Product Transparency Notice

For any queries, please contact privacyteam@symantec.com

Symantec Endpoint Protection Small Business Edition (SEP SBE)

This Privacy Transparency Notice describes how Symantec Endpoint Protection Small Business Edition (SEP SBE) ("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

SEP SBE is an endpoint security product that is centrally managed through a web interface. We use NIS and SEP* agents to protect endpoint computers and we allow admins and users to sign into a web portal to manage and view the company's agents. For Mac computers we use an unmanaged version of Norton For Mac (NFM). Events, reports, alerts, policy are handled through server-side services managed by Symantec.

Further information about the Product is available at:

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

2. Personal Data Collection And Processing

Sources of Data

The data collected by SEP SBE is obtained from the customer through the creation of a company account, the creation of user accounts and the installation of the endpoint software.

Purchase or trial of the service requires a contact name, email, company name and address. The payment information is not handled or stored by the service.

A user of the service must provide a name, email and phone number. We collect basic telemetry around product usage, diagnostics and portal login activity.

Installation of the endpoint software by the customer provides data such as computer name, OS, IP address, system manufacturer and model, and endpoint protection software information, such as current security settings, scan results, virus and risk detection, product version and last connection date.

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 and company identifiers (names) and	Customer employees and contractors	User account creation, portal login, alerting.

contact information (email, phone number, address)		
Online identifiers and trackers (IP and MAC address, computer name, session cookie)	Customer employees and contractors	Endpoint software management, portal login and session tracking
Network activity data (browsing activity, session logs, proxy information at the customer's discretion, traffic data)	Customer employees and contractors, individuals interacting in or with the customer's environment	Portal login and session tracking, online and network security event logging
Communications data (content of electronic communications, web form entries)	Customer employees and contractors	Support and feedback

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

Personal Data Retention Schedule

Network activity data is retained for 90 days and event data for 13 months. 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, if applicable, 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

No third-party sub-processor is involved in delivering the Product.

International Transfers of Personal Data

Data is stored in a Symantec data center in Tucson, Arizona, U.S.A. It can be remotely accessed by engineering and support teams in the U.S.A, Canada, the UK and India. You are advised that, Symantec and its affiliated entities will transfer Personal Data to locations outside of the European Economic Area, including potentially 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 customer call obtain from customer care or support the update of their primary customer information, and after service cancellation, data deletion can also be requested. Users can log into the SEP SBE portal to change or delete their name, email address and phone number.

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

Access to customer data is strictly controlled through the operations team for direct access. Support tools are only accessible through clearly defined roles; data access and tools are only available on the Symantec VPN. No financial information is stored by the service and authentication is handled by Norton Secure Login.

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.

* 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.