Product Transparency Notice

For any queries, please contact privacyteam@symantec.com

Symantec Endpoint Protection Mobile*: Symantec Mobile App Defense

This Privacy Transparency Notice describes how the Symantec Mobile App Defense product ("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 Service. It is to be read in conjunction with Symantec's Global Privacy Statement available on the Symantec Privacy - GDPR Portal.

1. Service Description

Symantec Mobile App Defense provides customers with an SDK toolkit designed to enable developers to embed security in their mobile applications ("Customer Applications") by natively leveraging Symantec Endpoint Protection Mobile* threat protection technology. The service also provides customers visibility into security incidents that take place within those applications.

Further information about the Service is available at:

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

2. Personal Data Collection And Processing

Sources of Data

The Service API collects device ID from the Customer Application.

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
Device ID	Customer Application users	Device identification

The Service 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 Service 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 Service. The list and locations of Symantec affiliated entities 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
Amazon Web Services (AWS)	Device ID	Hosted storage	U.S.A., Germany (Customer will be provisioned from the closest location)

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

Customers in the EMEA region will be provisioned from the EU-based data center indicated above, thus Symantec will not transfer EU personal data out of the EU unless instructed to do so by the Customer. In such circumstances, 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

The collection of device location data by the Service is subject to prior end-user opt-in. The data transmitted to Symantec in the context of the use of the Service are not processed by Symantec in any way or for any purpose that requires or involves the identification of the user. Data subject rights are thus unlikely to apply to it. Nevertheless, 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 feasible, with the fulfillment of the Customer's obligation to respond to requests for exercising Data Subjects' rights (such as 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 and all of its affiliated entities 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 Service.

* For further information on the Personal Data processing involved in the use of other Symantec Products or Services referenced in this Notice, please refer to those Products' or Services' Transparency Notices on the Symantec Privacy - GDPR Portal.