Product Transparency Notice

For any queries, please contact privacyteam@symantec.com

Enterprise Global Technical Support

This Privacy Transparency Notice describes how Enterprise Global Technical Support ("Service") 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 Service.

1. Product Description

Technical Support is available for all Symantec enterprise products & service offerings other than Managed Security Services (MSS)* which have a separate dedicated support function.

Further information about the Product is available at:

https://support.symantec.com/en_US.html

2. Personal Data Collection And Processing

Sources of Data

Customer data processed by Technical Support for case management purposes is collected from Symantec's SalesForce.com (SFDC) customer database for case management. Customer logs and telemetry processed for the purpose of case work are collected from the customer via Symantec's MFT secure file transfer system. Relevant case data will be shared with Symantec's internal ticketing and case handling systems such as JIRA and Cachezilla, notably for the purposes of raising bug fixes and enhancement requests to Symantec's Development team. Similarly, case information on threat intelligence will be shared with Symantec Security Technology And Response (STAR)* for the purposes of improving threat capture rates and reducing false positives.

Respective Roles of Symantec and Customer

With respect to Personal Data transmitted from the Customer to Symantec for the purposes of the Service, 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
Depending on what is submitted by the customer and relevant to the case: • Individual and online identifiers • Contact information • Device, system, network location data • Network activity data • Communications metadata and content	Depending on what is submitted by the customer and relevant to the case: • Customer employees and contractors • Customer clients and suppliers • Other individuals inter-acting with or operating in the customer systems concerned	Delivery of technical assistance, troubleshooting and other support services as requested by the customer

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

Personal Data Retention Schedule

Customer logs and telemetry in the MFT system are archived 30 days after case closure, stored for 2 years from collection, and then deleted. Customer call recordings, if any, are stored for 60 days before being purged.

Customer relations data in Symantec's SFDC customer database is retained for the duration of the customer's contractual relationship with Symantec. Identifiable data elements such as contact information can however be removed at any time upon Customer request. 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), as necessary for the facilitation or provision of the Service. 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 Service are:

Sub-Processor	Personal Data	Purpose of processing	Locations
Concentrix	Individual and online identifiers and characteristics, location data, network activity data, communications metadata and content	Delivery of technical support services	U.S.A., India, Costa Rica
NICE	Voice communications metadata and content	Storage of customer call recordings, if any	Depending on the location where the call is logged: Brazil, Canada, Estonia, India, Ireland, Japan, Singapore, Thailand, U.K., U.S.A.
Salesforce.com	Contact information, communications metadata and content	Storage of support case logs and records	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

Symantec can delete customer data on valid request from the customer if and as appropriate. To ensure that no data is unduly disclosed, accessed or erased, and that the integrity and availability of case-critical data is not altered or compromised, such requests will be processed manually by Symantec and cannot be executed directly by the customer.

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 limited to members of Symantec Technical Support worldwide, and to Concentrix for the services that this sub-processor supports. All customer data, logs and telemetry in SFDC and MFT are encrypted at rest. Access to both systems requires two factor authentication. All staff concerned follow the regular privacy and security trainings mandated by Symantec's Global Privacy Office and Global Security Office.

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.