ONFIDO IDENTITY SERVICES

PRODUCT PRIVACY NOTICE

Contents

Onfido Identity Services Product Privacy Notice

Last updated: May 29, 2024

Onfido Identity Services

This product privacy notice describes how Onfido Ltd. (who, being a subsidiary of Entrust Corporation, is referred to in this notice as "**Entrust**") will collect and process personal data as a service provider/processor pursuant to applicable data privacy laws in order to provide the Onfido Identity Services. This notice has been created to help our Customers understand this processing and explain it to their Users (each as defined below). This notice does not provide details of the processing that Entrust conducts in relation to the Onfido Identity Services as a controller. Details of such processing are in the Onfido Privacy Policy.

Description

The Onfido Identity Services help our Customers to verify their Users so they can access their services quickly, easily, and securely. When Entrust verifies an identity, carries out checks related to an identity, or provides user authentication services, Entrust is committed to protecting the privacy and security of that identity.

Personal Data Collection and Processing

To provide Onfido Identity Services to a Customer, Entrust will collect certain personal information about the Customer's Users.

- Entrust's **"Customers"** are organizations that have asked Entrust to verify someone's identity, or to carry out checks related to their identity.
- Entrust's Customer's **"Users"** are the individuals whose identities a Customer has asked Entrust to verify or otherwise check.

Entrust may collect personal information about a User from the Customer, from the User, or from third party data providers ("**Data Providers**"). Data Providers are trusted third party service providers or public authorities who provide additional information depending on the Onfido Identity Services a Customer has chosen to use.

The precise personal data Entrust collects on behalf of a Customer varies depending on:

- how a Customer chooses to interact with Entrust (for example, via our API or the Onfido Dashboard as set out in Part 1 of the table below);
- what data collection method the Customer chooses to use (for example, our Applicant Form or SDK as set out in Part 2 of the table below); and
- which Onfido Identity Services the Customer chooses to use (as set out in Part 3 of the table below).

The table below sets out the personal data Entrust may process in order to provide the Onfido Identity Services.

<table>
<tr><td colspan="2">1. Customer initiates a check/process and interacts directly with Entrust</td></tr>
<tr><td>Personal Data Type</td><td>Customer Interaction Method with Entrust and Description</td></tr>
<tr><td rowspan="3">Categories of Personal Data:

• Onfido User unique identifier Check status/outcome and related information (e.g., a Report)
• Optional data fields selected by Customer from those technically supported and listed in Onfido's API Documentation (for example, the User's title - Mr., Mrs., Miss)
• Technical metadata as described in Onfido's API Documentation
• IP address and associated city/country level location information
• All data uploaded by Customer via 'custom input' or 'send/receive' features within the Onfido Identity Services for use during a workflow
• All other information processed by Entrust relevant to the applicable Onfido Identity Services
(Note - Entrust will also collect the full name, login credentials, and usage logs for Customer personnel accessing the Onfido Dashboard)</td><td>Application Programming Interface (API)

The API is based on REST principles and uses standard HTTP response codes to enable Customer to transmit and receive data from Entrust, as further described in the API Documentation.</td></tr>
<tr><td>Onfido Dashboard

The Onfido Dashboard is a graphical user interface to Onfido's API, as further described in the API Documentation.</td></tr>
<tr><td>Studio

Studio is a visualisation layer and workflow builder providing the Customer with no/low-code tools to create and configure dynamic user journeys incorporating the Onfido Identity Services.</td></tr>
<tr><td>Categories of Personal Data:

• Onfido User unique identifier
• Check status/outcome and related information (e.g., a Report)
• Optional data fields as listed in Onfido's API Documentation</td><td>Third Party User Tracking System

The Customer procured a third-party User tracking system to interact with Onfido's API and track Users</td></tr>
<tr><td colspan="2">2. Entrust collects additional information directly from Users on behalf of the Customer</td></tr>
<tr><td>Personal Data Type</td><td>Data Collection Method and Description</td></tr>
</table>

Categories of Personal Data: ● Images and text-based data (as specified in the relevant check or process) ● Email address ● Content of email sent to Users as a reminder to complete the Applicant Form ● Onfido User unique identifier *(Note - the Customer must have already provided Entrust with an email address so Entrust can send the Applicant Form to the User)*	**Applicant Form** Enables the User to enter data on an Onfido provided form
Categories of Personal Data: ● Images/video and information describing the images/video (as specified in the relevant check or process) ● Telephone number (web SDK only and optional) ● Content of SMS (web SDK only and optional) ● IP address and associated city/country level location information ● Anonymised usage data ● Onfido User unique identifier ● Technical metadata as described in Onfido's API Documentation	**SDK** The SDK provides the Customer with a drop-in set of user interface screens for mobile (iOS and Android) and web applications to allow the capture of identity documents and facial photographs/video for use with the Onfido Identity Services.
3. Entrust processes the data collected in (1) and (2) above and the following data on behalf of Customer in order to provide the Onfido Identity Services	
Personal Data Type	**Name of Onfido Identity Service and Description**
Categories of Personal Data: ● Full name ● Date of birth ● Address and postcode (Customer optional) ● National identifiers where applicable (e.g., Social Security Number for U.S Users)	**Identity Record Check** Searches third party database(s) to identify whether a User is included in the relevant database(s) and confirms the personal data provided by the User

• Telephone number	
Categories of Personal Data: • Image(s) of the identity document and information describing the identity document • Information extracted from the identity document electronically, where applicable	**Document Check** Assesses the likelihood the identity document provided is genuine.
Categories of Personal Data: • Image(s) of the identity document and information describing the identity document • Information extracted from the identity document electronically, where applicable • Video of the identity document and information describing the identity document	**Document Check – Video** Assesses the likelihood that the identity document provided is genuine and enhances the identity verification process by synchronously capturing a 1.5-second video of the identity document alongside the image. While the video itself is not used for checks, it is stored for customer access, providing an additional layer of security.
Categories of Personal Data: • Image(s) of the identity document and information describing the identity document • Information extracted from the identity document electronically, where applicable	**Document Check - Driver Verification** Assesses the likelihood the identity document provided is genuine and extracts driving licence information.
Categories of Personal Data: • Image of the User's face • Image of the face in the identity document • Scans of face geometry	**Facial Similarity Check - Selfie** Compares the face displayed on an identity document with a facial image captured of the User, to verify that they are the same.
Categories of Personal Data: • Image of the User's face • Image of the face in the identity document • Scans of face geometry	**Facial Similarity Check - Selfie Auto** Automatically (and without any human review) compares the face displayed on an identity document with any other image of a face, to verify that they are the same.
Categories of Personal Data:	**Facial Similarity Check - Video**

• Video of the User (including audio recordings) • Image of the face in the identity document • Transcribed text data from the video clip (if applicable) • Scans of face geometry • Data that may be construed as a voiceprint	Compares the face displayed on an identity document with a facial image captured from a video of the User, to verify that they are the same, while requiring the User to undergo liveness detection.
Categories of Personal Data • Image or video of the User's face • Onfido User unique identifier • Check status/outcome and related tracking information • Scans of face geometry	**Known Faces** (1) Compares the face on an image or video against a database of scans of face geometry of the faces from past checks completed by the Client and alerts if there is a match, and (2) adds the extracted scans of face geometry from the face on the image or video to the database in (1). For this service, scans of face geometry are used for the purpose of uniquely identifying a natural person.
Categories of Personal Data: • Full name • Date of birth (Customer optional) • Address and post/zip code (Customer optional)	**Watchlist Report – Enhanced** Searches third party watchlist and sanctions databases to identify whether a User is included in that database.
Categories of Personal Data: • Full name • Date of birth (Customer optional) • Address and post/zip code (Customer optional)	**Watchlist Report - Standard** Searches third party watchlist, politically exposed persons and sanctions databases to identify whether a User is included in that database
Categories of Personal Data: • Full name • Date of birth (Customer optional) • Address and post/zip code (Customer optional)	**Watchlist Report - AML** Searches third party watchlist, politically exposed persons, sanctions, and adverse media databases to identify whether a User is included in that database
Categories of Personal Data: • Full name	**Watchlist AML Ongoing**

• Date of birth • Address and post/zip code (Customer optional)	Searches third party watchlist, politically exposed persons, sanctions, and adverse media databases every 24 hours to identify whether a User is included in that database
Categories of Personal Data: • Full name • Date of birth • Address and post/zip code (Customer optional)	**Watchlist Standard Ongoing** Searches third party watchlist, politically exposed persons, sanctions, and adverse media databases every 24 hours to identify whether a User is included in that database
Categories of Personal Data: • Full name • Address and postcode • Image of proof of address document and information describing the document	**Proof of Address Check** Checks that a non-ID document is a suitable proof of address
Categories of Personal Data: Image of the identity document and information describing the identity document	**Autofill** Classifies identity documents and using optical character recognition technology, returns automatically extracted human-readable data from the identity document
Categories of Personal Data: • Full name • Document ID number • US state code • Optional data fields from the identity Document (at Customer's option)	**American Association of Motor Vehicle Administrators (AAMVA) Check** Uses the AAMVA Driver's License Data Verification (DLDV) service (via a third party sub-processor) to search participating US state DMV databases to match a User's personal details
Categories of Personal Data: • Full name • Date of birth • Personal Account Number (PAN)	**India Tax ID** Verifies that the PAN provided by the User or Customer matches the PAN number found on the database held by the Income Tax Department of the Government of India
Categories of Personal Data:	**Phone Verification Report**

• Full name • Address • Mobile number • Mobile number network history details • Mobile account details • Mobile risk score	(1) Searches a range of mobile network operator databases (via a third party) to verify if a phone number provided by a User is active and reachable; and (2) Considers additional phone intelligence attributes to help the Customer to assess the fraud risk associated with the phone number
Categories of Personal Data: • Onfido User unique identifier • Image of the identity document and information describing the identity document • Information extracted from the document • Document image hash number • Information about anomalous cross-matches with other documents	**Repeat Attempts** Personal Data extracted from the document during a check are stored in the Repeat Attempts Database and are compared to the same data points from other documents submitted by the Customer's new Users for the purposes of detecting and preventing fraud. Abnormal/inconsistent matches will be flagged as a possible indicator that the document presented by the new User is not genuine.
Categories of Personal Data: • Video of the User • Image of the face in the identity document • Background audio recording (at Customer's option) • Scans of face geometry	**Motion** Compares the face displayed on an identity document with a facial image captured from a video of the User, to verify that they are the same, while assessing whether the User in the video is a real person or a presentation attack/spoof.
Categories of Personal Data: • Onfido User unique identifier • Document number and other data extracted from any associated document check; • IP address and IP address type, including associated city/region/country level location and detection of any IP masking tools such as a VPN or Proxy; • Check status/outcome and related tracking information; • Inferences and outputs from Device Intelligence e.g. risk score, risk level;	**Device Intelligence – Standard** Analysis of technical data, device signals, IP address, geolocation, and other fraud signals (collected via the SDK or standard tracking technologies (e.g. JavaScript snippets) from Users as they interact with the Onfido Identity Services) to assess the likelihood that the User is genuine

• Device Fingerprint, device identifiers including audio and video fingerprint, Android/Google Advertising ID (AAID or GAID), hardware-based identifiers (e.g. MAC address); • Images and videos uploaded by U ser and any related metadata and metatags; • Information about Users' device including hardware and software attributes (e.g. device type and model, manufacturer, operating system type and version (e.g. iOS or Android), browser type and version, user-agent, navigator, screen details, plugins, fonts, memory, WebGL, battery information, language, time zone, camera name, microphone name, aspect ratio, resolution, frame rate, etc.); • Information about a User's behaviour when interacting with the Onfido Identity Services, including how the User uses the Onfido Identity Services such as start/stop time, forms/fields completed, pointer and touch events, time zone offset, distraction events; • Application Authenticity - Whether the device is using stolen security tokens; and • Other fraud signals listed in Onfido's API Documentation	
Categories of Personal Data: • Full name • Email address • Telephone number; and • Information extracted from, or describing, the identity document	**Qualified Electronic Signature ("QES") Package** ETSI certified identity verification and issuance of a qualified electronic signature, as set out in the product guide
Categories of Personal Data: • Telephone number; and	**One-Time Password ("OTP")**

• Information related to the risk profile of a telephone number, where applicable	Verifies that the User is in possession of the phone number by sending a unique code to the User's phone number for validation

Retention Period

Entrust provides the Onfido Identity Services on behalf of its Customers for a variety of different reasons. Those reasons are identified by the Customer and Entrust relies on them to tell Entrust when they no longer need to store the personal information Entrust has collected on their behalf, subject to maximum retention periods imposed by applicable laws or defined by Data Providers or by Entrust. (For example, the Onfido Facial Scan and Voice Recording Policy explains that the maximum period of time for which Entrust will retain photos/videos (including audio recordings) is three (3) years following submission of the photos/videos. Where Entrust has a legitimate legal reason, it may store personal information for longer than described above (e.g., where it is under a binding legal order not to destroy information).

Use of Sub-Processors

Entrust will need to share personal data relating to the Customer's Users with third party service providers (**"sub-processors**") in connection with the provision of the Onfido Identity Services to Customers. For the current list of sub-processors, visit https://www.entrust.com/legal-compliance/data-privacy/sub-processors.

International Data Transfers

The sharing of personal data with a sub-processor may involve the cross-border transfer of personal data. 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 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 and if there is no alternative transfer safeguard.

Data Protection Measures

Where possible, we pseudonymize, de-identify and/or aggregate personal data to protect privacy and minimize security risks. Pseudonymized data is where we replace, transform, or remove information so that it no longer identifies an individual without additional information. Entrust also takes appropriate administrative, physical, technical and organizational measures designed to help protect the information it holds from loss, theft, misuse and unauthorized access, disclosure, alteration and destruction. For more information about information security in relation to the Onfido Identity Services, please visit the Guide to Security at Onfido.

Data Privacy Rights

The Customer is the controller for all personal data processed by Entrust for the purpose of providing the Onfido Identity Services. If you are a User of an Entrust Customer and you wish to exercise your data privacy rights in relation to how we use your personal data as described in this product privacy notice, please contact the Customer so they may respond to you directly. If you contact us instead of our Customer, we will notify the Customer so they may fulfill your request.

Entrust, 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 the Onfido Identity Services.

Amendments to this Privacy Notice

We reserve 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 privacyrequests@onfido.com.