Product Transparency Notice

For any queries, please contact privacyteam@symantec.com

Managed Security Services (MSS)

This Privacy Transparency Notice describes how Managed Security Services ("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 Managed Security Services (MSS) extends an organization's internal security operations program by expertly monitoring the environment 24x7 and applying global threat intelligence to detect advanced attacks. Symantec MSS complements the infrastructure already in place and helps security leaders to improve their security operations program and better manage their organizations' security posture before, during, and after an attack.

Further information about the Product is available at:

https://www.symantec.com/services/cyber-security-services/managed-security-services

2. Personal Data Collection And Processing

Sources of Data

All customer logs are transported securely to the MSS Security Operations Center (SOC) Data Center. Symantec MSS gathers security logs from customer security devices via our proprietary Log Collection Platform (LCP). The LCP securely and efficiently collects, compresses and securely (via SSL or VPN) delivers event logs to Symantec MSS Data Center for storage, analysis, and correlation. MSS does share de-identified (where possible anonymized, and otherwise pseudonymized) information with the Symantec Global Threat Network (GIN).

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 and Characteristics (Names)	Customer's employees, contractors, clients, suppliers, other business contacts, as well as other persons interacting electronically in or with the customer's networks	Such data is necessary to identify authorized customer personnel, and may also be included in security logs transmitted by the customer to MSS for the purpose of environment monitoring.
Contact Information (business email address, corporate	Customer's employees and contractors, as well as potentially clients, suppliers,	To be able to contact the person if and where

phone number, business mailing address)	other business contacts and other persons interacting electronically in or with the customer's networks	necessary for the effective delivery of the service
Location data (device and network locale), online identifiers and trackers, network activity data	Customer's employees, contractors, clients, suppliers, other business contacts, as well as other persons interacting electronically in or with the customer's networks	Such data is part of network diagrams and can be part of the security logs transmitted by the customer to MSS for the purpose of environment monitoring.
Communications data	Customer's employees, contractors	Such data is collected to record the customer's portal activity, such as when the customer uses the chat feature, opens a service case, or uses any of the features of the portal.

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

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)	Individual identifiers and characteristics, contact information, location data, online identifiers and trackers, network activity data	Data is encrypted and not accessible to the third party provider	U.S.A
Digital Realty (formerly DuPont Fabros Technology)	Individual identifiers and characteristics, contact information, location data, online identifiers	Data is not accessible to the third party provider	U.S.A

	and trackers, network activity data		
Iron Mountain	Individual identifiers and characteristics, contact information, location data, online identifiers and trackers, network activity data	Data is not accessible to the third party provider and a secure storage of backup media is in place for the MSS environment	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 will be transferred or accessed (including for storage, backup and archiving) in 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, 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

In the MSS portal customer employees with the administrator role assigned can create, edit or delete their employees' information. They can also contact their Symantec MSS team to edit their information for them. Information gathered in the course of provisioning, setup, and configuration of the services is not and cannot be mined for Personal Data.

As regards Personal Data which are part of security logs for the purpose of environment monitoring, customers may transmit such logs to MSS on the basis of their legitimate interest in collecting and processing Personal Data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security. Network and information security means the ability of a network or of an information system to resist events, attacks or unlawful or malicious actions that could compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data, or the security of the related services offered by, or accessible via those networks. In the interest of the customer's own system compliance and security, it is indispensable to preserve the integrity of such security logs. Consequently keeping them unedited and un-editable is critical to the protection of the customer's network and information security. Therefore Symantec takes specific information security measures as detailed below to ensure that Personal Data in MSS customer security logs is securely transported, processed and stored.

Further, pursuant to the applicable Data Processing Addendum, and to the extent possible considering the nature of the processing (in particular as regards security logs as explained above), 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

MSS pursues, holds and maintains the following information security certifications, audits and practices:

- Annual SOC 1 Type II Audit
- Annual PCI Audit
- Annual ISO 27001 Audit
- Penetration Tests for every major release or twice a year, conducted by Symantec's internal penetration testing team as well as top penetration testing companies

For the performance of Managed Endpoint Detection and Response services, MSS uses a tool supplied by a separate business unit within Symantec, therefore such tool is out of the scope of the aforementioned audits.

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.