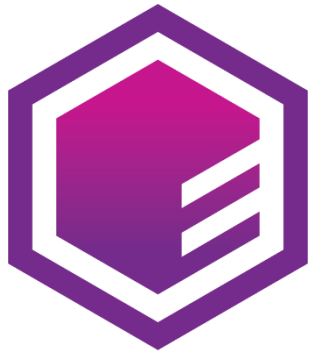

ENTRUST

MANAGED PUBLIC KEY INFRASTRUCTURE (PKI) SERVICES

PRIVACY STATEMENT

Contents

Managed PKI Services

Last Updated: February 17, 2022

Managed PKI Services

This product privacy notice describes how Managed PKI Services collects and processes personal data pursuant to applicable data privacy laws.

Description

With the Entrust Managed PKI Service, our experts manage your Entrust PKI, helping you ensure best practices, policies, and procedures are applied to your certificates. Your PKI is hosted in a highly available, fully redundant infrastructure with intelligent monitoring, robust data backup, and exceptional disaster recovery. We provide PKI compliance and functionality without the need for in-house expertise, secure facilities, and hardware or software.

Personal Data Collection and Processing

Personal Data Type	Purpose for Processing
Certificate Data	Public Trust Compliance
Email Address	User Authentication
IP Address	Security
Name	Public Trust Compliance
Password	User Authentication
Username	User Authentication
Department/Agency	PKI Compliance

Retention Period

All personal data collected by Managed PKI Services is retained in accordance with the terms set forth in Customer signed CPS (Certificate Practice Statement). If a contract is not renewed, personal data will be retained as below as per the type of End customer

- For Enterprise customers (Basic & Medium Assurance CAs – US & Canada MPKI) : Minimum of 3 Years

- For Enterprise customers (High Assurance Cas – US, Canada & UK MPKI) : Minimum of 7 Years
- For Federal (US Government agencies) customers : 10 Years & 6 months

Use of Sub-Processors

For the current list of sub-processors, visit https://www.entrust.com/legal-compliance/privacy/sub-processors.

International Data Transfers

Entrust's Managed PKI Services make use of three mPKI data centers. Customers can select to have their data housed in one of three data center locations (United States, Canada, and the United Kingom). To the extent that Customers are located in a different country than the data center, there may be cross-border transfers of personal data. Any cross-border transfers of personal data are made in accordance with relevant data privacy law requirements (e.g., the Standard Contractual Clauses for EU personal data transferred out of the EU).

Data Protection Measures

For more information on how Entrust processes personal data collected by this product, please refer to Schedule 2, Appendix 2 of our standard customer data processing agreement (DPA) found here.

Data Privacy Rights

The Customer is the data controller for all personal data collected by [Product]. Entrust Corporation, as the data processor, will assist the Customer, to the extent reasonable and practicable, in responding to verified data subject access requests the Customer receives with respect to [Product].

Amendments to this Privacy Statement

We reserve the right to amend this Product Privacy Statement from time to time as our business, laws, regulations and industry standards evolve. Any changes are effective immediately following the posting of such changes to https://www.entrust.com/legal-compliance/data-privacy/product-privacy-notices. We encourage you to review this statement from time to time to stay informed.

Contact Information

For questions about this product privacy notice, please contact privacy@entrust.com. For Entrust Corporation's general privacy notice, please click here.