Protelion NIDS

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 NIDS.

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 NIDS 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 NIDS process?

Protelion NIDS 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 NIDS user data

To control access to features and to ensure non-repudiation, Protelion NIDS uses an authentication mechanism based on:

- Account name
- Full user name
- User role

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

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

- Sorting by one of the columns
- Customizations of columns and their order.

3.2 Data about the Protelion NIDS user activity

User actions related to configuring Protelion NIDS are logged.

Report details contain information about the creator.

3.3 Data about the Protelion NIDS user's device

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

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

To analyze the network activity of a user's device in a corporate network, Protelion NIDS stores and allows you to:

- Download copies of device network packets related to a security event in the PCAP format
- Download a network session fragment related to a security event

3.5 Data about the corporate user's device

When configuring Protelion NIDS, you should specify the IP addresses range of user devices in the corporate network protected by Protelion NIDS.

If Protelion NIDS is managed by , the IP addresses range of corporate network devices is transferred from .

Corporate network traffic analysis provides the following data:

- Security events
- User's device IP address
- User's device MAC address
- Device location country and city

In Protelion NIDS, a user can generate and download statistical reports with security events captured on the user’s devices.

3.6 Data about the corporate network user

The e-mail address of the corporate network user is used for security event alerts.

3.7 What are personal data used for?

Causes of the personal data processing

Description of reasons for processing your personal data	Category of personal data used for the processing purposes
Protelion NIDS user logons/logoffs	Protelion NIDS user data
Logging of the user actions to ensure non-repudiation	Data about the Protelion NIDS user activity
Security incident detection	Data about the corporate network user's device
Security event analysis	Data about the network activity of the corporate user’s device Data about the corporate network user's device
Security event alerting	Data about the corporate network user’s device Protelion NIDS user data Corporate network user data
Security incident transfer to or a third-party SIEM system	Data about the corporate network user's device
Ensuring the remote connection of the Protelion NIDS user	Data about the Protelion NIDS user's device
User experience improvement in Protelion NIDS web interface (Web Access)	Protelion NIDS user data

3.8 Who can access personal data?

As part of information security processes supported by Protelion NIDS, 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 NIDS
Administrator	Analysis of the Protelion NIDS user activities in the audit log
User	Security event analysis Generating and downloading statistical reports
or a third-party SIEM system	Transferring security event data and captured packet payloads for further processing and analysis
Protelion NIDS or corporate network user	Receiving security event alerts by e-mail

3.9 How long are personal data stored?

Protelion NIDS 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 NIDS, outside the product.

Personal data storage term and conditions

Storage	Storage term or conditions
Protelion NIDS	• Protelion NIDS user data are deleted explicitly or on the product removal. • Statistical reports with details of security events captured on corporate network user devices are deleted explicitly or on the product removal. • Custom report data are deleted explicitly when the report is deleted or on the product removal. • Data about the corporate network users' devices in the Protelion NIDS settings (IP addresses range of the protected networks) are deleted explicitly or on the product removal. • User activity data (audit logs) are deleted when the hard drive runs out of space or on the product removal. • Security events of a corporate user's device and network packet payloads are deleted explicitly, when the hard drive runs out of space, 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 NIDS user device	Protelion NIDS 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 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 purpose.
  - 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:

  - Security event export into a CSV file

    See Exporting Event Details to a File.

  - Downloading the network packet payload as a PCAP file

    See Downloading a Malicious Packet or File

  - Downloading a network session fragment as a PCAP file

    See Downloading the Network Session Fragment.

  - Exporting a statistical report to a file

    See Event Reports.

- **Right to rectification**

  For the user, the right to rectification is exercised as the right to rectify the user name. Data about the user’s activity in the product or device security events 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:

  - Due to rotation of user activity data, security events, network packet payload, and network session fragments
  - By explicitly deleting user data, security events, network packet payload, and network session fragments

  Data about the activity of the data owner cannot be deleted explicitly as this would be against the legitimate interests of the company using Protelion NIDS.

- **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 NIDS does not provide for obtaining the consent for data processing operations performed using Protelion NIDS. 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 Protelion NIDS.

PROTELION

protelion.com

Product version: 3.10.0

© 2024 Protelion GmbH. All rights reserved.

All brands and product names that are
trademarks or registered trademarks are the
property of their owners.