Product Transparency Notice

For any queries, please contact privacyteam@symantec.com

Control Compliance Suite (CCS)

This Privacy Transparency Notice describes how Control Compliance Suite (CCS) ("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

Control Compliance Suite enables automation of IT assessments with best-in-class, pre-packaged content for servers, applications, databases, network devices, endpoints, and cloud from a single console based on security configuration, technical procedures, or third-party controls. It also enables identifying misconfigurations and prioritizing remediation.

Further information about the Product is available at:

https://www.symantec.com/products/control-compliance-suite

2. Personal Data Collection And Processing

Sources of Data

Control Compliance Suite collects data from various IT assets programmatically, either by remotely connecting to the asset via network or through an agent that is pre-installed on the asset.

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 (names) and contact information (email address, phone number)	Customer's employees, contractors and potentially clients	To manage users and role based access control
Online identifiers and trackers (IP addresses, usernames, passwords and similar tokens, device IDs and similar unique identifiers, cookies and other user and device trackers, product settings)	Customer employees, contractors, clients, suppliers and other business contacts	To perform technical security assessments
Network activity data (browsing activity, telemetry, usage data, session logs,	Customer employees, contractors, clients, suppliers and other business contacts	To perform technical security assessments, logging and troubleshooting

traffic data, electronic communications metadata)		

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

Personal Data Retention Schedule

Personal Data is retained until removed by the Customer. Authorized users' individual identifiers and contact information are retained as long as the user is a valid employee, is present in the relevant Active Directory, or until the email address is disabled by the Customer.

For the duration of the contractual relationship with the Customer, other 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
Service Now	Online identifiers and trackers	To auto-remediate failed security configuration checks (optional, per Customer's configuration)	Depends on the region selected by the Customer for deployment
Amazon (AWS)	Online identifiers and trackers, contact information	To securely host the Product's process data (optional, per Customer's configuration)	Depends on the region selected by the Customer for deployment
CyberArc	Online identifiers and trackers	To validate user passwords for technical security assessments (optional, per Customer's configuration)	Depends on the region selected by the Customer for deployment
RSA Archer	Online identifiers and trackers	To leverage the out-of-the-box compliance and risk reports provided by Archer (optional, per	Depends on the region selected by the Customer for deployment

		Customer's configuration)	

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 locations that depend on the region selected by the Customer for deployment. You are advised that where necessary to meet the Customer's configuration settings, 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

Pursuant to the applicable Data Processing Addendum, and to the extent possible considering 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 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, considering 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.