Product Transparency Notice

For any queries, please contact privacyteam@symantec.com

Secure Access Cloud

This Privacy Transparency Notice describes how Secure Access Cloud ("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

Secure Access Cloud provides application-level access of authorized personnel to corporate resources. It allows users to access any application from any device in any location, regardless of the underlying infrastructure. The Service can grant granular access to specific applications, with specific times and circumstances, to both internal users and third parties. Automation and rules engines will enforce policy, improve performance, and help block fraudulent access attempts.

Further information about the Product is available at:

https://www.symantec.com/products/secure-access-cloud

2. Personal Data Collection And Processing

Sources of Data

Personal data for the purposes of the Service is collected from the Customer, including direct submissions by administrators and end-users, as well as collection from their devices as and when necessary for Service delivery.

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
General identifiers and credentials (user names, corporate email addresses, passwords)	Customer administrators and end-users	Identification of and service communication with admins and user, authentication and access to resources
Device information (operating system and browser version) network and online activity trackers (IP addresses and session IDs)	Customer administrators and end-users	Service delivery and logging

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

If and as necessary, 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 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
Amazon Web Services (AWS)	General identifiers and credentials, device information, network and online activity identifiers	Service hosting, provisioning, logging and backup	U.S.A., EU (Ireland)
Microsoft Azure			
Auth0	General identifiers and credentials	Identity platform provision	U.S.A., EU (Ireland, failover: Germany)
SalesForce	Support case data as and when submitted by Customer	Service Support	U.S.A., European Economic Area
Atlassian StatusPage	General identifiers and credentials	Maintenance and service status notifications	U.S.A., EU (Ireland)

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

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

ISO 27001, SOC 2 TYPE II, PCI-DSS (documentation available on request)

This notice is the sole authoritative statement relating to the Personal Data processing activities associated with the use of this Service. It supersedes any prior Symantec communication or documentation relating thereto.