Protelion Enterprise Messenger

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 Enterprise Messenger.

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 Enterprise Messenger 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 Enterprise Messenger process?

Note: Protelion Enterprise Messenger 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.

User device data

Personal data collected on Protelion Enterprise Messenger enrollment and necessary to get started, in particular:

- Device ID
- Device Protelion ID
- Device Protelion name

User data

Data collected in the course of Protelion Enterprise Messenger operation, necessary for group chats to function and to ensure the postponed data delivery:

- User messages in group chats
- Files sent by a user

Activity data

Data collected in the course of user activity to improve user experience, including:

- Outgoing call log
- Incoming call log
- User status
- Message status

Call details and message delivery events are written to the log generated on user request; a user can send the log to the Support Team to troubleshoot Protelion Enterprise Messenger.

What are personal data used for?

Description of reasons for processing your personal data	Categories of personal data used for the processing purposes
Device wakeup	Device data
User experience improvement	Activity data
Analysis, diagnostics, and troubleshooting	Activity data
Ensuring links between users	User data Device data

Who can access personal data?

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

User category	Reason for granting access
Employees	Each user needs a contact list to send messages and make calls. Protelion Enterprise Messenger identifies users by device Protelion name.
Protelion ecosystem servers	Servers ensure the wakup of devices you want to call or send a message to. Servers also store your messages and the files you shared in group chats, as well as ensure the postponed delivery to the turned off devices.
Vendor's technical support	The Support Team needs your outgoing call and message details to analyze, diagnose, and troubleshoot. This data is generated and delivered on your initiative only.

How long are personal data stored?

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

Storage	Storage term or conditions
User device	User data gets deleted when Protelion Enterprise Messenger is uninstalled.
Group chat server	User files get deleted automatically in case of the server disk overflow.
Push server	Device IDs and host IDs do not get deleted.

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 purposes
- 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.

- **Right to rectification**

  Data rectification is unavailable in Protelion Enterprise Messenger, except for device Protelion name. Device can be renamed via Protelion SMC.

- **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.

  Device data and activity details are deleted on the VPN host removal from Protelion SMC. (See the document “Protelion SMC. Primary Administrator’s Guide,” the section “Viewing and Removing Organization's Devices.”)

  Protelion Enterprise Messenger does not allow for deleting user's private messages, group chat messages, and shared files.

  Selective deletion of user messages is unavailable.

- **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 Enterprise Messenger does not provide for obtaining the consent for data processing operations performed using Protelion Enterprise Messenger. 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 removing an “Enterprise Messenger” role from the user's Protelion devices via Protelion SMC. (See the document “Protelion SMC. Primary Administrator's Guide,” the section “Allowing the Protelion Enterprise Messenger App to a Single User.”) After the role has been removed from the user's Protelion devices, calling and chatting become unavailable.