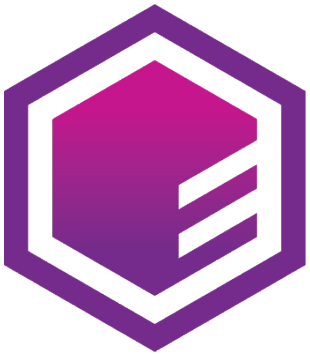

ENTRUST

ENTRUST HOSTED PKI SERVICES

PRODUCT PRIVACY NOTICE

Contents

Entrust Hosted PKI Services Product Privacy Notice

Last updated: February 3, 2026

This product privacy notice describes how the following Entrust PKI Hosted Services collect and process personal data pursuant to applicable data privacy laws:

- Managed Public Key Infrastructure (PKI) Services
- PKI as a Service
- Verified PKIaaS

Description

With Managed PKI Services, Entrust manages and operates a PKI for customers according to either commercial or U.S. Federal policy and practice requirements. PKI as a Service (PKIaaS) is a cloud-hosted highly available, scalable, turnkey PKI that's quick to deploy. For Verified PKIaaS, Entrust uses its PKI expertise and resources to perform limited verification and issuance of private trust TLS and mobile device digital certificates. PKI as a Service (PKIaaS) and Verified PKIaaS include a web-based management platform/console that helps customers manage their licenses, users, solution features, and digital certificates.

Personal Data Collection and Processing

PKI Hosted Service	Personal Data Type	Purpose for Processing
All	Email Address	User authentication, certificate application verification
All	IP Address	Security
All	First and Last Name	Account management, user authentication, certificate application verification
All	Username	User authentication
All	Password	User authentication
All	Phone number	Account management, user authentication, certificate application verification
All	Certificate Data Certificate data can be submitted automatically by the customer to the PKI Service or manually by the customer. This data can include any information that is valid for the make-up of a X.509 digital certificate, including the public	Creation and delivery of digital certificates

PKI Hosted Service	Personal Data Type	Purpose for Processing
	key. These data fields will be defined in the applicable Certificate Policy and could include: • Name • Affiliated Organization • Email Address • Locality	
PKIaaS, Verified PKIaaS	Job Title/Position	Account management, certificate application verification
Verified PKIaaS	Data processed for Entrust's Identity as a Service (IDaaS)	User authentication

Retention Period

All personal data collected by Managed PKI Services is retained in accordance with the terms set forth in the applicable Certificate Policy. If a contract is not renewed, personal data will be retained below according to 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

For PKIaaS and Verified PKIaaS, account information is retained for 7 years after account termination.

For Verified PKIaaS, verification and certificate data are kept for 7 years after certificate expiry.

Use of Sub-Processors

Different sub-processors are used depending on how the customer implements the PKI Hosted Services and management platform (e.g., SMS or IDaaS for authentication). For the current list of sub-processors, visit https://www.entrust.com/legal-compliance/data-privacy/sub-processors.

International Data Transfers

Entrust's Managed PKI Services' customers can select to have their data housed in one of three data center locations (United States, Canada, and the United Kingdom).

Personal data for PKIaaS and Verified PKIaaS is hosted in data centers in Canada, the EU or the US.

To the extent that customers are in a different country than where their data is hosted, there may be cross-border transfers of personal data. Entrust makes cross-border transfers of personal data in accordance with relevant data privacy law requirements (e.g., European Commission approved Standard Contractual Clauses (and/or their UK and Switzerland equivalents) if they are not in a country that has the benefit of an adequacy decision.

Data Protection Measures

For more information on how Entrust processes personal data collected by the PKI Hosted Services, please refer to Schedule 2 Annex II to the Standard Contractual Clauses of our standard customer data processing addendum (DPA) found here.

Data Privacy Rights

The customer is a controller of all personal data processed by Entrust for the purpose of providing the PKI Hosted Services, including in situations where Entrust's Hosted PKI Services are integrated with our Identity as a Service (IDaaS). Entrust Corporation, as the processor/service provider, will assist the customer, to the extent reasonable and practicable, in responding to data subject requests the customer receives with respect to PKI Hosted Services. For more details about Entrust's role as a processor in connection with our Identity as a Service (IDaaS) offering, please review our IDaaS Product Privacy Notice here.

Amendments to this Privacy Notice

Entrust reserves the right to amend this product privacy notice 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/product-privacy. We encourage you to review this notice from time to time to stay informed.

Contact Information

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