thorough analysis and security incident detection, products that interact with Protelion TDA provide the following:

- Protelion TDM centralized management and monitoring system:
  - IP address ranges of user devices protected by the Protelion NIDS network sensor
- Protelion NIDS Network Sensor:
  - Security events detected on network
  - User's device IP address
  - User's device DNS name

    - MAC address of the user's device network interface
- Protelion FW Network Sensor:
    - Security events detected on network
    - User's device IP address
- Protelion EPP Host-Based Sensor Server:
    - Security events both detected on hosts and within network
    - User's device IP address
    - User's device MAC address
    - User's device ID
    - File names and paths
    - Applications, services, tasks, and operating system processes
    - Registry keys, their paths, and values
    - Missing operating system updates

On configuring Protelion TDA, the following data are provided:

- IP address ranges of user devices of the corporate network protected by Protelion NIDS
- IP address ranges of user devices of the corporate network protected by Protelion FW

Security event details are enriched with information about CVE vulnerabilities on users' devices and uploaded to Protelion TDA.

Upon analyzing security events, Protelion TDA generates the following data:

- Security incident
- Country, city, and geolocation of the user's device
- List of CVE vulnerabilities on the user's device

A user can generate and download summary and statistical reports with security incidents and events captured on the user's devices.

3.6 Data about the corporate network user

Notifications about incidents and incident investigation progress employ the user email address.

For a thorough analysis and security incident detection, products that interact with Protelion TDA provide the following:

- Protelion EPP Host-Based Sensor Server:
    - Name, domain, and security ID of the target and active user account
    - Operating system event log with user actions

3.7 What are personal data used for?

Causes of the personal data processing

Cause	Personal data category
Protelion TDA user logons/logoffs	Protelion TDA user data
Logging of the user actions to ensure non-repudiation	Data about the Protelion TDA user activity
Building the Protelion TDA infrastructure	Data about the corporate network user's device

Cause	Personal data category
Collection and enrichment of information security events	Data about the corporate network user's device Corporate network user data
Security incident detection	Data about the corporate network user's device
Security incident and event analysis	Data about the network activity of the corporate user's device Data about the corporate network user's device Corporate network user data
Generating summary and statistical reports about security events and incidents	Data about the corporate network user's device
Security incident alerting	Protelion TDA user data Corporate network user data Data about the corporate network user's device
Transfer of security incident details to Protelion TDA or other SIEMs	Data about the corporate network user's device
Ensuring the remote connection of the Protelion TDA user	Data about the Protelion TDA user's device
User experience improvement in Protelion TDA web interface (Web Access)	Protelion TDA user data

3.8 Who can access personal data?

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

Categories of the personal data recipients

Recipient category	Reason for granting access
Primary Administrator	Configuring Protelion TDA
Administrator	Configuring Protelion TDA
Operator	Security incident and event analysis Generation and download of the summary and statistical reports
Auditor	Analysis of the Protelion TDA user activities in the audit log
Protelion TDA or a third-party SIEM system	Incident data transfer for further processing and analysis
Protelion TDA or corporate network user	Email notifications about incidents and their investigation progress

3.9 How long are personal data stored?

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

Protelion TDA stores the following data:

- Protelion TDA user data are deleted explicitly or on the product removal.
- Data about the corporate network users' devices in the Protelion TDA infrastructure (IP addresses range of the users' devices of the corporate networks) are deleted explicitly or on the product removal.
- Data about the CVE vulnerabilities on the corporate network users' devices are deleted explicitly or on the product removal.
- Data about the user actions (audit log events) are deleted on the product removal, on exceeding 100,000 entries in the log, or after 3 years.
- Security events captured on the corporate network users' devices are deleted on the product removal or after 45 days.
- Security event incidents detected based on the events captured on the corporate network users' devices are deleted on the product removal or after 3 years.
- Summary and statistical reports about security events and incidents are deleted explicitly or on the product removal.
- Online IDs of devices are deleted on user logoff. Session can be timed out due to the specified user idle time (1 minute to 24 hours). Administrator can turn off the idle session time-out.

Protelion TDA user's device stores the Protelion TDA Web Access settings in the browser storage; these settings are deleted explicitly by the browser tools or on the web browser removal.

3.10 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 owner has the right to request the controller to confirm whether their personal data is being processed and, if so, has the right to access the personal data and the following information:

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

  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.

  Copies are granted using the following tools:

  - Tabular data export (accounts, events and incidents, email notification recipients, audit log) to a CSV file

    See Exporting Data to a File.

  - Incident details export to a file of the selected format

    See Viewing the Incident Details.

  - Downloading the network packet duplicates from Protelion NIDS as a PCAP file

    See Viewing the Events Detected Within Network.

  - Export of summary and statistical reports to a file of the selected format

See Reports on Events and Incidents.

- Export of infrastructure to a text file

  See Managing the Infrastructure.

- **Right to rectification**

  For the user, the right to rectification is exercised as the right to rectify the user email. Other data processed by Protelion TDA cannot be rectified.

- **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 user activity, events, and incident
  - Through explicit deletion of user data

  Explicit deletion of data about the data subject activity and security events 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 TDA does not provide for obtaining the consent for data processing operations performed using Protelion TDA. 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**

  Right to object and right to restriction of processing is not exercised in this product.