Product Transparency Notice

For any queries, please contact privacyteam@symantec.com

Web Security Service

This Privacy Transparency Notice describes how Web Security Service ("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 involved in using the Product.

1. Product Description

Web Security Service (WSS) is a cloud delivered Secure Web Gateway service providing customers a comprehensive integration of many Symantec Network Protection Products via a multi-tenant, distributed infrastructure. Administrative users configure the services via a hosted management portal and/or APIs. End-Users have their Internet web-browsing and other traffic directed through Web Security Service. This End-User traffic is subject to the inspection, control and logging while within Web Security Service. The transactional log data generated for End-User traffic is then stored and available for reporting retrieval by administrative users via the Web Security Service management portal and APIs.

Further information about the Product is available at:

https://www.symantec.com/products/cloud-delivered-web-security-services

2. Personal Data Collection And Processing

Sources of Data

Administrators use an email address as a login name and can provide name, address, and telephone. As part of the service configurations administrators may input End-User usernames. End-User transaction logs are generated during traffic proxying. In certain deployments additional data regarding the device used to access Web Security Service (laptop or mobile) may be captured. If configured Web Security Service can integrate to Data Loss Prevention* (DLP) tools. Both the customer's own DLP servers and Symantec's Data Loss Prevention cloud service are supported. DLP analysis applies to the End-User requests and upload data.

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 (name), contact information (email, phone, address)	Customer employees and contractors	Email: mandatory for account setup and login, and optional for notification of detections if advanced malware sandboxing is used. Note: administrator name, as well as phone and address are not necessary for the product

		to function, but required for software downloads to complete export compliance checks
Online identifiers and trackers (end-user source IP address, username, device ID), location data (country-level end-user location)	Customer employees and contractors, other individuals interacting in the customer's environment	Transactional logging and audit
Network activity data (browsing activity, session data) electronic communications data (metadata, content)	Customer employees and contractors	Web Security Service access control and reporting, and, if applicable, data loss prevention and advanced malware sandboxing

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

Personal Data Retention Schedule

Administration individual identifiers and contact information are retained for the duration of the subscription. The retention of location data, online identifiers and trackers and network activity data is defined per-license. The service includes features to permit customers to control the content of the transactional logs at creation, removing identifiers based on various trigger conditions. Transactional log data is at most stored for 1 year. Communication data subject to data loss prevention is not retained. Sample files processed for advanced malware sandboxing are deleted after detonation by clean-up process as storage space is required.

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	Administrative data: configuration portal and associated email notification	U.S.A
Synapsis	Contact information, online identifiers and trackers, network	Customer support services	Uruguay

	activity data, location data		

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 will be transferred or accessed (including for storage, backup and archiving) to the U.S.A. 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

Administrators can amend, rectify, or delete any information regarding their administrative portal login – except the login ID (an email address) itself. Other administrators of the same customer can delete admin accounts (removing the email address). Administrators can remove End-User usernames from configuration. After generation there are is no support for modifications of the End-User transactional logs.

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

ISO27001 and SSAE16 SOC3

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.