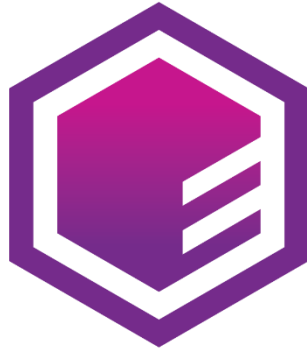




ENTRUST

DATA PRIVACY FREQUENTLY ASKED QUESTIONS

Contents

Data Privacy Frequently Asked Questions (FAQs).....	3
Privacy Laws and Regulations.....	3
Personal Data Processing	4
Contacts and Resources	6

Data Privacy Frequently Asked Questions (FAQs)

Last updated: December 23, 2024

Please find below answers to commonly asked questions about Entrust's data privacy program. Additional information can be found under the [Data Privacy](#) tab in the [Legal & Compliance](#) section of www.entrust.com.

Privacy Laws and Regulations

With global operations and customers located around the world, Entrust continually evaluates its program against current and emerging data privacy regulations. While we monitor all applicable global data privacy laws, Entrust's program is built around compliance with the EU General Data Protection Regulation (GDPR) to ensure we comply with the most stringent set of data privacy requirements regardless of where we are processing personal data. To comply with the GDPR and other applicable data privacy regulations, Entrust does the following:

- Oversees global company policies and notices around data protection
- Completes impact assessments for higher risk personal data processing
- Utilizes appropriate data transfer mechanisms for cross-border transfers of personal data
- Regularly trains colleagues on data privacy requirements
- Periodically conducts internal audits of data protection policies and procedures
- Investigates, remediates, and provides appropriate notice to data subjects and/or regulators in the event of a security incident
- Holds sub-processors to the same data management, security, and privacy practices and standards to which Entrust holds itself
- Responds to data subject requests and assists customers in responding to these requests as needed
- Ensures our products and services include adequate and appropriate technical safeguards and security control
- Incorporates data privacy considerations at the outset of product design and enhancement

You can find more detail in our [Global Personal Data Protection Policy](#).

Are Entrust products compliant with HIPAA?

To date, Entrust has only formally evaluated IDaaS against HIPAA requirements. This product may be used to process protected health information (PHI) (e.g., for use in authenticating patients in patient portals). To enter into a BAA with Entrust for this particular use case, visit the [Data Privacy](#) page and scroll down to the section entitled "HIPAA-Covered Services."

Cross-Border Transfers of Personal Data

How does Entrust handle cross-border personal data transfers where these are restricted or require special controls be in place under equivalent data protection legislation?

Under certain data protection legislation (e.g., EU GDPR, UK GDPR, Swiss FADP, and China PIPL), Entrust may only transfer personal data across borders where there is an adequate level of protection

in the country where the data is to be transferred and/or where Entrust has put appropriate measures in place to ensure data protection. Companies within the Entrust group (i.e., all corporate entities and subsidiaries) must enter into Entrust's Intra-Group Data Transfer Agreement in order to ensure appropriate safeguards for cross-border transfers of personal data within the Entrust group. Third party vendors who process personal data for or on behalf of Entrust (regardless of whether Entrust is acting as a data controller or data processor) must enter into a Data Processing Addendum (DPA) with Entrust to ensure appropriate safeguards for cross-border transfers of personal data. The DPA contains language to ensure the third party has appropriate technical and organizational measures in place to comply with relevant legislation (e.g., including the most recent version of relevant standard contractual clauses) and to ensure the protection of data subject rights.

To access Entrust's standard DPA templates, visit the [Data Privacy](#) page and scroll down to the section entitled "Data Processing Addenda (DPAs)." You can also enter your email address to be automatically notified of material changes to Entrust's standard DPA templates.

How does Entrust respond to law enforcement requests for customer personal data?

While Entrust will comply with mandatory, legal requests for information, we are also committed to complying with data privacy laws. As such, we will take appropriate measures to ensure that affected customers are notified as soon as legally possible, and we will disclose the minimum amount necessary to satisfy the requirements of the order. For customers with specific information about the potential reach of U.S. law enforcement under FISA, E.O. 12.333 or the ECPA to their personal data processed by Entrust, please refer to our whitepaper on this topic found [here](#).

Personal Data Processing

Is Entrust a data processor or a data controller?

Entrust acts as both a data processor and a data controller with respect to customer personal data. When customers use Entrust services and products that process customer personal data, Entrust acts as a data processor. When Entrust processes customer personal data and determines the purpose and means of processing with respect to that data (e.g., customer account information, customer service and support ticketing information) Entrust acts as a data controller.

How do I know if Entrust processes my personal data?

To review specifics related to navigation across our websites, please visit our [Web Privacy Statement](#). To review specifics related to our products and services, please visit our [Product Privacy Notices](#).

Does Entrust use any sub-processors to process my personal data?

You can find an accurate and detailed list of Entrust's sub-processors broken down by product [here](#). Entrust has appropriate DPAs in place with all of its sub-processors.

Does Entrust use a third party to manage cookies on their website?

Entrust uses Osano to manage cookies. Refer to our [Cookie Policy](#) for more information and to manage your cookie preferences.

How do I execute a DPA with Entrust?

Entrust makes it simple for our customers and vendors to sign and submit our DPA by making available pre-signed DPAs on our website. We strongly recommend proceeding with our standard DPAs as they have been carefully crafted and reviewed by internal and external privacy counsel and are designed specifically to address Entrust's business. The deviations that we will be able to make

to our standard DPAs are extremely limited; however, we hope that you will find our DPAs thoughtful, thorough, and fair.

The [Customer DPA](#) is for engagements where Entrust will be acting as the data processor for a Customer purchasing, accessing, and/or licensing Entrust products or services.

The [Vendor DPA](#) is for engagements where Entrust will be acting as the data controller and purchasing, accessing and/or licensing products or services from a third party who will act as a data processor.

How does Entrust secure my personal data?

When processing personal data, Entrust takes adequate measures to ensure personal data remains secure and protected against unauthorized or unlawful processing, accidental loss, destruction or damage. Entrust does this by maintaining an ISO 27001 and 27701-certified security and privacy program.

ISO 27001 is one of the most widely recognized and internationally accepted information security standards. It identifies requirements for a comprehensive Information Security Management System (ISMS) and defines how organizations should manage and handle information in a secure manner, including appropriate security controls.

ISO 27701 is the first global privacy standard that focuses on the protection of personally identifiable information (PII). ISO 27701 extends the requirements of ISO 27001 to include data privacy, and provides a framework for implementing, maintaining, and continuously improving a Privacy Information Management System (PIMS). While there is no specific EU GDPR certification, the ISO 27701 controls directly map to the articles of the GDPR and also take into account other national data protection laws.

To learn more about our ISO 27001 and 27701 certifications, please click [here](#).

How does Entrust ensure its employees have proper privacy education and training?

Entrust provides colleagues with data privacy training at the time of hire and annually thereafter through online Code of Ethics, Data Privacy, Records Management and Information Security Awareness trainings. Entrust also maintains a robust data privacy page with resources and information available on demand to all colleagues.

How would Entrust respond to a data breach or security incident?

Entrust makes every effort to ensure personal data remains protected; however, in the event of a security breach or security incident involving personal data, Entrust has a detailed security incident response plan that will be activated to ensure swift action is taken, including appropriate remediation and notification to affected data subjects and regulators as required by law.

How does Entrust handle data subject requests?

Entrust respects the rights of individual data subjects to request access to and/or correction and deletion of their personal data processed by Entrust. To submit a data subject request, we ask that you complete our [DSR form](#) to ensure we have all of the information required to appropriately investigate and respond to your request. Alternatively, you may call 1-888-563-9240 to submit your request.

Note that we may need to request additional information from you to verify your identity or understand the scope of your request, although you will not be required to create an account with us to submit a

request or have it fulfilled. We will require you to provide, at a minimum, your full name and email address.

Contacts and Resources

If you have questions about Entrust's privacy program, please contact:

Entrust Corporation
Attention: Jenny Carmichael, VP, Compliance
1187 Park Place Shakopee, MN 55379
privacy@entrust.com

How can I stay up to date on Entrust's privacy program?

The best place to find accurate and current information about our program is to visit the [Data Privacy](#) section of www.entrust.com. To share thoughts or feedback related to our program, please email privacy@entrust.com.