Protelion SMC

Privacy Policy

This section describes the measures to ensure personal data security and measures to protect personal data subjects' rights, as implemented in Protelion SMC that comprises the following modules:

- Protelion SMC VPN
- Protelion SMC Rollout
- Protelion SMC Monitoring
- Protelion SMC Policies
- Protelion SMC Enterprise Messenger Book

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

An identifiable natural person is a person who can be identified directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, online ID, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

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 SMC 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 "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 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.
- 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 TDS, 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 SMC process?

Note: Protelion SMC 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,data concerning health or data concerning a natural person's sex life or sexual orientation.

Protelion SMC processes personal data of users of two types: users of the Protelion server solutions and users of the Protelion endpoint solutions, such as Protelion VPN and Protelion Enterprise Messenger.

Protelion SMC user data

- User name: information that identifies a user in the Protelion SMC GUI.
- Email: if Protelion SMC is connected, Protelion SMC users are notified on the Protelion network issues.
- User description: additional user details that facilitates the user list usage.
- User role: Protelion SMC user permissions necessary to control access to features. For details, see the section “Role-Based Administrator Access” in the Protelion SMC documentation.
- Organization name: information on whether a Protelion SMC user belongs to an organization. Necessary to control data access within an organization.

- Department: information on whether a user belongs to an organization department. Necessary to arrange users into logical groups and control access within a department.
- Login: user name used on the Protelion SMC notification system.
- User ID: internal unique user ID used in the interface to unambiguously identify a user even if the user name changes.

Protelion network user data

- User name: information that identifies a user in the Protelion SMC GUI. If Protelion SMC Rollout is connected, this information is used in Protelion SMC Rollout to manage setup invitations and access to Rollout service.
- Phone and email: if Protelion SMC Rollout is connected, this information is used in Protelion SMC Rollout to manage Protelion VPN software setup invitations, to transfer credentials and VPN key set password.
- User description: additional user details that facilitates the user list usage.
- User photo: if Protelion SMC Enterprise Messenger Book is connected, this information is used to identify a user in the Protelion SMC GUI and in Protelion Enterprise Messenger.
- Organization name and ID: information on whether a Protelion SMC user belongs to an organization. Necessary to control data access within an organization.
- Department: information on whether a user belongs to an organization department. Necessary to arrange users into logical groups and control access within a department.
- Internal phone number: if Protelion SMC Enterprise Messenger Book is connected, a virtual number is used to call and accept call via Protelion Enterprise Messenger.
- Login and password: access to Protelion user key set requires authentication. It supports both Active Directory authentication and accounts created in the authentication system itself. When generating a setup invitation for a Protelion user, Protelion SMC Rollout creates an account on the side of the Protelion SMC authentication service and delivers login and password in the user invitation by email or SMS. Protelion SMC Rollout does not neither process nor stores Protelion user login and password in any way.
- User ID: internal unique user ID used to unambiguously identify a user even if the user name changes.
- User links: Protelion SMC VPN processes links of a user with other Protelion network users and corporate resources the user needs to work with.
- User group: if Protelion SMC VPN is connected, you can arrange Protelion network users into logical groups to facilitate linking. Group names also can contain personal data that identifies a user.
- User access to key sets: if Protelion SMC Rollout is connected, you can manage and process information about user's key set access permissions for user devices. When a user is authenticated in the Protelion SMC notification system at the Protelion endpoint deployment, Protelion SMC Rollout checks whether the user has sufficient permissions to access a VPN key set.
- Event log: displays administrator actions in the modules, as well as the Protelion SMC events.
- Protelion Enterprise Messenger call and message history: a Protelion SMC Monitoring operator can poll a device for the Protelion Enterprise Messenger logs with the app's technical details and message history. Protelion Chat Server can be polled for call history. The logs store only the time of calls and messages and the device name of a contact. The logs can help the support team in troubleshooting Protelion Enterprise Messenger. Call and message contents are not retained in any way.

- User's permission level for communication via Protelion Enterprise Messenger: if Protelion SMC Enterprise Messenger Book is connected, the level determines whether a user can call and chat another employee via Protelion Enterprise Messenger.
- Additional parameters from an external data source: if Protelion SMC Enterprise Messenger Book is connected, this means any additional information about a user or user workstation. For example, department or title, as well as additional contacts. This information facilitates the corporate network management for a Protelion user or Protelion SMC administrator.

Protelion SMC user device activity data

- Online ID: necessary to connect to Protelion SMC and all the connected modules via Web Access; gets deleted on session termination or after 15-minute user idle time.
- Device ID in the SMC core: necessary for Protelion SMC Monitoring to identify a device the monitoring data came from.
- Device token: necessary for Protelion SMC Monitoring to authenticate a device the monitoring data came from.

Protelion network user device data

- Protelion user device name: displayed in Protelion SMC and its modules (Protelion SMC Monitoring, Protelion SMC Rollout, Protelion SMC Policies, Protelion SMC VPN); allows for tracking the key sets, monitor devices, and configure links. Created in Protelion SMC on configuring or generating a key set; can contain a user name. Stored in Protelion SMC as well.
- Protelion user device type: device OS details to configure device in Protelion SMC and its modules. Allows an administrator to manage a corporate Protelion network.
- User login that started VPN service on a device: for some products, Protelion SMC Monitoring can collect information about a login having started VPN service on a device.
- Protelion ID of a Protelion user device: If Protelion SMC VPN is connected, it also processes device's Protelion ID displayed in the product GUII. ProtelionID facilitates administering in Protelion SMC and is necessary for Protelion networks to function.
- Key set: a key set is created in Protelion SMC manually and can be saved to a Protelion SMC server or to Protelion administrator workstation. A key set can also be requested by the Protelion VPN software via Protelion SMC Rollout. In this case, key sets are stored in the Protelion SMC Rollout storage protected by unique passwords known only to the key set owners. A key set contains the following personal data:
  - Protelion device user's Protelion name that can contain a user name
  - Protelion ID of the Protelion user device
  - Protelion name of a Protelion network user
  - Protelion ID of the Protelion user device
  - List of the Protelion user devices linked with a device; contains devices' Protelion names and IDs
  - List of the Protelion users linked with a user; contains users' Protelion names and IDs
- Key set password: a key set is password-protected to enhance security. The password is generated automatically on administrator request or at key set generation in Protelion SMC Rollout; then, it is passed to Protelion SMC to protect a generated key set. At the same time, the password is delivered to a user by email or SMS, or directly to the user's Protelion VPN software. A password is neither processed nor stored anywhere else.

- Data for Protelion SMC Monitoring to monitor the network details:
  - User device's Protelion name
  - User device's Protelion ID
  - User's Protelion ID
  - User computer's name
  - OS user currently logged in
  - OS activation key
  - User device IP addresses
  - User device MAC addresses
- Network activity on a device: a Protelion NVS operator can poll a device with the Protelion VPN software installed for an IP packet log with device network activity.
- Protelion VPN software logs: if a device with the Protelion VPN software installed is added to Protelion SMC Monitoring, a Protelion SMC Monitoring operator can collect a device's Protelion VPN software logs that contain the following:
  - Information about smartphone firmware and settings:
    - Phone model
    - CPU type
    - Mobile provider
    - Firmware version
    - System DNS server
    - DNS name
    - Regional settings
    - Time zone
    - Serial number
  - Smartphone network settings (name, IP address, MAC address)
  - App list
  - Running processes
  - List of devices linked with a Protelion user device
- Additional parameters from an external data source: if Protelion SMC Enterprise Messenger Book is connected, this means any information about a user or user workstation. For example, department or title, as well as additional contacts. Facilitates the corporate network management for the Protelion SMC administrator, and Protelion products usage for a user.

Data of the organization network devices

Protelion SMC Monitoring can scan an organization network for devices with no Protelion software and for devices not added to Protelion SMC. The module processes IP/MAC addresses and passes them to the Protelion SMC Monitoring server. A discovered device can be added to Protelion SMC. Protelion SMC Monitoring agrees its device list with Protelion SMC; so, new devices appear in Protelion SMC Monitoring automatically. The following data is processed:

- Device name: information that identifies a device in Protelion SMC

- Device description: any additional device details
- Organization name: information on whether a device belongs to an organization
- Department: information on whether a device belongs to an organization department.

Protelion SMC user activities

Protelion SMC logs all the user activities on configuring Protelion SMC, managing the Protelion SMC user access, creating Protelion users and their devices. This is necessary to detect incorrect or illegal activities of employees that had a severe impact for an organization.

Protelion SMC VPN logs all activities of a Protelion SMC user in Protelion SMC VPN on configuring Protelion SMC VPN, liking devices and users, creating user groups.

Protelion SMC Rollout logs all activities of a Protelion SMC user in Protelion SMC Rollout on configuring Protelion SMC Rollout, managing the Protelion user access to key sets, sending a setup invitation.

Protelion SMC Monitoring logs all activities of a Protelion SMC user in Protelion SMC Monitoring on configuring the monitoring and obtaining logs from Protelion user devices.

Protelion SMC Policies logs all Protelion SMC user activities in Protelion SMC Policies on centralized policy management on Security Gateways on the organization's Protelion network.

Protelion SMC Enterprise Messenger Book logs all Protelion SMC user activities in Protelion SMC Enterprise Messenger Book on managing the Protelion Enterprise Messenger address book.

Protelion network user activity data

Protelion SMC Rollout logs user requests for key sets. Protelion SMC Rollout does not keep the logged events and delivers them to Protelion SMC.

What are personal data used for?

Description of reasons for processing the personal data	Personal data category
Secure data exchange between the Protelion network user devices	Protelion SMC user details Protelion network user data Protelion network user device data
Protelion network user authentication and authorization	Protelion network user data
VPN host key set setup	Protelion network user data Protelion network user device data Protelion network user activity data
Logging of the user actions, ensuring of non-repudiation	Protelion SMC user activities
Monitoring of Protelion user devices in order to detect Protelion network issues	Protelion network user device data
Security policy management on the Protelion network devices	Protelion network user data Protelion network user device data

Who can access personal data?

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

Recipient category	Reason for granting access
Protelion network user	Need for authentication
Protelion SMC user	Secure data exchange between the Protelion network user devices Manage the key set installation Monitoring of Protelion user devices in order to detect Protelion network issues Security policy management on the Protelion network devices
Protelion VPN	Authentication in Protelion SMC Key set acquisition
Protelion Enterprise Messenger	Ensuring secure corporate communications

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

How long are personal data stored?

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

Storage	Data	Storage terms and conditions
Protelion SMC	Key set (if Protelion SMC Rollout is used)	Stored for no more than a day, from the moment it was created till the moment the key set request limit runs out. To clarify the key set storage terms and conditions, contact the Protelion SMC administrator.
	Event log entries	Deleted on the event log cleanup. By default, stored for no more than a year and then deleted automatically.
	Device monitoring data, Protelion VPN logs, event log in Protelion Enterprise Messenger, device network activity (if Protelion SMC Monitoring is used)	By default, stored for no more than 90 days and then deleted automatically. To clarify the storage terms and conditions, contact the Protelion SMC administrator.
	User permission level for communication via Protelion Enterprise Messenger	Deleted explicitly or on the organization user removal from the system.

Storage	Data	Storage terms and conditions
	User photo, internal phone number, additional parameters from the external data source	Deleted explicitly on organization user removal from the system. When data is deleted from Active Directory, Protelion SMC data get deleted after syncing with Active Directory. Make sure to delete a user photo in Active Directory; otherwise, it gets restored after syncing with Active Directory.
	User device type, name, and ID	Get deleted on device removal from Protelion SMC A device removed from Protelion SMC VPN remains in the SMC core with the name that was specified. Device type and Protelion ID are nor preserved. Protelion SMC Monitoring stores the data for as long as specified in the module itself, even if the data was deleted from Protelion SMC VPN or Protelion SMC.
	User links, list of devices linked with a Protelion user device	Deleted manually by an administrator in order to restrict access to the network objects or automatically on the user removal from Protelion SMC.
	User groups	A group is deleted or a user is removed from a group manually by an administrator or automatically on the user or group deletion from the system.
	Other SMC user data and Protelion network details	Deleted explicitly on on the organization 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 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.

  Key set for a particular device is provided to a user on request during the setup and is deleted when the request limit is exceeded.

Event log can be downloaded any time necessary; a Protelion SMC administrator can use it to obtain data subject details. See the section “Viewing the Event Log” in the Protelion SMC documentation.

The following logs can be obtained from the log store: logs of the Protelion VPN software installed on a user device, IP packet log with device network activity details, and Protelion Enterprise Messenger log. See the section “Receiving the Log Files From a Device” in the Protelion SMC Monitoring documentation.

Protelion SMC Enterprise Messenger Book does not allow for exporting the user details.

Protelion SMC user data and Protelion user device data are available in the Protelion SMC GUI. Protelion SMC does not allow for exporting the user details to third-party systems and media.

- **Right to rectification**

  For a user, the right to rectification is exercised as the right to rectify the user details, user name, phone, email, organization name, department name, permissions, logon credentials, user device list, and user device names (provided that changes to the device list does not affect the connectivity). Other data cannot be rectified.

  When working in Protelion SMC Policies, an administrator can use information provided by the SMC core and Protelion SMC VPN. Rules can contain any user name. User names specified this way cannot be used as an account and are not added to the SMC core; they are only uploaded to devices as a part of the resulting policy.

- **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.

  Erasure of data subject data applies to key set, device monitoring data, and event log through rotation. Erasure of user data is performed through explicit removal of a user from the system or at removal of an organization a user belongs to.

- **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 SMC does not provide for obtaining the consent for data processing operations performed using Protelion SMC. 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 Protelion SMC, the right to object and to restrict the processing can be exercised through removal of a user from the system, provided that it does not affect the connectivity. To restrict the data processing in Protelion SMC Monitoring, you can remove a device from the module and uninstall the Protelion SMC Monitoring agent from the device.

© 2023 Protelion GmbH. All rights reserved.

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