SecurID™

May 2021

Privacy Considerations

Introduction

The intent of this document is to provide information about SecurID's position on some applicable aspects described in various privacy regulations including, but not limited to, the General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA) related to the processing of personal data.

The SecurID product is an authentication and identity assurance product that uses risk analytics and context-based awareness of users, which may be delivered via advanced token or token-less authentication and biometrics (locally stored in customer's device) authentication.

Product Specific

1. Has SecurID appointed a Data Protection Officer (DPO)?
   Yes. Data subjects may contact the DPO at privacy@rsa.com
2. What is the retention period of the personal data processed?
   Personal data may be deleted upon customer's request, as agreed in the service agreement, or deleted in accordance with our backup retention policy, which is within 12 months.
3. What is the purpose of processing personal data?
   Personal data may be processed for the purposes of providing warranty, support, and/or deployment of services, as relevant and defined by the applicable agreements.
4. What is the nature of processing?
   Authentication services, IT support, service support, product or service issue resolution, and to delete data contained in data storage devices.
5. What are the categories of data subjects whose personal data may be processed?
   The data subjects are customer's end users, which may include individuals, employees, contractors, suppliers, and other third parties.
6. What types of personal data are processed?
   SecurID Service Offerings, in general, may process first name, last name, email address, username, primary and secondary unique identifiers, account status, account expiration, telephone, geolocation, and patterns of software usage. Customers may, at their discretion, submit additional personal information.

   Biometric data (e.g. face recognition, etc.) used to log into the service offering is not disclosed to, stored, or processed by SecurID. Such data is stored and processed locally in the user's cellphone device.

   If Customer Support is contacted, then additional information may generally be processed, such as language of preference, computer name, IP address, permission access level, account and delegate information for communication services, chat communication data, and voice and video recordings with customer's consent.

7. How can SecurID be contacted for additional questions or comments?
   For data privacy and protection inquiries please contact privacy@rsa.com

   See our Privacy Statement.