Privacy Transparency Notice

For any queries, please contact privacyteam@symantec.com

Security Technology and Response (STAR)

This Privacy Transparency Notice describes how Symantec's Security Technology and Response (STAR) division 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 Symantec Products that leverage the capabilities enabled in Symantec enterprise and consumer products by the STAR applied research and technology development organization.

1. Product Description

Symantec's Security Technology and Response (STAR) division is a global team of security engineers, virus hunters, threat analysts, and researchers that provides the underlying security technology, content, and support for all Symantec corporate and consumer security products. The group is Symantec's eyes and ears when it comes to monitoring and keeping a finger on the pulse of the Internet security threat landscape. STAR's anti-malware security technologies break down into four categories: File-based Protection, Network-based Protection, Behavior-based Protection, Reputation-based Protection.

One of the key capabilities of STAR available to customers is Symantec's proprietary Cynic malware analysis service. Cynic is a cloud hosted world leading sandbox. Taking receipt of unknown files and applications submitted by customers, Cynic uses dynamic threat detection, file reputation, context intelligence, and network traffic analysis to evaluate whether the submitted file or application is clean or malicious. The result of this evaluation and contextual information around it are returned to the submitting customer.

The knowledge acquired by Symantec's security sensors and STAR researchers has great value not only in developing innovative security technology, but also for informing computer users on threat trends and security best practices.

Further information about the Product is available at:

Overview of technologies deployed in Symantec products:
https://www.symantec.com/en/aa/theme/star

Landscape analysis and threat information:
https://www.symantec.com/security-center/threat-report

2. Personal Data Collection And Processing

Sources of Data

With response centers located throughout the world, STAR monitors malicious code reports from systems and network sensors in 200+ countries and to track 25,000+ vulnerabilities affecting more 55,000+ technologies from 8,000+ vendors. The team uses this vast intelligence to develop and deliver the world's most comprehensive security protection.

Personal Data Elements Collected and Processed, Data Subjects, Purpose of Processing

Personal Data Category	Data Subject Category	Purpose Of Processing
Personal identifiers, professional roles and titles,	Customer employees / contractors / agents	Service setup, administration, provisioning and delivery, including responding to

physical location information and contact information		customer support inquiries, investigations and requests
Personal Data, if any, that may be contained in threat telemetry collected by STAR, including device location, online identifiers and trackers, network activity logs and electronic communications metadata and content	Data subjects acting in or interacting with the networks and systems in which the Customer uses Symantec Products leveraging STAR capabilities	Detection and analysis of cyberthreats and improvement of protection
Personal Data, if any, that may be contained in files or applications submitted by customers of relevant Symantec Products to the Cynic malware analysis service	Unknown data subjects, if any, whose identity Cynic neither can, nor needs to determine	Sandboxed execution and analysis of files and applications submitted by customers for the purpose of malware detection

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

Personal Data Retention Schedule

Threat intelligence data:

Raw threat telemetry in the inbound queue is kept for 2 days. Processed threat telemetry data is first stored in 'hot tables' for 7 days, and then for 3 years in 'cold tables'. Backups of processed telemetry are kept for 3 years, and backups of raw telemetry are kept for 5 years. Deletion of expired data happens automatically on a daily basis in each of these five repositories.

Cynic malware analysis data:

Customers can submit a data retention policy along with their submitted file or application, which will govern what Symantec can do with that file or application and with the intelligence generated as a result of its execution.

- Malicious files can be retained within Cynic for a maximum of 30 days.
- Files that Cynic deems to be of interest or of a suspicious nature can be retained for up to 7 days.
- Files that are deemed clean are removed immediately.

Additionally, the following policy options are available for customers to apply to any submitted file or application after its analysis is complete:

- Any intelligence driven through the execution of the submitted file or application will only benefit the submitter. The file or application itself and the intelligence driven from its execution will be deleted after the analysis is completed and the evaluation provided.
- Any intelligence driven through the execution of the submitted file or application will benefit all users of Cynic within the region where the file or application has been processed.
- Any intelligence driven through the execution of the submitted file or application will benefit all users of Cynic globally, but the file or application will still be retained within the submitting region.

Product-specific retention schedules independent from STAR and Cynic:

For the duration of the contractual relationship with the Customer using any specific Symantec Product leveraging STAR's capabilities, Personal Data is retained as described in the applicable product description(s). After the expiry or termination of the contractual relationship and where the purpose for which the Personal Data was collected is no longer current, 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)	Residual personal data that may remain in threat telemetry	Improve protection and advanced security analytics	U.S. / EU
Microsoft Azure	Residual personal data that may remain in threat telemetry	Improve protection and advanced security analytics	U.S. / EU

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

For the purposes of STAR, Symantec and its affiliated entities will transfer Personal Data contained in threat telemetry 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

STAR only processes any residual Personal Data that may remain in aggregated threat telemetry in ways and for purposes that do not require the identification of any data subject. Nevertheless, requests to exercise data subject rights in relation to Personal Data processed by STAR may be submitted through the customer care processes applicable to the specific Symantec Products used by the Customer. If the customer provides additional information that enables STAR to attribute an element of aggregated threat telemetry to the particular customer, then STAR may be able to work with relevant Product teams and Symantec's IT Department to enable the customer to amend, rectify or delete their Personal Data, as well as help the customer take relevant action in their own environment.

5. Information Security

Technical and Organizational Measures

As a rule, STAR seeks to aggregate, anonymize, pseudonymize and tokenize all threat telemetry it processes. This covers both data in motion and at rest.

For the development and implementation of its capabilities, STAR also subjects itself to stringent security requirements, including through security training and testing of its personnel, the use of secure development best practices and tools, code reviews, threat modelling performed on software changes, remediation of any issues detected through regular penetration testing and vulnerability scanning, and systematic reviews of any cryptographic tools and third party software used.

It is also 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 with links to the individual products that incorporate STAR technologies.

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.