ENTRUST BIOMETRIC DATA POLICY

Contents

Entrust Biometric Data Policy

Last updated: 20 December 2024

This Entrust Biometric Data Policy applies to Users (defined below) located in the United States.

Entrust Corporation and its affiliate companies ("**We**") provide services to our business customers which may necessitate the collection and processing of Biometric Data as defined below ("**Services**").

Under the terms of our contracts, our business customers are responsible for ensuring that their use of these Services is compliant with all applicable laws governing their collection, possession, storage, use, disclosure, and/or transmission of Biometric Data (including, for example, by providing notice to and obtaining consent from those individuals whose Biometric Data is processed via the Services ("**Users**") and by developing and complying with their own biometric data policies).

However, Entrust has created this Biometric Data Policy to: (a) describe how the Services collect and process Biometric Data (to help our customers understand this processing and explain it to their Users); and (b) discharge any legal obligations which US biometric privacy laws (such as the Illinois Biometric Information Privacy Act) may impose on Entrust regarding the publication of a policy establishing a retention schedule and guidelines for permanently destroying Biometric Data in its possession.

What is Biometric Data?

As used in this policy, "Biometric Data" means, collectively, "biometric identifiers" and "biometric information." Common examples of "biometric identifiers" include retina or iris scans, fingerprints, voiceprints, and scans of hand or face geometry. "Biometric information" means any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier and used to identify an individual.

What Biometric Data Do We Collect?

When a User of an Entrust customer uses a Service, they may (depending on the Service involved) be required to provide a photo or video of their face, and/or an image of their government issued or other identity document. In order to provide the Service, Entrust and its service providers may need to review these images to detect the geometry of the User's face, and/or create a scan of their face geometry (sometimes called a "faceprint"). This information may be construed as Biometric Data.

How Do We Use Your Biometric Data?

We and our service providers may use Biometric Data for the following purposes:

1. To provide our customer with the requested Service. The purpose of the Service may be, for example:

2. to verify a User's identity by comparing facial Biometric Data extracted from the photo/video of a User's face, to facial Biometric Data extracted from the photo in their identity document;
3. to authenticate a User and their use of the customer's services by comparing facial Biometric Data from a reference image (for example, an image the User provided to the customer when they signed up for an account or the photo in their identity document), to the facial Biometric Data extracted from a new photo/video of the User's face;
4. to evaluate the authenticity of images and videos and identity documents, including detecting whether there is a genuine human or physical document in a User's photos/videos or signs of tampering; or
5. to consider whether a photo submitted by a User for use in an identity document meets the customer's quality requirements, including by locating the face within the photo and locating the position of facial landmarks (such as the tip of the nose and the corners of the eyes);
6. To comply with our legal, regulatory, or contractual obligations, and
7. To improve the Services where permitted by applicable law.

To Whom Do We Disclose Your Biometric Data?

As noted above, Entrust uses service providers to assist with the provision of the Services. We may disclose Biometric Data to those service providers, and they may further disclose that Biometric Data to the service providers that help them provide the Services.

We and our service providers may also disclose Biometric Data to other third parties (to the extent permitted by law) to: (i) enforce our or their legal rights; (ii) to comply with our or their legal and contractual obligations; (iii) to cooperate with law enforcement agencies concerning conduct or activity that we or they reasonably believe may violate applicable law; (iv) if required by a subpoena, warrant, or other valid court order; (v) to prevent harm, loss, or injury to others; and (vi) with your or your authorized representative's express consent.

Neither Entrust nor its service providers will sell, lease, trade, or otherwise profit from Biometric Data. (Entrust may use Biometric Data to improve the Services as explained further herein.)

For our current list of service providers (sometimes referred to as sub-processors), visit https://www.entrust.com/legal-compliance/data-privacy/sub-processors.

How Long Do We Retain Your Biometric Data?

We and our service providers may retain Biometric Data until: (i) the initial purposes for collecting Biometric Data have been satisfied; (ii) within 3 years of your last interaction with our customer; or (iii) such shorter period to the extent required by applicable law, whichever occurs first. Upon the occurrence of either (i), (ii) or (iii), we will permanently destroy your Biometric Data.

How Do We Secure Your Biometric Data?

We and our service providers use a reasonable standard of care to store, transmit, and protect Biometric Data from unauthorized disclosure. Such storage, transmission, and protection from unauthorized disclosure will be performed in a manner that is the same as or more protective than the manner in which Entrust and its service providers (as applicable) store, transmit, and protect other confidential and sensitive information from unauthorized disclosure.

Data Privacy Rights

If you are a User with questions about how your Biometric Data may be processed via the Services, please contact our customer directly since they are the controller for this processing. (Entrust merely processes data on the customer's behalf as their processor and service provider when providing the Services.)

Entrust is the controller when using Biometric Data directly to improve its Services. If you have questions about this processing, you may contact us here.

Amendments to this Policy

We reserve the right to amend this Biometric Data Policy 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 policy from time to time to stay informed.

Contact Information

For questions about this policy, please contact privacy@entrust.com.