Product Transparency Notice

For any queries, please contact privacyteam@symantec.com

Symantec Email Security.cloud

This Privacy Transparency Notice describes how Symantec Email Security.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. Service Description

Symantec Email Security.cloud is a complete email security solution that safeguards cloud email such as Office 365 and G Suite and on-premises email such as Microsoft Exchange. It blocks new and sophisticated email threats such as ransomware, spear phishing, and business email compromise. Email Security.cloud repels spear phishing attacks with comprehensive defense that includes protection, isolation, visibility, and user awareness. It also accelerates attack response with analytics that provide the deepest visibility into targeted attack campaigns.

Further information about the Service is available at:

https://www.symantec.com/products/email-security-cloud

2. Personal Data Collection And Processing

Sources of Data

The customer routes their email to Symantec's .cloud infrastructure. Symantec scans the email to evaluate whether the email is suspected spam, suspected malware or clean. Clean emails pass through and get delivered to the intended recipient. Suspected spam and suspected malware are diverted into quarantine in Symantec's Data Centers. Quarantined email can be retrieved by the customer's administrator or by the users, depending on customer-selected configuration options. Alternatively, the customer can also choose spam emails to be dropped rather than quarantined. In that case suspected spam emails are not stored in Symantec's systems.

Symantec collects email metadata and the results of customer directed screening. Such data is stored in the central database in the Management System where the customer's administrator can perform various analyses and produce reports.

Data is stored for customers to run reports on it, and is also available to customer support engineers for triage of incidents, performance management and problem resolution.

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
Email addresses	Customer administrators	Service configuration
Network activity logs	Customer administrators	Service usage tracking

Metadata (header) and content (body, attachments) of emails routed to the service by the customer, and any personal data submitted by the customer for directed screening purposes	Senders and recipients of email routed to the service by the customer	Security scanning, spam and malware detection and quarantine, threat analysis and reporting.

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

Personal Data Retention Schedule

Suspected spam in quarantine is stored for 14 days, unless the customer configures the service to drop the email rather than to store it in quarantine.

Suspected malware in quarantine is stored for 30 days.

Email metadata and the results of customer directed screening are stored in the central database in the Management System for 30 days, and deleted on a rolling basis as they reach their expiration date, unless the customer configures the service not to store the results of directed screening.

Customer configuration data is stored for 6 months after service termination, to facilitate service resumption if the customer chooses to return.

Network activity logs are stored for 1 year to facilitate service usage traceability and potential dispute resolution.

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 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)	Suspected spam and malware in quarantine, email metadata and the results of customer directed screening	Secure hosting. Data is encrypted and not shared with AWS	Germany Ireland
Echoworx (optional add-on the customer may subscribe to)	Email metadata and content	Encryption	UK / U.S.A. (configurable)
Interxion Data Centers	Email metadata and the results of customer directed screening	Hosting. Data is not encrypted	Netherlands
Virtus Data Centers	Email metadata and the results of	Hosting. Data is not encrypted	UK

	customer directed screening		
Zix (optional add-on the customer may subscribe to)	Email metadata and content	Encryption	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

Based on contractual arrangements with the customer, the processing of personal data collected for the purposes of service configuration and usage tracking can be provisioned from locations in the European Economic Area or in North America. You are advised that where necessary to deliver the service in line with the contractual arrangements between Symantec and the customer, Symantec and its affiliated entities will transfer Personal Data from the European Economic Area to locations outside of that Area, potentially 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

Data erasure happens on a rolling daily basis. Customers can choose to make data invisible to themselves, without however taking it off from Symantec's systems before their expiry date. Customers can also change certain configuration settings so that data related to customer directed screenings is not collected, nor retained.

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

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 certification. Relevant documentation and topic-specific explanations of applicable security controls can be provided to customers upon 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.