Product Transparency Notice

For any queries, please contact privacyteam@symantec.com

Information Centric Encryption

This Privacy Transparency Notice describes how Information Centric Encryption ("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

The Symantec Information Centric Encryption (ICE) Service enables customers to encrypt, track and revoke sensitive documents. Features include:

(1) Tracking sensitive files that have been encrypted and shared with internal or external users;

(2) Enabling permission sets (such as edit, print and offline access) for sensitive documents;

(3) Providing access to information for employees and third party recipients;

(4) Revoking access to shared data.

The customer can access the Information Centric Encryption administrative console by using a secure password-protected login. The ICE administrative console provides the ability for the customer to configure and manage the service, access telemetry, and view statistics when available as part of the service. The service is managed on a twenty-four (24) hours/day by seven (7) days/week basis and is monitored for hardware availability, service capacity and network resource utilization. The service is regularly monitored for service level compliance and adjustments are made as needed.

Further information about the Product is available at:

https://www.symantec.com/products/information-centric-security

2. Personal Data Collection And Processing

Sources of Data

Data is collected as administrators create policies and as end-users decrypt documents. The data is entered in by users and is obtained by Symantec as the information is transmitted to the ICE Cloud Service.

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
Corporate contact information (name, email, phone, address) and	Customer employees and contractors	Licensing and invoicing

corporate location data (country locale)		
Individual identifiers (names, usernames, passwords), contact information (email)	Customer employees and contractors, business contacts and other third party individuals who interact with documents that the customer protects through the product	Identification of users to provide access policies and to audit documents
Any Personal Data contained on drives / in files which the customer encrypts using the product	Any data subject whose Personal Data is contained on drives / in files which the customer encrypts using the product	Protection of information
Online identifiers and trackers (IP addresses, hots/usernames, device IDs and similar)	Customer employees and contractors	Traffic monitoring, forensics, service administration
Communications data (email and webform metadata and contents)	Customer employees and contractors	Proof of concept and 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 and contractors, business contacts and other third party individuals who interact with documents that the customer	Infrastructure as a Service hosting the ICE Cloud Service	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

The product-specific controls implemented include strict AWS access controls for Symantec employees, IP restrictions only allowing connections from Symantec egress IP addresses and AWS RDS Encryption.

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

Information Centric Encryption

Information Centric Security Module