Protelion SG RPi

Privacy Policy

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

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 SG RPi 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 the 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 (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 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 personal for a procedure that supports timely and regular erasure of personal for prevent uncontrolled storage of personal data.

- Principle of integrity and confidentiality

  To ensure adequate security of personal data, the Protelion GmbH 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.
- Document the event, 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 SG RPi process?

Protelion SG RPi processes:

- User data

  User role differentiates access to the system features. Information is generated the moment the user activity is detected on remote access.

- User activities

  User activities are written to the system log. The log entry contains:

  - Date and time of the remote user of Protelion SG RPi
  - IP address of the device used to perform the activities
  - Configuration and management operations
  - Role used to perform the operations

- User device data

  Correct remote work with Protelion SG RPi via Web Access requires the online ID that gets deleted as the session terminates or after 15-minute user idle time.

- VPN device activity data

  To control and log the traffic filtering rule violations, Protelion SG RPi logs the network activity of Protelion user devices:

  - IP addresses of the sender's and the recipient's devices
  - Network activity time
  - Name and ID of the sender's and the recipient's VPN hosts

  To provide the Protelion network diagnostics, Protelion SG RPi displays details about the MFTP packets that contain indirect information about file exchange between Protelion user devices.

  Protelion SG RPi also checks the linked devices for connectivity.

- Unprotected device activity data

  If Protelion SG RPi functions as a firewall, it logs activity of unprotected devices whose traffic it logs:

  - IP addresses of the sender's and the recipient's devices
  - Network activity time
- VPN device details

  Protelion SG RPi obtains the following details about all the VPN hosts from the management software:

  - Links between VPN devices

    Information about links between VPN devices is necessary to route the encrypted traffic.
  - Device name

    Protelion SG RPi receives the names of the devices linked with it for the purpose of Protelion network diagnostics.
  - Device's Protelion ID

    Protelion SG RPi receives only IDs of device linked with it for the purpose of Protelion network diagnostics.

Note: Protelion SG RPi does not process confidential personal data (“special categories of personal data”):

- 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

What are personal data used for?

Description of reasons for processing the personal data	Personal data category
Filtering rule violations	VPN device activity data Unprotected device activity data
Logging of the user actions, ensuring non-repudiation	User data User activities User device data
User authentication and authorization.	User device data User activities
Diagnostics of Protelion network operation	VPN device activity data VPN device details
Encrypted traffic routing	VPN device details

Description of reasons for processing the personal data	Personal data category
Ensuring fault tolerance	VPN device activity data VPN device details

Who can access personal data?

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

Recipient category	Reason for granting access
Protelion SG RPi user or administrator	Protelion SG RPi configuration and management Protelion network diagnostics
External monitoring system	Transferring Protelion network details to monitoring systems Data transferred: • Device network activity • Devices linked with Protelion SG RPi • Connectivity of linked devices
Protelion SG RPi	Ensuring fault tolerance A Security Gateway can transfer the following to another Security Gateway: • Network activity data • Linked between VPN hosts

Note: Protelion SG RPi administrator can be an organization employee who uses Protelion service or a representative of the service provider that provides this service to the organization.

How long are personal data stored?

Protelion SG RPi 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 SG RPi, outside the product.

Data	Storage	Storage terms and conditions
IP packet log Contains information about device network activity	Protelion SG RPi	Get deleted when the log size is exceeded (cyclic buffer) or on user request
System log Contains information about Protelion SG RPi user activities	Protelion SG RPi	On user request
MFTP packet log Contains information about	Protelion SG RPi	On user request

network activity of the VPN devices		
VPN host links Contain information about VPN hosts and links between them	Protelion SG RPi	Get deleted on the Protelion SG RPi decommissioning or on user request

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:

  - Purposes of the processing
  - Categories of personal data
  - 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.

  Information about VPN hosts linked with the user host is provided via the management Protelion software.

  Information about the network activity of user devices is provided through exporting the IP packet log. For details, see the document “Configuring Using CLI,” the section “Event Logging and Viewing the Logs” > “Exporting the IP Log.”

  Information about the Protelion SG RPi user activities is provided through exporting the system log. See the document “Configuring Using CLI,” the section “Event Logging and Viewing the Logs” > “Working with the System Log” > “Exporting to a Removable USB Drive.”

- Right to rectification

  The data processed by Protelion SG RPi 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.

  The data subject's data are erased, in case of the host links, on decommissioning.

  System log, IP packet log, and MFTP logs are erased through the log cleanup feature. For details, see the documents “Configuring Using CLI” and “Configuring Using Web Access,” the section “Event Logging and Viewing the Logs” > “Cleaning Up the Logs.”

- 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 SG RPi does not provide for obtaining the consent for data processing operations performed using Protelion SG RPi. 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

  As for this product, the right to object and to restrict the processing can be exercised for unprotected user devices only by disconnecting the device from the network; for VPN devices, by deleting the links with the Security Gateway.