ENTRUST IDENTITY VERIFICATION SERVICES

PRODUCT PRIVACY NOTICE

Contents

Entrust Identity Verification Services Product Privacy Notice

Last updated: April 24, 2025

Entrust Identity Verification Services

The Entrust Identity Verification Services ("**Services**") help Entrust Customers 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.

When Entrust Corporation and its subsidiaries ("**Entrust**") collect and process personal data for the purpose of providing the Services to a Customer, Entrust acts on the Customer's behalf as their service provider and processor. The section of this notice headed "*The Personal Data We Process on Behalf of Our Customers*" describes this processing. NOTE: Customers are responsible for explaining this processing to their Users.

As well as handling personal data on behalf of a Customer for the purpose of providing the Services to them, Entrust also collects and processes personal data on our own behalf as a controller. For example, we may use the personal data that we collect when providing our Services, and personal data that is publicly available, to develop and improve the Services. The section of this notice headed "*Using Personal Data as Controller*" explains this processing.

The Personal Data We Process on Behalf of Our Customers

To provide the Services to a Customer, Entrust collects and processes certain personal data about the Customer's Users.

- **"Customers"** are organizations that have asked Entrust to provide the Services in order to verify someone's identity, or to carry out checks related to their identity.

- **"Users"** are the individuals whose identities a Customer has asked Entrust to verify or otherwise check via the Services.

Entrust may collect personal data 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 Services a Customer has chosen to use.

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

- How a Customer chooses to interact with Entrust (for example, via our API or the 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).
- Which 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 collect and process to provide the Services. Customers should refer to the API Documentation and Guides for more details.

<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:

• 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 the API Documentation) for example, the User’s title - Mr., Mrs., Miss)
• Technical metadata as described in the 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 Services for use during a workflow
• All other information processed by Entrust relevant to the applicable Services

(Note: Entrust will also collect the full name, login credentials, and usage logs for Customer personnel accessing the 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>Dashboard

The Dashboard is a graphical user interface to the 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 Services.</td></tr>
<tr><td>Categories of Personal Data:

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

The Customer procured a third-party User tracking system to interact with the 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>
</table>

Personal Data Type	Data Collection Method and Description
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 • User unique identifier *(Note: 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 Entrust 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 • User unique identifier • Technical metadata as described in	**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 Services.
3. Entrust processes the data collected in (1) and (2) above and the following data on behalf of Customer to provide the Services	
Personal Data Type	**Name of Service and Description**
Document Checks Document Checks verify identity documents from across the globe by analyzing an image or video of the document. Our system extracts information from the image/video or, if possible, from the security chip embedded in the document. Our models analyze the authenticity of the document, which may include machine-readable zones, barcodes, QR codes, and security chips, to verify whether the document is genuine or shows signs of tampering. We will also compare the image or video of the identity document with information about compromised identities that have been leaked or otherwise made publicly available. NOTE: Users living in the Netherlands should be advised that Entrust may automatically mask the BSN number on their identity document in our back-end systems when required under Dutch law, and particularly the Dutch Prevention of Money Laundering and Terrorist Financing Act.	

Categories of Personal Data: • Image(s) of the identity document • Information extracted from the identity document (for example name, document number, date of birth, nationality, type of document, issuing country, expiration date, information embedded in barcodes, QR codes, security chips and features (which will vary depending on the type of document)) • Data that may be construed as a scan of face geometry*	**Document Check** Analyses an image of an identity document (including the portrait photo area) to assess the likelihood that the document is genuine.
Categories of Personal Data: • Video of the identity document • Image(s) of the identity document • Information extracted from the identity document (for example name, document number, date of birth, nationality, type of document, issuing country, expiration date, information embedded in barcodes, QR codes, security chips and features (which will vary depending on the type of document)) • Data that may be construed as a scan of face geometry*	**Document Check – Video** Analyses an image of an identity document (including the portrait photo area) to assess the likelihood that the document 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 • Information extracted from the identity (for example name, document number, date of birth, nationality, type of document, issuing country, expiration date, information embedded in barcodes, QR codes, security chips and features (which will vary depending on the type of document)) • Data that may be construed as a scan of face geometry*	**Document Check - Driver Verification** Analyses an image of an identity document (including the portrait photo area) to assess the likelihood that the document is genuine, and extracts driver's license information.
Biometric Checks and Authentication When providing biometric checks as part of our Services, we'll ask for an image or video (which may include an audio recording) of a User's face (a "**Selfie**"), as well as an image or video to use as a reference image (for example, an image of their identity document). We generate two scans of	

<table>
<tr><td colspan="2">the user's facial geometry (one scan using the Selfie, and one scan using the reference image) and we compare those two scans to assess whether the person in the Selfie is likely to be the same person pictured in the reference image. We will also evaluate the authenticity of the images and videos (including audio recordings) and identity documents, including detecting whether there is a genuine human or physical document in your photos/videos, and identifying signs of tampering, coercion or social engineering.

Except as described under the section below headed "Fraud checks, including device integrity and fraud signals", when performing biometric checks, we do not store the extracted face scans once the check is complete. Where a Customer has asked us to provide an authentication service, the Customer may ask Entrust to store a reference image chosen by the Customer for each relevant User. (This image is retained in accordance with retention periods set by the Customer and subject to any maximum retention periods specified by Entrust or in applicable laws.) When Entrust is asked to authenticate a User, we will generate two face scans - one using a new image of the User and one using the reference image we have stored. If the two images match, the authentication is confirmed. Customers who wish to use an authentication service without the need for Entrust to store a reference image can choose to store an encrypted version of the face scan relating to a reference image themselves (including on the User's device). When Entrust is asked to authenticate a User, we will be given access to the stored face scan, and we will compare it to a new face scan that we generate using a new image of the User. If the two images match, the authentication is confirmed.

NOTE: These services involve the use of data that may be construed as a scan of face geometry or voiceprint, and which may be considered to be biometric identifiers or biometric information by applicable U.S. biometric privacy laws. Users located in the U.S. should refer to the Facial Scan and Voice Recording Policy for details.</td></tr>
<tr><td><u>Categories of Personal Data:</u>

● Image of the User's face
● Image of the face in the identity document / reference image
● Scans of face geometry*</td><td>Facial Similarity Check - Selfie

Compares the face displayed on an identity document or reference image with an image of the User's face, to verify that they are the same.</td></tr>
<tr><td><u>Categories of Personal Data:</u>

● Image of the User's face
● Image of the face in the identity document / reference image
● Scans of face geometry*</td><td>Facial Similarity Check - Selfie Auto

Automatically (and without any human review) compares the face displayed on an identity document or reference image with an image of the User's face, to verify that they are the same.</td></tr>
<tr><td><u>Categories of Personal Data:</u>

● Video of the User (including audio recording)</td><td>Facial Similarity Check - Video

Compares the face displayed on an identity document or reference image with a facial</td></tr>
</table>

<table>
<tr><td>

- Image of the face in the identity document / reference image
- Transcribed text data from the video clip
- Scans of face geometry*
- Data that may be construed as a voiceprint*

</td><td>image captured from a video of the User, to verify that they are the same while also performing liveness detection. Includes mandatory processing of audio.</td></tr>
<tr><td>

Categories of Personal Data:

- Video of the User (including background audio recording at Customer's option)
- Image of the face in the identity document / reference image
- Transcribed text from the video clip (if applicable)
- Scans of face geometry*
- Data that may be construed as a voiceprint*

</td><td>

Motion

Compares the face displayed on an identity document or reference image with a facial image captured from a video of the User, to verify that they are the same, while also performing liveness detection. Includes optional processing of audio.

</td></tr>
<tr><td colspan="2">

Data Verification

Entrust provides Customers with data verification checks via a network of trusted Data Providers (defined above) and our own internal checks. These checks enable Customers to verify their Users, detect fraud and comply with anti-money laundering (AML) and Know Your Client (KYC) requirements.

We conduct these checks by comparing personal data provided by the Customer or the User with information held by Data Providers or information extracted from documents, e.g. a utility bill for proof of address checks. Our global network of data verification services varies depending on a User's location and includes voter and driving license registers and other government databases, police databases, consumer credit agencies, sanctions and Politically Exposed Persons (PEP) lists, adverse media sources, utility companies, mobile network providers and other trusted commercial sources.

At the request of a Customer, these services may be provided on an ongoing basis, for example where a Customer's regulatory obligations require ongoing monitoring against sanction and PEP lists.

The information collected will vary depending on the availability of checks in the User's location and the Services selected by the Customer but may include contact details such as postal address, email address, telephone number, social security number or other national identity number, information extracted from a utility bill a User uploads or other information provided by the Data Provider e.g. a user's mobile network operator, publicly available information from media searches, sanctions and PEP lists.

</td></tr>
<tr><td>Categories of Personal Data:</td><td>Identity Record Check</td></tr>
</table>

• Full name • Date of birth • Address and postcode (Customer optional) • National identifiers where applicable (e.g., Social Security Number for U.S Users) • Telephone number	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.
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 • Date of birth • Address and post/zip code (Customer optional)	**Watchlist AML 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 • 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	**Proof of Address Check** Checks that a non-ID document is a suitable proof of address.

• Image of proof of address document and information describing the document	
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: • Full name • Address • Mobile number • Mobile number network history details • Mobile account details • Mobile risk score	**Phone Verification Report** (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.
Fraud checks, including device integrity and fraud signals Entrust leverages several different fraud detection capabilities. Some of these depend on the scope of the Services selected by the Customer, whereas other fraud checks are applied across all of the Services. (For example, Entrust will analyze the metadata associated with the User's Selfie and the image or video of their identity document (to identify whether any editing software can be detected) to assess the likelihood that the User is genuine.) **Device Intelligence.** Entrust can help Customers to determine whether a device, email address or phone number has previously been used in relation to suspected fraudulent activity, shows unusual usage patterns, has been manipulated or otherwise indicates that the user may not be genuine. At a Customer's request, Entrust and our Data Providers may collect 'passive signals' from the	

<table>
<tr><td colspan="2">Customer (for example mobile number or email address) or a User's device as they engage with the Customer's website or app or Services. Such information may include device identifiers, IP address, information about the device (for example the operating system used, whether the device is providing false randomized device and network information or has otherwise been compromised) and how the User interacts with:
• The Services. For example, information about the upload time, which version of our software was used, the camera name and model used to capture any images and whether there are any indicators that the device has been tampered with or emulated; and
• Their device. For example, fraudsters will cut and paste large volumes of information from their clipboard, use this functionality multiple times and otherwise navigate between applications on their device very differently from a genuine User.

Entrust and our Data Providers may also use such information to infer other information about the User, for example their broad geographical location from their IP address, or to calculate an identity risk score.

Together this information helps Entrust and our Data Providers assess the likelihood of an individual being a genuine User, assign a risk score and infer certain information such as a User's broad geographical location from their IP address.

Repeat Attempts, Known Faces and Document Known Faces. At a Customer's request, we can check whether we have previously verified a User on behalf of that Customer by comparing the information submitted as part of a new Document Check and/or Biometric Check, to information we have previously verified for that Customer. (More specifically, at a Customer's request we will retain information (including face scans depending on the service the Customer has chosen to use) extracted from a User's identity document or Selfie and compare this retained information to the newly submitted information. As explained further below, Customers determine how long we retain the extracted information). This helps our Customer not only verify Users' identities but further protects them and their Users from fraud by helping Customers understand when a User may be generating multiple identities, editing and tampering with documents or manipulating device or network information. NOTE: Known Faces and Document Known Faces involve the use of data that may be construed as a scan of face geometry, and which may be considered to be biometric identifiers or biometric information by applicable U.S. biometric privacy laws. (Users located in the US should refer to the Facial Scan and Voice Recording Policy for details.)</td></tr>
<tr><td>Categories of Personal Data:

• 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</td><td>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 Services) to assess the likelihood that the User is genuine.</td></tr>
</table>

• Check status/outcome and related tracking information • Inferences and outputs from Device Intelligence e.g. risk score, risk level; • 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 User 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 Services, including how the User uses the 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 • Other fraud signals listed in the	
<u>Categories of Personal Data:</u> • User unique identifier • Image of 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 • User unique identifier • Image or video of the User's face ∉ Check status/outcome and related tracking information • Scans of face geometry*	**Known Faces** (1) Compares the face on the image / video of the User provided for the purposes of a new Facial Similarity Check against a database of faces supplied for previous Facial Similarity Checks performed on the Customer's behalf and alerts if there is a match, and (2) adds the scan of face geometry extracted from the newly provided image/video to the database in (1).
Categories of Personal Data • User unique identifier • Image of the identity document • Check status/outcome and related tracking information • Scans of face geometry*	**Document Known Faces** (1) Compares the face on an image / video of the User's identity document provided for the purposes of a new Document Check against a database of faces supplied for previous Document Checks performed on the Customer's behalf and alerts if there is a match, and (2) adds the scan of face geometry extracted from the newly provided image/video to the database in (1).
Other Services	
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 • Information related to the risk profile of a telephone number, where applicable	**One-Time Password ("OTP")** Verifies that the User is in possession of the phone number by sending a unique code to the User's phone number for validation.

Entrust Identity Verification Services integrate with other Entrust offerings including Identity as a Service (IDaaS), Identity Verification as a Service (IDVaaS) and Workflow Signing Services. For more information about privacy considerations for these offerings, review the relevant Entrust Product Privacy Notice.

Additional Obligations regarding U.S. Users

Where the Customer makes any of the following Services available to a User who is located in, or resident of, the United States (a "**U.S. User**"), the Customer is required to comply with additional obligations as set out in the agreement between Entrust and the Customer. This is because (as summarised in the section above headed "*The Personal Data We Process on Behalf of Our Customers*") these Services involve the processing of personal data that may be construed as a scan of face geometry or a voiceprint under U.S. Biometric Data Protection Laws:

- Facial Similarity Check – Selfie, Selfie Auto, Video, Motion
- Known Faces
- Document Known Faces
- Document Check, Document Check Video, Document Check Driver Verification

Reports

Once Entrust has verified an identity or run a check, we share the results with the Customer in a report ("**Report**"). Each Report contains an overall result of 'Clear' or 'Consider':

- If we're able to verify the identity of a User, and the requested checks do not show signs of fraud or other anomalies, we notify the Customer that the checks are Clear.
- If we're unable to verify the identity of a User, or the User is unable to pass all requested checks or the checks show signs of fraud or other anomalies, we return a Consider result. If we return a Consider result, we will also provide a detailed breakdown of the reasons why. (The reasons are generated from the different machine learning models and/or human powered processes that are used to verify an identity or perform a check.)

Reports contain recommendations only and the reasons behind them. It is then for the Customer to decide how to proceed with a User - based on the content of the Report but also based on other information available to them (including additional information they may have or decide to request from their Users).

By providing our customers with these detailed Reports, our aim is to empower our Customers to make informed decisions about their Users and to provide help to Users that are having difficulty in passing a check.

Using Personal Data as Controller

As explained above, when we use personal data to provide the Services to our Customers, we are acting on their behalf as their service provider and processor. However, we also process the personal data of Users, and others, on our own behalf (as a "Controller") for the purposes described in this section. If a User is in the European Economic Area or United Kingdom, we will only use your personal

data for a particular purpose where we have a "legal basis" for this. We have set out below the legal bases we rely upon for each purpose. Onfido Ltd is the Controller for this processing. For information on how to contact Onfido Ltd, see the section below headed "*Contact Information".*

To develop and improve the Services (including machine learning technologies)

At Entrust, our vision is to simplify digital identity. To do this, provided we have the permission of our Customers and it is not prohibited by applicable law, we use the personal data we collect about our Customers' Users (as described above) to improve and develop the Services. For the same purpose, we may also use personal information that has been made publicly available or that we have obtained from a third party provided this is not prohibited by applicable law.

Developing and improving the Services includes building and improving our technology (such as our machine learning technologies and algorithms) and developing and testing new checks, products and services to better verify a User's identity and/or detect fraud. For example, we may need to train our models to recognise a novel fraud attack, a new version of an ID document or to minimize bias and improve performance. As part of this work, we train our technology to recognize specific patterns in information and make predictions about new sets of information based on those patterns. This is known as machine learning. We also train our human analysts to perform those tasks so they can assist when our machine learning models aren't best suited for the task or are still learning. Sometimes, we'll also re-run and re-submit checks to ensure the Services are working properly, particularly when testing a new feature or service for quality checks. Together, these developments help make the Services stronger and safer for all Customers and Users.

We process personal data for these purposes on the basis that it is necessary for the legitimate interest of our Customers and Entrust. Financial crime, fraud, and corruption are serious issues that affect not only the law enforcement community but financial institutions, the private sector, and other major corporations – as well as individuals themselves. As such, Entrust considers there is a clear legitimate interest in improving and developing the Services for the purpose of continuing to effectively tackle and reduce fraud.

Where we use sensitive personal data for these purposes (for example, information which could potentially reveal information about someone's racial or ethnic origin), we primarily process this information on the basis that it is necessary for reasons of substantial public interest. Such public interests include ensuring equality of treatment across all types of Users by measuring and mitigating algorithmic bias with a view to providing fair and inclusive Services, which effectively detect fraud, and are balanced against the rights and freedoms of Users. When developing the Services, we implement specific measures to safeguard the rights and freedoms of those individuals whose data is used for this purpose, including pseudonymisation (where possible), impact assessments and strict security controls to safeguard their fundamental rights and their interests.

To compile statistics, benchmarking and analytics

We use personal data (such as check results, identity document type, and device metadata) to create statistics regarding the use and performance of the Services. We provide these statistics to our Customers so that they and we may use them to, for example, conduct benchmarking and analytics (for example, to compare a Customer's missed fraud rates to the general missed fraud rate for an industry, or to analyze fraud trends). We also use these statistics to gain market insights (for example, to enhance understanding of missed fraud trends and identify fraud patterns) and to inform our decision making on product improvements. An individual cannot be identified from these statistics and where possible, we pseudonymise, aggregate and/or de-identify (and where feasible anonymise) personal information which is used for these purposes.

We process personal data for these purposes on the basis that it is necessary for Entrust's and our Customer's legitimate interests in understanding (at the aggregate level) how people are using our Identity Services.

For compliance with applicable law/regulation, to exercise, establish or defend legal rights or claims, or to protect someone's vital interests

Entrust may process the personal data we collect about our Customers' Users (as described above) where this is necessary for compliance with a legal obligation, to exercise, establish or defend legal rights or claims, or to protect someone's vital interests. For example, we may be required by law to:

- disclose information in response to a request from a government or law enforcement body as described in the section below headed "*Government and Law Enforcement Requests"*;
- collect a User's broad geographic location (e.g. country or city-level location), either directly from them or the Customer or by approximating this based on the User's device's IP address, to enable Entrust and our Customers to comply with global sanctions requirements and the increasing number of biometric and privacy laws that apply to the Services. We use this broad geographic location to determine a User's location to display the relevant consent screen and collect any necessary biometric consents or identify if a User is located in a sanctioned country where we are prohibited by law from providing services.

In connection with a business transaction or to obtain professional advice

Entrust may need to process a User's personal data in connection with an actual or proposed divestiture, merger, acquisition, joint venture, bankruptcy, dissolution, reorganization, or any other similar transaction or proceeding, or to obtain professional advice. We process personal data for these purposes on the basis that it is necessary for Entrust's legitimate interest in running its business in a commercial and compliant manner.

Retention Period

Where Entrust processes the personal data of a User on the Customer's behalf to provide the Services, the Customer determines how long Entrust retains that personal data (subject to any

maximum retention periods imposed by applicable law or defined by Entrust or Data Providers). See here for more details.

Where Entrust processes personal data as Controller, Entrust retains that data for as long as is necessary to complete the purpose for which the information is processed, subject to any maximum retention periods imposed by applicable law.

Data Sharing and Use of Sub-Processors

In addition to sharing personal data with Customers and Data Providers (as described above), Entrust also shares personal data:

- With third parties who help us provide the Services and perform tasks on our behalf. This includes information technology and related infrastructure providers (who provide us with a place to store your personal information); data analytics providers (who help us to analyze trends and provide market insights); and our business process outsourcing partners (whose staff perform human review and quality checks). For the current list of third-party service providers ("**sub-processors**") who process User personal data to provide the Services, visit https://www.entrust.com/legal-compliance/data-privacy/sub-processors.
- With companies in the Entrust group of companies who help us to provide our services (for example, by providing ancillary engineering, technical or customer support);
- With an actual or potential buyer, investor or partner (and its agents and advisers) in relation to a business transaction;
- With parties that provide Entrust with professional (e.g. advisory and auditing) advice and services;
- With a competent law enforcement body, regulatory, government agency, or court;
- With any other person where instructed to do so by a Customer. For example, if a Customer has configured the Services to check whether an identity document has been previously identified as lost, stolen, fraudulent, or otherwise compromised by a government or other external party, Entrust may share that compromised identity document on behalf of that Customer, and the government or other external party may retain a copy to the extent they consider it necessary, proportionate, and lawful. Under the instruction of Customers and as permitted by applicable law, Entrust currently shares identity documents with the UK Metropolitan Police as part of the Amberhill Database for such purposes; and
- To any other person where we have a legitimate legal reason for doing so.

Whenever legally possible, we seek to protect the personal information we share by imposing contractual privacy and security safeguards on the recipient of that information. In some cases, however, it's not possible for us to do so — for example, when we have a legal obligation to disclose information to a government authority and that government authority is not willing to enter into such contractual safeguards.

International Data Transfers

The sharing of personal data 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. You can request a copy of these clauses by contacting us using the details in the section below headed "*Contact Information*."

Security 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 Services, please visit .

Data Privacy Rights

The Customer is the controller for all personal data processed by Entrust for the purpose of providing the 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 the section of this notice headed "*The Personal Data We Process on Behalf of Our Customers*", 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 are able to address 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 Services.

Entrust is the controller for the processing of personal data described under the section of this notice headed "*Using Personal Data as Controller.*" Depending on where you live and subject to applicable privacy law, you may have the following rights in respect of this processing:

- the right to request access to and disclosure of your personal data.
- the right to change and/or correct your personal data if it is inaccurate.
- the right to block or suppress our processing of your personal data. (This enables you to request that Entrust suspends the processing of your data in certain circumstances.)
- the right to object to our processing of your personal data where we are relying on a legitimate interest (or those of a third party) and you feel such processing impacts on your fundamental rights and freedoms. (In some cases, we may demonstrate that we have compelling legitimate grounds to process your personal data which override your rights and freedoms.)
- the right to request that we delete your personal data, subject to certain exceptions.
- the right to request portability of your personal data. We will provide to you, or a third party you have chosen, with your personal data in a structured, commonly used, machine-readable format.
- the right to withdraw your consent, if applicable. Withdrawing your consent will not affect the lawfulness of any processing we conducted prior to your withdrawal, nor will it affect processing of your information conducted in reliance on lawful processing grounds other than

consent.

- the right to lodge a complaint with your local data protection authority or regulator.

If you wish to exercise your rights in relation to how we use your personal information as described under the section headed "*Using Personal Data As Controller*", please contact us at identity-privacyrequests@entrust.com or at the postal address below. If you exercise any of your data protection rights detailed in this section, we will not discriminate against you.

Government and Law Enforcement Requests

If you are a government or law enforcement body that wishes to request personal data or confidential information related to a check that we may have conducted on a particular User, please contact the Customer on whose behalf the check was carried out. Since we provide our Services on behalf of our Customers, we are not able to disclose any information related to a specific check unless the relevant Customer directs us to do so, or we are subject to a legal requirement (such as a court order or statutory power mandating disclosure) to do so. If you wish to request the disclosure of information in respect of which there is such a legal requirement, please contact us at identity-privacyrequests@entrust.com providing clear details of the legal requirement in your message. providing clear details of the legal requirement in your message.

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. If we make material changes, we will publish those changes before they come into effect and notify our Customers so they can consider whether to update their own policies and notify their users.

Contact Information

If you would have any questions about this notice, please contact Onfido Limited at identity-privacyrequests@entrust.com or at: Attention: Privacy Office, Onfido Ltd, 14-18 Finsbury Square, 3rd Floor, London, EC2A 1AH, United Kingdom.

If you would like to raise a concern or otherwise communicate with our Data Protection Officer, you may contact them at DPO@mishcon.com Attention: Entrust DPO, Mishcon de Reya LLP, Africa House, 70 Kingsway, London, WC2B 6AH, United Kingdom