

Product Transparency Notice

For any queries, please contact privacyteam@symantec.com

Symantec Endpoint Protection (SEP)

This Privacy Transparency Notice describes how Symantec Endpoint Protection (“Product”) collects and processes Personal Data. Its purpose is to provide You (our current or prospective “Customer”) the information You need to assess the Personal Data processing that is involved in using the Product.

1. Product Description

Symantec Endpoint Protection (SEP) is a comprehensive endpoint protection platform that is designed to stop a spectrum of traditional and next generation threats that aim to compromise the integrity of the endpoint and the data resident on it.

Further information about the Product is available at:

<https://www.symantec.com/products/endpoint-protection>

2. Personal Data Collection And Processing

Sources of Data

The Product consists of a management server and client software. The administrator supplies the data. The software uses some system information, such as IP address, in the protection of the device. In addition, the product collects data as part of its operation and submits it via telemetry to Symantec.

Respective Roles of Symantec and Customer

With respect to Personal Data submitted by the Customer to Symantec for the purposes of the Product, the Customer is the Controller, and Your Symantec contracting entity as specified in Your applicable Agreement (“Symantec”) acts as a Processor. The rights and obligations of both parties with respect to Personal Data processing are defined in the applicable Data Processing Addendum available on the [Symantec Privacy - GDPR Portal](#).

Personal Data Elements Collected and Processed, Data Subjects, Purpose of Processing

Personal Data Category	Data Subject Category	Purpose of Processing
Individual identifiers (names, Windows usernames)	Customer employees and contractors	Product management
Contact information (email address mandatory, any other data at customer admin’s discretion)	Customer employees and contractors	Notifications and password reset
Online identifiers and trackers, location data (IP and MAC addresses, device ID and location, cookies)	Customer employees and contractors	Policy determination and reporting
Network activity data (as configured by the customer: traffic data, session logs,	Customer employees and contractors	Detection of and protection against cybersecurity threats

electronic communications metadata, firewall logs)		
Communications data (as and if configured by the customer: email content)	Customer employees and contractors, customer’s other email correspondents	Customer submission of email determined as malicious for analysis by Symantec STAR*, additional security features per customer choice if used in conjunction with Symantec ATP and/or WSS.

The Product does not need and is not meant to collect or process any Special Categories of Personal Data.

Personal Data Retention Schedule

The default retention period of the data is 30 days past the last login by the user, but can be configured by the customer. For the duration of the contractual relationship with the Customer, Personal Data is retained as described in the applicable product description. After the expiry or termination of the contractual relationship, Personal Data is decommissioned except where its retention is required by applicable law, in which case Personal Data covered by such requirement will be further retained for the legally prescribed period.

3. Disclosure and International Transfer of Personal Data

Recipients of Personal Data

Symantec will send Personal Data to internal recipients (affiliated Symantec entities) and, if applicable, external recipients (third party sub-processors), in the facilitation or provision of the Product. The list of Symantec affiliated entities and their geographical locations are available on the [Symantec Privacy - GDPR Portal](#).

Third-Party Sub-Processors

No third-party sub-processor is involved in delivering the Product.

International Transfers of Personal Data

You are advised that, if necessary for service delivery or on customer instruction, Symantec and its affiliated entities will transfer Personal Data to locations outside of the European Economic Area, including potentially to external recipients, based on European Commission Decision C (2010)593 on Standard Contractual Clauses (processors), or of any alternate, legally permitted means.

4. Exercise Of Data Subject Rights

SEP itself does not gather any Personal Data that leaves the customer's environment. The data lives in an SQL database for which the customer administrator has full access. Subject to the customer’s choice, SEP may interact with SEP 14.1/Hardening*, Symantec Security Technology And Response* (STAR), Symantec Web Security Service* (WSS) and Advanced Threat Protection* (ATP).

Pursuant to the applicable Data Processing Addendum, and to the extent possible considering the nature of the processing, Symantec will assist the Customer, insofar as this is feasible, with the fulfillment of the Customer’s obligation to respond to requests for exercising Data Subjects’ rights such as the rights of access, rectification, deletion and objection laid down in Chapter III of the EU General Data Protection Regulation (GDPR).

5. Information Security

Technical and Organizational Measures

The customer is solely responsible for the security of any data collected by the product and stored in the customer's environment. Symantec has no access to it. As regards product design and any data submitted by the customer to Symantec during or pursuant to the use of the product, it is Symantec's and all its affiliated entities' commitment to implement, and contractually require all sub-processors to implement, appropriate technical and organizational measures to ensure an appropriate level of security, considering the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk for the rights and freedoms of Data Subjects. Additional security documentation is available on the [Symantec Customer Trust Portal](#).

This notice is the sole authoritative statement relating to the Personal Data processing activities associated with the use of this Product. It supersedes any prior Symantec communication or documentation relating thereto.

* For further information on the Personal Data processing involved in the use of other Symantec products referenced in this Notice, please refer to those products' Transparency Notices on the [Symantec Privacy - GDPR Portal](#).