**Symantec Information Centric Encryption Key Store Virtual Appliance**

This Privacy Transparency Notice describes how the Symantec Information Centric Encryption Key Store Virtual Appliance (“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

The Product is an on-premise store for Information Centric Encryption (ICE)* end-users’ encryption keys. It uses SafeNet Hardware Security Modules and provides proxy support.

Further information about the Product is available at:


### 2. Personal Data Collection And Processing

**Sources of Data**

The Product only collects and processes the Customer’s admin credentials and end-user encryption keys.

**Respective Roles of Symantec and Customer**

With respect to data collected, stored and processed within the Customer’s environment, the Customer is the Controller. Symantec does not in any way intervene as a Processor.

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

<table>
<thead>
<tr>
<th>Personal Data Category</th>
<th>Data Subject Category</th>
<th>Purpose Of Processing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator usernames and passwords</td>
<td>Customer admins</td>
<td>Authentication for administration purposes</td>
</tr>
<tr>
<td>End-user encryption keys</td>
<td>Customer end-users</td>
<td>Secure storage</td>
</tr>
</tbody>
</table>

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

### 3. Disclosure and International Transfer of Personal Data

**Third-Party Sub-Processors**

No third-party sub-processor is involved in delivering the Product.

**International Transfers of Personal Data**

The Product does not require or rely on any international transfers of data. The Customer has full authority and control over any movement of the virtual appliance, or of the data it contains, within the Customer’s infrastructure.

### 4. Exercise Of Data Subject Rights

The Customer is the sole Controller with access to all admin and end-user data in the appliance.
5. Information Security
Technical and Organizational Measures

All passwords are stored in non-reversible, industry standard salted, hashed, iterated format. 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 or Services referenced in this Notice, please refer to those Products’ or Services’ Transparency Notices on the Symantec Privacy - GDPR Portal.