ENTRUST

IDENTITY AS A SERVICE

PRIVACY STATEMENT

Contents

Identity as a Service Privacy Statement

Last updated: January 22, 2024

Identity as a Service

This product privacy notice describes how Identity as a Service (IDaaS) collects and processes personal data pursuant to applicable data privacy laws.

Description

IDaaS is a cloud-based authentication solution designed to help organizations deploy multi-factor authentication for accessing networks, devices, and applications. The applications that can be protected using multi factor authentication include VPN, Firewall, Cloud SaaS and on-premise applications. Consumer facing applications can leverage built in REST APIs to enable multifactor authentication. Identity as a Service supports a broad range of authenticators including OTP, Hardware Token, Soft Token, Push Notification, Smart Card, Virtual Smart Card, FIDO2, Grid card, Email, and Password.

Personal Data Collection and Processing

Personal Data Type	Mandatory/Optional	Purpose for Processing
Audit information (user actions such as authentication times, self-management actions)	Mandatory	User authentication
Custom Attributes (as designed by customer)	Optional	User authentication
Biometric Data	Optional	User authentication, identity proofing; product improvement
Device Fingerprint	Optional	User authentication
Email Address	Optional	User authentication
Geo-location Data	Optional	User authentication
Identification Documents (Driver's License, Passport, etc.)	Optional	Identity proofing
IP Address	Mandatory	User authentication, auditing

Knowledge Based Question and Answers (e.g. which street did you grow up on?)	Optional	User authentication
Name	Optional	User authentication
OTP, Hardware Token, Soft Token, Push Notification, Smart Card, Virtual Smart Card, FIDO2, Grid Card, Email, Temporary Access Code	Optional	User authentication
Password	Optional	User authentication
Phone Number	Optional	User authentication
User ID	Mandatory	User authentication

Retention Period

Entrust's retention of biometric data is governed by the Entrust Biometric Data Notice. The personal data captured by Identity as a Service is otherwise kept until the user is deleted by an administrator. Audit records are kept in searchable format for a rolling period of 6 months and are subsequently maintained for 3 years in archived storage format.

Use of Sub-Processors

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

International Data Transfers

Personal data for Identity as a Service is hosted by AWS. Customers can select to have their data housed in one of three AWS server locations (Brazil, Ireland, Germany and the United States). If a customer is located in a different country than the one they have selected for hosting, 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 1 of our standard customer data processing agreement (DPA) found here.

Legal Basis for Processing Personal Data

The legal basis for the processing personal data by IDaaS is performance of a contract.

Data Privacy Rights

The Customer is the data controller for all personal data collected by Identity as a Service. 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 Identity as a Service.

HIPAA Compliance

The IDaaS solution is compliant with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule and can be used to process protected health information (PHI) as defined under HIPAA (e.g., for use authenticating patients in patient portals). Entrust will enter into a Business Associate Agreement (BAA) with customers who want to use IDaaS for this purpose.

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.