# Product Transparency Notice

**For any queries, please contact privacyteam@symantec.com**

# Cloud Workload Protection for Storage (CWP-SA)

This Privacy Transparency Notice describes how Cloud Workload Protection for Storage - AWS Agent ("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 Cloud Workload Protection for Storage (CWP-SA) service helps in protecting the data that is stored in AWS S3 buckets from malware infections. The product scans the S3 buckets for security threats (like malware) with the help of Symantec's security technologies. The service enables customers to deploy an Agent in a desired AWS region of the customer's account. Based on the configuration, the Agent will provide necessary protection to the data in AWS S3 buckets of the region in which the Agent is deployed. Agent instances of one or more AWS regions across multiple AWS accounts of the customer can be centrally managed through the cloud based Centralized Management Console.

The Cloud based Console of Symantec is shared with Symantec's other services like Cloud Workload Protection* (CWP) and will be shared with products like Symantec Protection Engine* (SPE).

Further information about the Product is available at:

https://www.symantec.com/products/cloud-workload-protection

## 2. Personal Data Collection And Processing

### Sources of Data

The CWP for Storage Console accepts personal information at the time of product enrollment from common cloud or AWS marketplace, specifically work email address, LiveUpdate Administrator* IP Address, AWS VPC & AWS Subnets for the purpose of configuring the Agent in the customer's AWS account and enabling the service.

To deliver the security service, the Product collects user IDs and machine IP addresses to identify the source of detected malware or infection. The violation information along with these details is sent from Agent to Cloud Console.

CWP for Storage Agent integrates internally with various security/anti-malware technologies from Symantec Security Technology & Response* (STAR) team.

### 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.

Document Version 1.2
Date of issue: October 5, 2018

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

| Personal Data Category | Data Subject Category | Purpose Of Processing |
|---|---|---|
| Contact information (email address) | Customer employees and contractors | Service configuration, user notifications about the deployment of the Agent |
| Online identifiers and trackers (AWS VPC & AWS Subnets, user ID, IP address, cookies) | Customer employees and contractors, other persons interacting with customer | Security service configuration and enablement, detection of the origin of infected files |

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

**Personal Data Retention Schedule**

Email addresses used to configure AWS services in the customer's account are retained within that account until the customer deletes the AWS (S3) Agent or the AWS account itself. LiveUpdate Administrator* IP Address is retained with the AWS (S3) Agent until the customer changes or removes it. It is also removed after the customer deletes the AWS (S3) Agent from their AWS account. AWS VPC and AWS Subnet data will stay in the configuration of various AWS services in the customer's AWS account until the customer removes the configuration or deletes the account.

Personal Data collected to identify users registered with the product is erased 30 days after the subscription expires or cancelled. Events data is erased after 90 days. For the duration of the contractual relationship with the Customer, any 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 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) | Individual identifiers, contact information, online identifiers and trackers | Services are deployed on AWS Infrastructure. CWP can be configured to export the events to AWS CloudWatch in customer account. | 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

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

The customer can request to amend/rectify or delete the data collected by CWP-SA. 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

Symantec authorized personnel have exclusive access to the secure data store. All the data is transferred on secure https/SSL channel and stored in secured data store. The Customer sensitive data is stored in encrypted form. 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.

* For further information on the Personal Data processing involved in the use of other Symantec products referenced in this Notice, please refer to those products' Transparency Notices on the Symantec Privacy - GDPR Portal.