Product Transparency Notice

For any queries, please contact privacyteam@symantec.com

Symantec Endpoint Encryption

This Privacy Transparency Notice describes how Symantec Endpoint Encryption ("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 Encryption (SEE) uses encryption to protect sensitive customer data stored on hard disks and removable media from leaking due to theft, loss, misplacement, etc. SEE does disk encryption and encryption of files on removable media, by means of client software installed locally on end users' machines, and server software to manage the clients. SEE also provides management of native OS encryption - BitLocker & FileVault.

Further information about the Product is available at:

https://www.symantec.com/products/endpoint-encryption

2. Personal Data Collection And Processing

Sources of Data

SEE is an on-premise product installed and managed by customers in their environment. All data is processed and is retained in the customer environment. Symantec does not obtain any data. SEE has a telemetry feature that must be turned on by the customer ("opt-in" feature). However there is no Personal Data in the telemetry data submitted to Symantec by customers who elect to use the telemetry feature.

Respective Roles of Symantec and Customer

The product is an on premise offering. The customer is the data controller of Personal Data collected in the course of the use of the product. The use of the product does involve Symantec as a data processor. However with respect to any Personal Data transmitted voluntarily from the Customer to Symantec for the purposes of the Product, the Customer remains the Controller, and Your Symantec contracting entity as specified in Your applicable Agreement ("Symantec") acts as a Processor. For such cases, 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), contact information (email, phone, address), financial information (payment information, banking details, financial transaction records)	Customer employees and contractors	Licensing, invoicing, sales & support

Online identifiers (usernames, passwords)	Customer employees and contractors	User authentication, helpdesk assisted recovery, server communications
Personal data contained in system information (e.g. computer OS information, product version)	Customer employees and contractors	Telemetry information such as Computer OS information and product version
Any Personal Data contained on drives / in files which the customer encrypts using the product	Any data subject whose Personal Data is contained on drives / in files which the customer encrypts using the product	Protection of information

Personal Data Retention Schedule

As the controller, the customer is solely responsible for defining and implementing the retention policies and periods applicable to Personal Data collected through the use of the product. The use of the product does not involve Symantec as a data processor.

For the duration of the contractual relationship with the Customer, Personal Data voluntarily transmitted by the customer to Symantec 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

If necessary to execute customer instructions, Symantec will send Personal Data voluntarily transmitted by the customer to internal recipients (affiliated Symantec entities) and external recipients (third party sub-processors) if necessary for 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

As the controller, the customer is solely responsible for complying with any rules applicable to the international transfers of Personal Data that the customer collects by using the product. The use of the product does not involve Symantec as a data processor.

You are however advised that if necessary to execute customer instructions, Symantec and its affiliated entities will transfer Personal Data voluntarily transmitted by the Customer to locations outside of the European Economic Area, including to external recipients, on the basis of European Commission Decision C(2010)593 on Standard Contractual Clauses (processors), or of any alternate, legally permitted means.

4. Exercise Of Data Subject Rights

The Symantec Endpoint Encryption (SEE) Product Administrator assigned by the customer can delete certain Personal Data elements. Note that all such data is retained in the customer's environment and is not available to Symantec.

However, pursuant to the applicable Data Processing Addendum if any, and to the extent possible taking into account 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

It is Symantec's and all of 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, taking into account 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.

Applicable Information Security Certifications

SEE uses FIPS 140-2 approved cryptography (cert available at https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/2377).

SEE implements NIST approved cryptographic controls to protect sensitive data (https://support.symantec.com/en_US/article.INFO2618.html).

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.

Appendix: List of offerings covered by this Notice

Endpoint Encryption