

# Product Transparency Notice

For any queries, please contact [privacyteam@symantec.com](mailto:privacyteam@symantec.com)

## Symantec Protection Engine (SPE) for Cloud Services (CS) & Network Attached Storage (NAS) Versions 7.9 and below

This Privacy Transparency Notice describes how Symantec Protection Engine for Cloud Services & Network Attached Storage, versions 7.9 and below (“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 Protection Engine (SPE) is an application that allows customers to incorporate malware and threat detection technologies into almost any application on Windows & Linux. SPE typically helps various applications or file storages in scanning the data at rest as well as on wire. SPE is available to customers in 2 separate SKUs: Symantec Protection Engine for Cloud Services (SPE for CS) and Symantec Protection Engine for Network Attached Storage (SPE for NAS).

SPE for CS enables customers to secure their applications/data exposed to the web. It also enables them to integrate its malware scanning capability in any application that supports scanning of files over ICAP protocol.

SPE for NAS allows customers to protect data saved, getting stored in & retrieved from NAS storages of various brands.

Standalone SPE instance comes with a (Java applet based) management which allows customers to configure & manage the same SPE instance.

For Live Update, protection Engine uses Live Update Administrator\* if configured by the customer.

Further information about the Product is available at:

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

### 2. Personal Data Collection And Processing

#### Sources of Data

SPE collects email metadata for email filtering as configured by customer-defined policy. This information is stored in SPE local logs which reside on the machine on which SPE is deployed and hosted. This hosting machine always remains in the customer's enterprise network and the information is not transferred to Symantec's backend systems, so that the customer keeps complete control over it.

SPE collects and reports to Symantec non-personal install time and runtime telemetry data of the deployed product. SPE internally integrates various security/anti-malware technologies from Symantec Security Technology and Response\* (STAR).

#### Respective Roles of Symantec and Customer

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

With respect to any Personal Data transmitted from the customer to Symantec for the purposes related to the Product (e.g. support), the customer is 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 (name) and contact information (email address)	Customer employees and contractors	User setup, service configuration
Contact information (email address)	Customer employees and contractors	Communication of security event notifications
Online identifiers and trackers (SSID of users accessing SPE logs; NAS Filer, NAS Filer Client, Client Application and VServer IP addresses and similar unique identifiers)	Customer employees and contractors, other individuals interacting in or with the customer’s environment	Security event logging and notification
Communications metadata (email address, email domain, email subject)	Customer employees and contractors, unknown persons/Others	Email-based filtering configuration

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

#### Personal Data Retention Schedule

Logs are retained for 365 day (configurable). All temporary data are cleaned before the process is stopped. Regarding any Personal Data that the customer chooses to transmit to Symantec pursuant to the use of the Product, 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

Regarding any Personal Data that the customer chooses to transmit to Symantec pursuant to the use of the Product, Symantec will send Personal Data to internal recipients (affiliated Symantec entities) and, if applicable, external recipients (third party sub-processors). 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

The customer can rectify or update the email IDs used for notification and email-based filtering.

All log files are collected and maintained on the system on which SPE is installed. These systems are running in the customer's enterprise network. Data such as log files are not sent back to Symantec automatically or without customer intervention. The customer keep full ownership of and control over these logs files, which can be deleted or cleaned up without restriction.

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

Log files are protected based on filesystem ACL. The customer is solely responsible for the security of any data collected by the product and stored in the customer's environment. 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](#).