Product Transparency Notice

For any queries, please contact privacyteam@symantec.com

Symantec Endpoint Protection Mobile

This Privacy Transparency Notice describes how Symantec Endpoint Protection (SEP) Mobile ("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. It is to be read in conjunction with Symantec's Global Privacy Statement available on the Symantec Privacy - GDPR Portal.

1. Product Description

SEP Mobile provides a complete Mobile Threat Defense solution, protecting mobile devices from a wide range of attacks including malicious applications, network attacks, physical threats and vulnerability exploits. In cases where a threat has been identified on a specific network, the user's access to the Internet through their mobile device may be routed through Symantec VPN servers to maintain a secure connection while the threat is persistent. Symantec will not monitor or store any content that the user uploads or downloads, such as text messages, contact list, content of emails, filled-in forms, and data that a website retrieved.

Further information about the Product is available at:

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

2. Personal Data Collection And Processing

Sources of Data

Your use of SEP Mobile is dependent on you providing certain Personal Data. Only such Personal Data is required as reasonably necessary for the product to deliver its expected functionalities. SEP Mobile collects data from the user's mobile device through the SEP Mobile app, obtaining data by using operating system exposed application program interfaces (APIs) after requesting the relevant permissions from the user. In some cases, additional info is collected by integrating with the customer's Enterprise Mobility Management (EMM) systems.

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
Contact information (email address, mobile number)	Customer employees and contractors	Provide instructions for installation and setup, send service-related updates and notices, register the user to the system and associate it with their organization, administrate licenses,

		associate events with a known user to reflect the user's device health and risk status
Location data (geolocation coordinates e.g. GPS, device/network locale), subject to user permission	Customer employees and contractors	Display malicious networks near the user's location, display the location where security events occurred
Online identifiers (MAC address, unique device ID, device serial number, IMEI, username, password), device properties (OS version and model, installed applications, specific devices configurations)	Customer employees and contractors	List user's active devices, correlate devices between SEP Mobile and the customer's EMM system, log in administrators to the SEP Mobile Management Console, integrate with EMM systems. **Note**: no personal content stored in the listed applications is collected by or for SEP Mobile
Malicious network activity data (browsing activity telemetry, session logs, traffic data, electronic communications metadata)	Customer employees and contractors	Detect security incidents to which each device was exposed, especially access attempts to organizational resources to protect traffic in case of compromised device. **Note**: Symantec does not analyze or save any traffic generated by enrolled devices, except for that generated by the SEP Mobile application.
Communications data (content of SMS messages)	Customer employees and contractors	Analyze any web links to detect phishing attempts

The Product does not need and is not meant to collect or process any Special Categories of Personal Data. In particular SEP Mobile is not directed to persons under 13, and we do not knowingly collect Personal Data from children under 13. If you become aware that your child has provided us with Personal Data without your consent, please call customer support. We will take steps to remove the information and to terminate the child's account.

Personal Data Retention Schedule

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)	Contact information, location data, online identifiers, network activity data, communication data	Store data, run the SEP Mobile web application which analyzes the data	U.S.A.
Engine Yard	Contact information, location data, online identifiers, network activity data, communication data	Platform services for running the SEP Mobile web application	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

You are advised that Symantec and its affiliated entities will transfer Personal Data 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

Anonymization of the data is possible by removing the application from the device, terminating the service with SEP Mobile, or causing 30 days of inactivity, subject to any time extension requested by the Customer. It is possible to receive/correct data stored on a specific user by issuing a support request.

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

Symantec secures stored information by use of encryption. Encryption is the industry standard (AES256). All endpoint communication is performed over TLS. A two-factor authentication process is required for accessing users' data. Access to user data is restricted to a small number of Symantec employees, including selected R&D team members as well as support and operations teams.

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.