Product Transparency Notice

For any queries, please contact privacyteam@symantec.com

Validation & ID Protection (VIP) Authentication Service (Cloud)

This Privacy Transparency Notice describes how Validation & ID Protection (VIP) Authentication Service (Cloud) ("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

VIP is a multi-factor authentication platform. The Service provides online service providers and enterprises with increased security of their applications in the form of multi-factor authentication and protection for their end users against account takeover. The service also enables end users to utilize a single Authenticator across all VIP-enabled service providers and enterprises.

Further information about the Product is available at:

https://vip.symantec.com/

2. Personal Data Collection And Processing

Sources of Data

Authenticators are single-factor one-time password (OTP) Authenticators that generate OTPs. These are hardware authenticators and software-based OTP generators installed on devices such as mobile phones and personal computers. These VIP Authenticators consist of a unique VIP Credential ID and an embedded secret, shared with the Service, that is used as a concept for generation of OTPs and does not require activation through a second factor. The "VIP Credential ID" is an alphanumeric string that can vary in length from 12 to 16 characters, which identifies both the VIP Authenticator manufacturer as well as the VIP Authenticator itself. This VIP Credential ID can be bound to a "User ID," which can be any string that uniquely identifies an end user within a customer. User ID is a string created by the customer, with the option to use a non-meaningful identifier. The customer may associate other identifying data with User ID for management purposes, such as an email address, but this is not required for authentication. VIP does not need to be aware of the identity of the customer's end user. Thus the data collected by VIP varies depending of customers' preferences and settings.

For the purpose of sending SMS or voice call OTPs, the customer can provide end user phone numbers.

If VIP Intelligent Authentication is activated by the customer, Symantec will collect and process the following information about an end user and end user's machine:

- Operating system
- IP address
- Browser type
- Network
- Geographic location, which may include city, state or country

- Existing Symantec endpoint software stored on the machine

To collect such information Symantec utilizes a persistent tag in End User's browsers, HTML cookies, various parameters that are made available by the browser and the IP address of the End User's device. The information is processed for the purpose of determining the end user's typical pattern of behavior. During the authentication process, the stored pattern is compared with the actual behavior in order to assess anomalies in a particular log-in event. This information is anonymized before storage. The information is stored on Symantec's servers in the United States.

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)	Customer employees and contractors, clients and suppliers	To issue a license and invoices, as well as for helpdesk/admin user management via VIP's management console
Contact information (email, phone)	Customer employees and contractors, clients and suppliers	To issue a license and invoices, as well as to associate with a credential ID, per the scope defined by the customer
Location data (geographic location which can include city, state or country), online identifiers and network activity data (IP address, cookies, persistent tags, browser parameters)	Customer employees and contractors, clients and suppliers	To determine the end user's typical pattern of behavior only for purpose of authentication, per the scope defined by the customer

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

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)	Individual identifiers, contact information, location data, online identifiers and network activity data	Information-as-a-Service hosting	U.S.A.
Twilio	Contact information	Delivery of SMS OTP	U.S.A.
Early Warning	Contact information	Delivery of Voice OTP	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 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 configure the collection scope and/or use our APIs to add, edit, or remove data. The Symantec VIP team can also perform a data patch upon customer instructions if necessary. 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

All End User data that is collected is encrypted in motion and at rest within the Symantec infrastructure and services. 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.

Applicable Information Security Certifications

VIP conducts an annual SOC2 audit.

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.