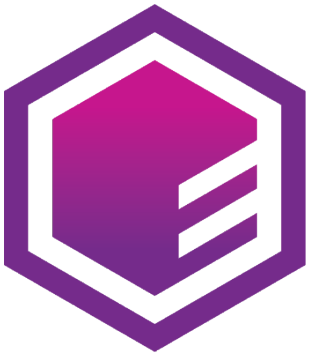

ENTRUST

IDENTITY AS A SERVICE

PRODUCT PRIVACY NOTICE

Contents

Identity as a Service Product Privacy Notice

Last updated: December 8, 2025

Identity as a Service (IDaaS)

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, Encrypted Biometric Token, Push Notification, Smart Card, Virtual Smart Card, FIDO2, Grid card, Passkey, Email, and Password.

A Customer may instruct Entrust to generate a scan of a User's face geometry using an image / video of the User or their identity document. Entrust adds the scan to an Encrypted Biometric Token ("**EBT**") that is stored by Entrust and by the Customer (either on the Customer's own server or on the User's device). The Customer may instruct Entrust to authenticate the User by comparing the scan stored within the EBT, to a scan of the User's face geometry that Entrust generates using a separate video of the User.

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
User ID	Mandatory	User authentication
Custom Attributes (as designed by customer)	Optional	User authentication
Device Fingerprint	Optional	User authentication
Email Address	Optional	User authentication

Geo-location Data	Optional	User authentication
Data processed for Entrust's Identity Verification Services	Optional	Identity proofing, user authentication
IP Address	Optional	User authentication, auditing
Encrypted Biometric Token	Optional	User authentication

Retention Period

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/data-privacy/sub-processors.

International Data Transfers

Personal data for IDaaS is hosted by Amazon Web Services (AWS). Customers can select to have their data housed in one of four 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. 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 this product, 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 the controller for all personal data processed by Entrust for the purpose of providing IDaaS, including in situations where IDaaS is integrated with our Identity Verification Services. 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 IDaaS. For more details about Entrust's role as a processor in connection with our Identity Verification Services, please review our IDV 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 Corporation's general privacy statement, please click here.