Product Transparency Notice

For any queries, please contact privacyteam@symantec.com

Data Loss Prevention - Cloud Service

This Privacy Transparency Notice describes how Data Loss Prevention - Cloud Service ("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. The list of offerings covered by this notice is in appendix.

1. Product Description

Symantec DLP Cloud Service for Email extends Data Loss Prevention capabilities to Microsoft O365 and Gmail for our Customers. Symantec DLP Cloud Service integrates with Symantec CASB, extends Data Loss Prevention capabilities to about 60 cloud applications including Box, DropBox, and Office 365. Symantec DLP Cloud Console is the central management console that the customer can use to define, deploy, and enforce data loss prevention policies for Data Loss Prevention Cloud Service for Email.

Further information about the Product is available at:

https://www.symantec.com/products/data-loss-prevention-cloud-email

https://www.symantec.com/products/data-loss-prevention-casb

2. Personal Data Collection And Processing

Sources of Data

Data Loss Prevention Cloud Services collect and process Personal Data comes from cloud applications managed and deployed by the customer. Personal Data may be transmitted to Symantec when the customer is using the cloud-based application to leverage DLP's inspection monitoring and redaction capabilities. This depends on how the customer configures their policies in the Data Loss Prevention – Cloud Service Application.

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, online identifiers and trackers, network activity data, communications data	Customer employees, contractors, visitors and other business contacts who conduct network-based communications in or from the customer's protected environment	To detect and enable the investigation of mishandlings of confidential information, and of other violations of customer-defined policies
Any categories of Personal Data, potentially including	Customer employees and contractors and any other	To protect, and prevent the loss, exfiltration of theft of

Special Categories, which the customer configures to protect in its policies	individuals whose personal data is protected by the customer's DLP policies	confidential information which the customer's DLP policy definitions mark as protected
Location data (device/network locale)	Customer employees and contractors	To provision the service in geographically closest data center for low latency
Online identifiers and trackers, network activity data (IP addresses and other device identifiers, cookies and other device trackers, product settings, traffic telemetry), communications data	Customer employees and contractors	To perform traffic monitoring, forensics, service administration, product improvement and proof of concept provisioning forms

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)	Customer employees, contractors, visitors and other business contacts who conduct network-based communications in or from the customer's protected environment	To provide secure Cloud Service Infrastructure (IaaS)	Global

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

DLP Cloud Service implements U.S. NIST-approved cryptographic controls to protect confidential data. 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.

Appendix: List of offerings covered by this Notice

CloudSOC CASB for SaaS E10 with DLP Cloud Detection Service
CloudSOC CASB for SaaS E20 with DLP Cloud Detection Service
CloudSOC CASB Gateway All E30 with DLP Cloud Detection Service
Data Loss Prevention Cloud Detection Service
Data Loss Prevention Cloud Detection Service for WSS Addon
Data Loss Prevention Cloud Detection Service Non Production Sandbox Option
Data Loss Prevention Cloud Service Email Standalone
Data Loss Prevention Cloud Service Email Standalone Non Production Sandbox Option
Data Loss Prevention Cloud Service Email Standalone with Cloud Console
Data Loss Prevention Cloud Service Email with Email Safeguard
Data Loss Prevention Cloud Service Email with Email Safeguard Non-Production Sandbox Option
Data Loss Prevention Cloud Service Email with Email Safeguard with Cloud Console