Protelion EndPoint Protection

Privacy Policy

This section describes the measures to ensure personal data security measures and measures to protect personal data subjects' rights, as implemented in Protelion EndPoint Protection that consists of Protelion EndPoint Protection Server, Protelion EndPoint Protection Server Console, and Protelion EndPoint Protection Agent.

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

Protelion GmbH 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 EndPoint Protection offers personal data security measures and features that help to 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 GmbH 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 GmbH 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 GmbH 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 GmbH products, such as Protelion TDA, Protelion NIDS, Protelion HIDS, already contain solutions to support the controller's accountability, assess risks and detect data security breaches.

What Personal Data Does Protelion EndPoint Protection Process?

Protelion EndPoint Protection 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 EndPoint Protection processes personal data of two user types: Protelion EndPoint Protection Server users and Protelion EndPoint Protection Agent users.

Protelion EndPoint Protection Server User Data

- `User name`, data that identifies a user in the Protelion EndPoint Protection Server GUI.
- `User login`, a user ID in the Protelion EndPoint Protection Server authentication system.
- `User role`, Protelion EndPoint Protection Server user permissions that differentiate access to various features.

Data About the Protelion EndPoint Protection Server User Activity

- `User actions`, Protelion EndPoint Protection Server logs user actions on configuring and working with the server.

Corporate Network User Data

- `Email`, to notify the concerned parties about new security incidents.
- `Device group`, device groups are arranged into hierarchy for categorization purpose and analysis rule assignment. Groups can be based on details obtained from Active Directory. These details can contain personal data, such as a department the device owner belongs to or his/her position.

Data About the Corporate Network User's Device

- `Security event`, Protelion EndPoint Protection Agent on the user's device identifies data on the occurring security events and transfers it to Protelion EndPoint Protection Server to be further analyzed by the Protelion EndPoint Protection Server users and then transmitted to external information systems for a thorough analysis. During the analysis, Protelion EndPoint Protection Agent collects the following information:
  - Data from the Windows registry and the Windows event log to detect changes in the registry keys
  - Data from the application log to track applications installation and removal
  - List of OS services, processes to track installation and removal of services, start and termination of processes
  - Data on launched applications to monitor application startup
  - Data on access of applications to other applications, files, the registry to monitor process activity
  - Data on the device's network activity to control malicious activities in the network traffic, including:
    - Source and destination IP addresses when security rules are triggered
    - Source and destination DNS names
    - Device MAC addresses
  - List of services with network activity (local and remote IP addresses) to monitor network activity of the applications on the device
  - File names to monitor file changes. When a file changes, its name and the change event are transferred. The change is calculated by the checksum.
- `Security event notification`, information about a security event created to notify the stakeholders.
- `Network device status`, generalized information about the user's network device security status; required to promptly detect critical security events on the device.
- `Network device availability`, information about whether a device is reachable; required for status control, monitoring of, and prompt response to security events.
- `Network device ID`, the device name, the user-defined name of the network device, the internal device ID assigned by Protelion EndPoint Protection, and the device IP address are used to identify the network device of the corporate network user.
- `Operating system event list`, to detect anomalies on the network device, Protelion EndPoint Protection Agent first collects a list of operating system events that are considered normal and sends them to Protelion EndPoint Protection Server for further comparison with current events on the device.

Protelion EndPoint Protection Agent User Data

- `User name`, data that identifies a user in the Protelion EndPoint Protection Agent GUI. The data is stored on the user device and is not transferred anywhere.
- `User login`, a user ID in the Protelion EndPoint Protection Agent authentication system. The data is stored on the user device and is not transferred anywhere.
- `User role`, Protelion EndPoint Protection Agent user permissions that differentiate access to various features. The data is stored on the user device and is not transferred anywhere.

Data About the Protelion EndPoint Protection Agent User Activity

- `User actions`, Protelion EndPoint Protection Agent logs user actions on configuring and working with Protelion EndPoint Protection Agent.

What Are Personal Data Used For?

Description of reasons for processing your personal data	Categories of personal data used for the processing purposes
Identification of security events on the users' network devices	Data about the corporate network user's device
Protelion EndPoint Protection Server user authentication and authorization	Protelion EndPoint Protection Server user data
Protelion EndPoint Protection Agent user authentication and authorization	Protelion EndPoint Protection Agent user data
Logging of the Protelion EndPoint Protection Server user actions to ensure non-repudiation	Data about the Protelion EndPoint Protection Server user activity
Logging of the Protelion EndPoint Protection Agent user actions to ensure non-repudiation	Data about the Protelion EndPoint Protection Agent user activity
Protelion EndPoint Protection diagnostics	Data about the corporate network user's device
Security events analysis and response	Data about the corporate network user's device

Who Can Access Personal Data?

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

Recipient category	Reason for granting access
Protelion EndPoint Protection Server user	Arrangement of security event monitoring Auditing user actions
External analytics systems	Profound event analysis and detection of the security incidents

Recipient category	Reason for granting access
Information Security Analyst	Preliminary event analysis and detection of the security incidents
System Administrator	Response to security events

How Long Are Personal Data Stored?

Protelion EndPoint Protection 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 EndPoint Protection, outside the product.

Storage	Storage term or conditions
Protelion EndPoint Protection Server	• Account information is explicitly deleted when the account is deleted or as a result of uninstalling the product. • Recent audit log events are deleted when the data storage time of 400 days expires, when the maximum number of 50,000 records is achieved, or as a result of uninstalling the product. • Device IDs are explicitly deleted when the device is removed from the interface or as a result of uninstalling the product. • Security events are deleted by the administrator, after 45 days, or as a result of uninstalling the product. • Security event notifications, device statuses and availability are processed but not stored on the server. • The email address is deleted when explicitly removed by the server administrator or as a result of uninstalling the product. • The logical structure is deleted when explicitly removed by the server administrator or as a result of uninstalling the product. • The list of “normal” events on the device is deleted when the behavioral analysis rule is explicitly removed by the administrator.
Protelion EndPoint Protection Agent	• Account information is explicitly deleted when the account is deleted or as a result of uninstalling the product. • Recent audit log events, security events during the network traffic analysis are deleted when the data storage time of 30 days expires, when the maximum number of 50,000 records is achieved, or as a result of uninstalling the product. • Device IDs are stored in the configuration file and are deleted as a result of uninstalling the

Storage	Storage term or conditions
	product. • Security events detected while analyzing data from the Windows registry, the Windows event log, the application log, the list of services and processes, data about launched applications, data about applications accessing other applications, registry files, data about file changes are deleted when the data has been stored for 30 days, when the maximum number of 50,000 records is reached, or as a result of uninstalling the product.
Protelion EndPoint Protection Server Console	• The login of the last successfully connected Protelion EndPoint Protection Server user is stored locally to improve the product usability; deleted on the Protelion EndPoint Protection Server Console removal.

How Does Protelion GmbH Help Safeguard the Rights of Data Subjects?

Protelion GmbH 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 purpose
- 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 above information may be provided to data subjects from this section. You can view the Protelion EndPoint Protection Server user data and the Protelion EndPoint Protection Agent user device data in the Protelion EndPoint Protection Server GUI. Copies are granted using the following tools:

- Exporting the Protelion EndPoint Protection Server event log for a certain Agent.
- Exporting the Protelion EndPoint Protection Server audit log entries about a certain user.

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.

The data subject's data is deleted for the audit log and the event log using rotation mechanisms. For device data, by explicitly removing the device from the Protelion EndPoint Protection Server GUI. For user data, by explicitly removing the account.

All data is deleted as a result of uninstalling the product.

Right to data portability. The right to data portability may exist in relation to the data subject's data, which he or she provided to a controller and processing of which is based on consent to rectification or an automated procedure. Protelion EndPoint Protection does not provide for obtaining the consent for data processing operations performed using Protelion EndPoint Protection. 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 to and restrict data processing in the context of this product can only be exercised independently by deleting the user and the user devices from the system.