Product Transparency Notice

For any queries, please contact privacyteam@symantec.com

Symantec Endpoint Protection Cloud (SEP Cloud)

This Privacy Transparency Notice describes how Symantec Endpoint Protection Cloud ("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 Cloud (SEP Cloud) is an easy to use security-as-a-service that protects and manages PC, Mac, mobile devices and servers from a single console.

Further information about the Product is available at:

https://www.symantec.com/products/endpoint-protection-cloud

2. Personal Data Collection And Processing

Sources of Data

Users are imported in the system via various Identity Providers or via self-enrolment. After enrolment the security agent is deployed on the system which in turn collects data and pushes it to Symantec servers.

Respective Roles of Symantec and Customer

With respect to Personal Data transmitted from 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) and contact information (email, phone, billing address)	Customer employees and contractors	User enrolment. Customers may enable SEP Cloud to sync from their Azure Active Directory
Online identifiers and trackers (IP addresses, device IDs and identifiers, session cookies)	Customer employees and contractors	Inventory processing & device enrolment
Network activity data (browsing activity, telemetry, session logs, traffic data, electronic communications metadata)	Customer employees and contractors, individuals interacting in or with the customer's environment	Security event log collection

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 data retention period is 30 days after the termination of the product contract. Event data will be purged after 90 days irrespective.

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 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

The third-party sub-processors involved in delivering the Product are:

Sub-Processor	Personal Data	Purpose of processing	Locations
Amazon Web Services (AWS)	Individual identifiers, contact information, online identifiers and trackers, network activity data	Service hosting	U.S.A.

This list is subject to change. Any planned change will be announced in advance on the Symantec Privacy - GDPR Portal. Customers can exercise their rights with respect to such changes according to the provisions of the applicable Data Processing Addendum.

International Transfers of Personal Data

Data Centers are located the U.S.A. Where 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 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

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

Personal Data is stored in encrypted form with due access control in place. 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.

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.