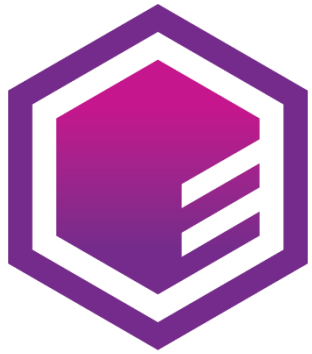

ENTRUST

IDENTITY VERIFICATION AS A SERVICE

PRODUCT PRIVACY NOTICE

Contents

Identity Verification as a Service Product Privacy Notice

Last updated: May 8, 2024

Identity Verification as a Service (IDVaaS)

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

Description

Identity Verification as a Service makes sure our customers' clients and applicants are who they claim they are by using a smartphone's Near Field Communication (NFC), Machine Readable Zone (MRZ) scanning of ID documents, selfies, and anti-spoofing liveness detection to quickly verify and authenticate their identities.

Personal Data Collection and Processing

Personal Data Type	Purpose for Processing
Identity Document (e.g., Passport, National ID) Data • Address • Biometric Data • Date of Birth • Email address • ID photo • Name • Nationality • Personal ID Number • Sex	Validate the authenticity of the identity document and user identity verification
Photo	User identity verification

Retention Period

Entrust's retention of biometric data is governed by the Entrust Biometric Data Notice. Entrust otherwise retains personal data for the duration necessary to authenticate the end user. Entrust deletes personal data following authentication or after the end user has abandoned the application. Our sub-processors retain personal data in accordance with their records retention schedules.

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 is collected from the end user's location while the application is in use, personal data may be passed to our sub-processors, and personal data is stored on AWS servers. Entrust makes cross-border transfers of personal data in accordance with relevant data privacy law requirements. For example, we ensure that personal data that is transferred outside of the European Economic Area (EEA) benefits from an adequate level of protection by requiring sub-processors to enter into the 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 IDVaaS. 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 IDVaaS.

Amendments to this Privacy Statement

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.