Product Transparency Notice

For any queries, please contact privacyteam@symantec.com

CloudSOC

This Privacy Transparency Notice describes how CloudSOC ("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

CloudSOC is a cloud hosted platform offering cloud application security services sold as separate subscriptions to enterprise Customers, including CASB Audit (Discovery), CASB Securlets (API), CASB Gateway (inline proxy). The Symantec CloudSOC platform enables companies to confidently leverage cloud applications and services while staying safe, secure and compliant. It provides visibility into shadow IT, governance over data in cloud apps, and protection against threats targeting cloud accounts.

Further information about the Product is available at:

https://www.symantec.com/products/cloudsoc-audit-shadow-it

https://www.symantec.com/products/cloudsoc-security-cloud-apps

https://www.symantec.com/products/cloudsoc-casb-gateway

2. Personal Data Collection And Processing

Sources of Data

CASB Audit collects data in the form of logs uploaded by the customer into the service. The logs come from the customer's firewalls and web proxies. Symantec obtains them when the customer uploads them to CloudSOC via a variety of transfer protocols.

CASB Securlets collect data from customer's cloud applications by invoking the APIs published by the cloud service providers. The customer authorizes Symantec to retrieve data via these APIs on their behalf from their cloud applications.

CASB Gateway collects data by inspecting the traffic sent by the customer's users to cloud applications. The data comes from web traffic generated when the customer's users access cloud applications, and Symantec obtains it when the customer sends that traffic via the Symantec service for inspection.

Processing of data collected by CASB Securlets and CASB Gateway includes inspection of content for sensitive information or threats (e.g. malware).

CloudSOC Platform (applies to all three services discussed above) collects data from the customer's employee directory (e.g. Active Directory). This is optional and requires the customer to use and configure Directory service connector available as part of the SpanVA software. The customer can configure what attributes from their directory they would like to synchronize to CloudSOC. Separately, the customer can also manually upload the list of users, groups and attributes into CloudSOC without using the Directory service connector.

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 and contact information	Customer's employees and contractors (users)	Provisioning the Cloud Security service, setting up administrators and contacts
Location Data (Device/network locale), online identifiers and trackers (IP addresses and similar unique network identifiers, usernames), network activity data (browsing activity, network telemetry, session logs)	Customer's employees and contractors (users)	Detecting from where and how users are accessing data in cloud apps
Individual identifiers and characteristics, contact and communication data, financial information, employment and education information, household information, including potentially sensitive or special categories of Personal Data such as government-issued ID, health records, etc.	Customer's employees, contractors, clients, suppliers, other business contacts, as well as other persons interacting electronically in or with the customer's networks, or whose Personal Data is contained in cloud apps, emails and files monitored	Performing the Cloud Security service by discovering Personal Data, PCI (e.g. credit card) and other types of confidential data stored in cloud apps, contained in emails and files (incidental processing when inspecting content for protected data categories like PII, PCI and others).

Personal Data Retention Schedule

Generally for the duration of the contractual relationship with the Customer, Personal Data is retained as described in the applicable product description.

In CloudSOC, the retention period for individual identifiers and contact information collected for the purpose of service provisioning and administration is limited to the term of the CloudSOC service subscription.

For location data, online identifiers and trackers and network activity data the active retention period is 3 months (90 days); the retention period in archives is for 12 months. For CASB Audit, the customer can configure a data retention period of 1 to 12 months.

For other categories of data processed to perform the Cloud Security service, the retention period is ephemeral, i.e. limited to the duration of processing. Such data is removed as soon as processing is complete.

Upon expiry of the subscription term, and following a 14-day grace period, all user activity and incident log data is archived for manual download or deletion by the customer for a period of 1 year, while configuration and other meta-data remain on the platform for the 1-year period. At the end of the 1-year period, the entire tenant including all data is removed. However, at any time

after the subscription term expiry, the customer can request a full deletion of their tenant including all data.

At the time of the tenant deletion, 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 and characteristics, contact and communication data, financial information, employment and education information, household information, including potentially sensitive or special categories of Personal Data such as government-issued ID, health records, etc.	Hosting service (IaaS)	U.S.A. for US CloudSOC Customers. EU (Ireland, Germany) for EU CloudSOC Customers
Mailgun	Individual identifiers, contact data	Customer communications	U.S.A.
Twilio	Individual identifiers, contact data	Customer communications	U.S.A., EU
Salesforce.com	Individual identifiers, contact information, location data, online identifiers and trackers, network activity data, communications data	Customer support/ticketing	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

Data will be transferred or accessed (including for storage, backup and archiving) in the U.S.A. for U.S.A. CloudSOC Customers, in the EU (Ireland, Germany) for EU CloudSOC Customers.

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

Concerning Personal Data collected and processed for the purpose of the Cloud SOC service, the following procedures govern the response to data subject right requests:

1. Rectification and erasure:

Some types of Personal Data are discovered by the service as part of its core functionality to help secure data in the cloud. These cannot be rectified or erased by the Customer as that dilutes the security offered by the service by compromising the integrity of records such as network or communication activity of a user showing the name of cloud app accessed, the time of access, the location, the type of activity performed (e.g. file delete), etc.

Some types of personal data such as names, email addresses etc. can be rectified if found to be incorrect (e.g. because of a spelling mistake). If specific data subject's data needs to be erased, the Customer can take action so that data related to that user(s) is not processed by CloudSOC going forward. For instance the customer can remove that user's web access so firewall/proxy logs uploaded to CloudSOC CASB Audit service do not contain the user's logs, nor will the CASB Gateway process his web traffic. Similarly, the customer can also remove the user's account in the cloud app, so the CloudSOC CASB Securlet does not receive any new data for that user via APIs.

Past data for a specific user that is already in CloudSOC cannot be deleted as that would undermine the level of security offered by the service. The customer can nevertheless request to delete their entire tenant (i.e. all users in their organization, not specific data subjects), in which case CloudSOC can terminate the service and execute the deletion.

2. Access and Export:

CloudSOC is an enterprise security solution provided to the IT Security department of the customer, and only security administrators are typically given login access to the CloudSOC console. Data subjects who are regular users without administrator privileges therefore do not have access to the CloudSOC solution for data access or export purposes. Administrators can however access and export data for a specific data subject via filtering features available on the CloudSOC console.

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 takes appropriate measures for information security. The service has passed SOC-2 audit and the audit report can be made available to Customers under Non-Disclosure Agreement (NDA). The report documents testing results of Symantec's control activities related to security, availability, confidentiality, integrity, and privacy of the system covering “Trust Service” principles and criteria. These controls span multiple categories including Administrative, Communication,

Risk Management, Logical Security, Physical Security, System Operations, Change Management, and Confidentiality.

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.