Product Transparency Notice

For any queries, please contact privacyteam@symantec.com

Incident Response

This Privacy Transparency Notice describes how Incident Response ("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

Symantec's Incident Response team partners with customers to prepare for and respond to cyber-attacks. Symantec's combination of readiness and response services empower organizations to react decisively and effectively when a security incident occurs and reduce overall impact and recurrence of incidents.

Further information about the Product is available at:

https://www.symantec.com/services/cyber-security-services/incident-response

2. Personal Data Collection And Processing

Sources of Data

The Symantec Incident Response (IR) service collects data from Customer representatives to identify a Customer point of contact, work location, and information regarding the Customer's corporate network. Additionally, log data and device digital forensic data are acquired from the Customer, either provided by the Customer via secure file share or in person, or obtained physically from the Customer's devices.

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 Characteristics (e.g. dates of birth, employment and education titles, or other personal attributes potentially contained in artifacts subject to incident investigation)	Employees, contractors of Customer, as well as Customer's clients, vendors, prospects, and any other business partners interacting with Customer through the networks concerned	Individual identifiers such as names are necessary to identify personnel authorized to use the service. Personal Data may also be gathered as part of incident investigation. Such information is only used if relevant to the investigation, and otherwise ignored.

Contact Information (e.g. email address, phone number, address, emergency or backup contact)	Employees, contractors of Customer, as well as Customer's clients, vendors, prospects, and any other business partners interacting with Customer through the networks concerned	Contact information is necessary to identify personnel authorized to use the service. Personal Data may also be gathered as part of incident investigation. Such information is only used if relevant to the investigation, and otherwise ignored.
Financial Information potentially contained in artifacts subject to incident investigation	Customer's employees, contractors, clients, vendors and other electronic correspondents	Such Personal Data may be gathered as part of incident investigations but will only be used if relevant to the investigation, and will otherwise be ignored.
Location Data, Online Identifiers and Trackers, Network Activity Data	Customer employees and contractors	Such Personal Data may be gathered as part of incident investigations but will only be used if relevant to the investigation, and will otherwise be ignored.
Communications Data	Employees, contractors of Customer, as well as Customer's clients, vendors, prospects, and any other business partners interacting with Customer through the networks concerned	Communications Data may be gathered as part of incident investigations but will only be used if relevant to the investigation, and will otherwise be ignored.
Special Categories of Data potentially contained in artifacts subject to incident investigation	Employees, contractors of Customer, as well as Customer's clients, vendors, prospects, and any other business partners interacting with Customer through the networks concerned	Such Personal Data may be gathered as part of incident investigations but will only be used if relevant to the investigation, and will otherwise be ignored.

Personal Data Retention Schedule

By default, Personal Data gathered for the purpose of incident investigation is kept for 3 months after the conclusion of the investigation. 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 necessary to meet record keeping obligations, or required by applicable law, in which case Personal Data covered by such requirement will be further retained for the lawfully 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)	Online identifiers and trackers, as well as network activity data of customer's employees and contractors	Digital forensic processing of system data	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

Data will be transferred or accessed (including for storage, backup and archiving) globally.

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, 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

The contact information collected can be provided to the data owner upon request, and any errors rectified by the IR Project Managers or other designees within the IR teams, any evidentiary data collected during IR investigations cannot be altered.

Further, 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

Symantec secures information by use of encryption for sensitive information. Encryption is the industry standard (AES256). As contractually stipulated, any client information pertaining specifically to an Incident Response engagement will only be accessed and used by the Incident Response team working on the case, and to the extent necessary by other authorized personnel of the Cyber Security Services teams whose assistance with the investigation is required.

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.