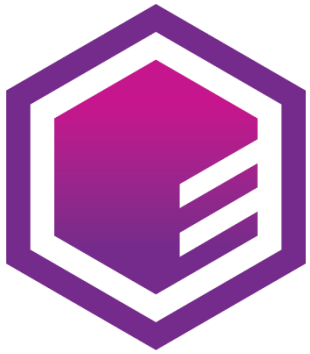

ENTRUST

IDENTITY VERIFICATION AS A SERVICE

PRIVACY STATEMENT

Contents

Identity Verification as a Service Privacy Statement

Last updated: May 23, 2023

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 • 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 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. If the end user is located in a different country than where the sub-processor or AWS hosting server is located, 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 or an adequacy decision 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 IDVaaS is performance of a contract.

Data Privacy Rights

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

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.