Protelion VPN

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 VPN.

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 VPN 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 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 "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, the products are developed using the Security Development Lifecycle. 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, Protelion HIDS, already contain solutions to support the controller's accountability, assess risks and detect data security breaches.

What personal data does Protelion VPN process?

Note: Protelion VPN 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 VPN user activity data

Protelion VPN logs locally all user actions related to the Protelion VPN configuration, as well as actions related to the product integrity control.

Protelion VPN copies the first 10 MB of the operating system log with the user logons/logoffs to `system-journal`.

Protelion VPN user device data

A Protelion VPN user can generate a report to identify problems in Protelion VPN operation and send it to the technical support. The report contains:

- The device name
- Operating system version
- Memory usage statistics
- Network interface settings
- List of processes loaded into memory

Protelion network user data

To protect the communication channel during deployment and operation, Protelion VPN receives the information about the host links generated by the management application, which includes the information about the connected devices and users, namely:

- Device's Protelion ID
- Device's Protelion address
- Device's Protelion name – may contain a user name

- User name
- User's Protelion ID

The user can also send this information to the technical support as a report generated in Protelion VPN.

Protelion user device activity data

Protelion VPN uses a built-in firewall to process the device's traffic and logs the information about the device's network activity to the local IP packet log:

- Source and destination IP addresses
- Network activity interval
- Protelion name and identifier of the sender's and recipient's VPN hosts

Also, Protelion VPN can show if the linked devices of Protelion network users are accessible over the network.

This information is used to diagnose the Protelion network state and the health of Protelion VPN.

What are personal data used for?

Description of reasons for processing the personal data	Personal data category
Provision of a protected communication channel	Protelion network user data
Ensuring non-repudiation of actions	Protelion VPN user activity data
Diagnostics of Protelion network operation	Protelion user device activity data
Protelion VPN diagnostics	Device data of a Protelion network user Protelion network user data

Who can access personal data?

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

Recipient category	Reason for granting access
Protelion network administrator	Diagnostics of Protelion network operation
User	Protelion VPN diagnostics
Protelion VPN	Provision of a protected communication channel

How long are personal data stored?

Protelion VPN supports automated erasure of data collected by Protelion VPN and stored in the application, as described below. If the controller considers that extended storage is required, they should arrange suitable storage beyond the period provided by Protelion VPN, outside the product.

Storage	Personal data category	Storage term or conditions
Protelion VPN	• IP Packet Log that contains the information about the network activity of the device on which Protelion VPN is installed. Log rotation affects the data older than 7 days. • Operating system event log with the user logons/logoffs.	Gets deleted when Protelion VPN is uninstalled.
	• Administrator log with the user actions related to the Protelion VPN configuration, as well as actions related to the product integrity control.	Gets deleted when reaches 10 MB or when Protelion VPN is uninstalled.
	• Host links that list VPN hosts linked with the user's Protelion VPN device.	Do not get deleted when Protelion VPN is uninstalled.

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 purpose
  - Personal data category
  - 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 above information may be provided to data subjects from this section. The information about the VPN hosts connected to the user's host, about the network activity of the user's devices, and about the Protelion VPN user activity can be viewed directly in the application.

- **Right to rectification**

  It is impossible to rectify the data processed by Protelion VPN.

- **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 are erased when the application is uninstalled and when the user's host is deleted from the management application.

- **Right to data portability**

  The right to data portability may exist in relation to the data subject's data, which was provided to a controller and processing of which is based on consent to rectification or an automated procedure. Protelion VPN does not provide for obtaining the consent for data processing operations performed using Protelion VPN. 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 host in the management application.