Product Transparency Notice

For any queries, please contact privacyteam@symantec.com

Symantec Encryption Desktop and Symantec Encryption Management Server

This Privacy Transparency Notice describes how Symantec Encryption Desktop and Symantec Encryption Management Server – including Gateway Email Encryption, Endpoint Encryption (PGP WDE), Desktop Email Encryption and File Share Encryption – ("Product"), collect and process 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 Encryption Management Server (SEMS) and Symantec Encryption Desktop (SED) together provide capabilities to manage and protect sensitive customer data at rest and in motion using encryption technologies.

SED allow users to use features like Whole Disk Encryption, File Share Encryption, Virtual Disk Encryption, Desktop Email Encryption and FileVault on Mac.

SEMS is used for managing various kinds of keys, users, certificates and policies for all the features.

SEMS also hosts features like Key Services, Gateway Email Protection, Web Email Protection (WEP) and Verified Key Directory (VKD).

Further information about the Product is available at:

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

2. Personal Data Collection And Processing

Sources of Data

SEMS/SED are on-premise products and installed and managed by customers in their own environment. All data is processed and is retained in the customer's environment. Symantec does not obtain any data.

The product collects data at the time of configuration, endpoint enrollment, email routing and regular communication from endpoints and external email communications. Gateway Email Encryption stores emails.

Emails are processed for enforcing policies. If emails are intended for external users and the customer-defined policy is to use Web Email Protection, then the emails for those external users are stored in the server database, so that the external users can visit the server to access their mails through a secure web interface. SEMS also synchronizes with LDAP directories, a feature used for creating consumer groups on which policies can be configured.

Respective Roles of Symantec and Customer

With respect to Personal Data collected by the product during its use, the customer is the controller. The use of the Product does not involve Symantec as a data processor.

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*, transaction records*)	Customer employees and contractors and potentially data subjects of other entities interacting with the customer	User management and reporting, license issuance and invoicing (data categories marked with an asterisk are only used for licensing and invoicing purposes)
Online identifiers (usernames, passwords and similar credentials)	Customer employees and contractors and potentially data subject of other entities interacting with customer	User management, outbound mail encryption, machine recoveries and product configuration
Communications data (metadata and contents of emails), including potentially any Personal Data, including of special categories, which may be contained in processed emails	Customer employees and contractors, data subject of other entities interacting with customer, and any data subjects whose Personal Data may be included in processed emails	Encryption of emails

Personal Data Retention Schedule

The retention period of communications data is 90 days and for other data categories it is 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 in Symantec's possession – if any at all – 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

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.

4. Exercise Of Data Subject Rights

Customer-assigned product administrators can manually update or delete all Personal Data.

Further, pursuant to the applicable Data Processing Addendum, 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

SED on Windows uses FIPS 140-2 approved cryptography (certificate available: https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/2377).

The product implements NIST approved crypto controls to protect sensitive data.

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

Desktop Email Encryption Powered by PGP Technology

Encryption Management Server Powered by PGP Technology

Endpoint Encryption / Symantec Encryption Desktop Drive Encryption (PGP WDE)

File Share Encryption Powered by PGP Technology

Gateway Email Encryption Powered by PGP Technology

Key Management Client Access and C++ API Powered by PGP Technology

Key Management Server Powered by PGP Technology

Mobile Encryption for IOS Email Management by Encryption Server Powered by PGP Technology