Website Privacy Statement

Last updated October 23, 2024

Entrust Corporation and any subsidiaries or affiliates that operate Websites ("Entrust") value and respect your privacy. This Website Privacy Statement ("Privacy Statement") describes the types of personal data we collect when you access our websites and browser-based portals that link to this Privacy Statement (the "Websites"), our practices for collecting, using, and sharing such personal data, and your rights with respect to such personal data. **We strongly encourage you to read this Privacy Statement in its entirety.**

Please note that this Privacy Statement does *not* apply to personal data collected by Entrust via Entrust's other business products and services, in which case Entrust typically acts as a service provider to our business clients (please see the section below titled "Entrust as a Service Provider" for additional information), and does not apply to personal data collected by Entrust (i) via Entrust's mobile applications, (ii) in its role as an employer or prospective employer, or (iii) through other means, e.g., information we collect when you interact with us at industry conferences or via phone or email, or information we collect from third parties, which, in each case, Entrust's data collection and processing practices are governed by separate privacy statements.

By continuing to use the Websites, you have accepted this Privacy Statement in its entirety and without modification and agreed to our collection, use, and sharing of your personal data, as described in this Privacy Statement. If you do not agree with this Privacy Statement, please do not use the Websites.

We may revise this Privacy Statement periodically and will post any changes to the Websites. Changes to this Privacy Statement are effective at the time they are posted, and your continued use of the Websites after posting will constitute acceptance of, and agreement to be subject to, those changes. Please review this Privacy Statement from time to time to ensure you are aware of changes to this Privacy Statement.

Entrust as a Service Provider. In providing services to our business clients Entrust acts as a service provider (also known as a "data processor"). Our clients – many of which are financial, healthcare, educational, retail, or governmental institutions – use our products and services to help securely process data of their customers and employees.

Therefore, if you are using Entrust products or services as a customer or employee of an Entrust client, then any information collected in connection with such use will be processed and shared in accordance with that client's privacy policies and practices and, to the extent applicable, our product-specific privacy notices in our capacity as such client's service provider. If you have questions about the processing of your personal data by an Entrust client using an Entrust product or service, please contact that client directly.

What Personal Data Does Entrust Collect?

When we refer to **personal data** (or "personal information") in this Privacy Statement, we mean information that identifies, relates to, describes, is reasonably capable of being associated with, or is linked or reasonably linkable to you, either alone or in combination with other information. More detail about the types of personal data Entrust collects is set forth below. References to "personal data" or "personal information" do not include aggregated and de-identified information. We will maintain and use this data only in a de-identified fashion and will not attempt to re-identify the data.

Information you provide to us

We collect the personal data that you provide to us when you visit our Websites. This includes the personal data you provide when you register to use our Websites (i.e., create an Entrust user account), request information about our services using our Websites' web forms, purchase or subscribe to products or services from our Websites, conduct searches on the Websites, or utilize our Websites' chat feature.

The information you provide may include identifiers, such as your name, phone number, email address, and mailing address; professional information, such as your job function, title and place of employment; your financial account or debit or credit card information; and any other information you choose to submit to us via the Website in connection with the foregoing.

Information collected automatically

When you visit our Websites, we collect information relating to the access, usage, and performance of our Websites, which is then stored in electronic records called logs. These logs may record online identifiers (e.g., usernames, unique device identifiers, or MAC addresses), IP addresses, the name and version of your operating system and browser, referring pages, the pages visited, dates and times of access, and information regarding errors and functionality.

We may also use cookies and similar technologies, and allow certain third parties to use cookies and similar technologies, to collect information related to your visit. This information typically includes your IP address, online identifier (e.g., username, unique device identifier, or MAC address), the identity of your Internet Service Provider, the name and version of your operating system and browser, information about your device type, the date and time of your visit, the pages you visit, the search terms you enter, and your preferences. For more information, please see our Cookie Policy.

Information We Infer. We may combine the information you provide to us and information we collect about you. We may also draw inferences from such information (including, for example, non-precise geolocation data) in order to create a profile reflecting your characteristics, interests, and preferences. We will use the combined information and inferences for the purposes set out below (depending on the types of information we receive).

For What Purposes Do We Use The Information We Collect?

Where applicable law requires us to have a so-called "lawful basis" for processing personal data, we only process personal data where we have such a lawful basis to do so (e.g., necessary for the performance of a contract, to comply with a legal obligation, to pursue our legitimate interests or where we have consent).

We collect and process personal data for various purposes, including:

- To set up and maintain your Entrust user account and validate your license to access our Websites, online products and services;
- To verify your information and to process and complete online transactions and send related communications and information, including transaction confirmations and invoices (we use your financial account or credit or debit card information only for the purpose of processing your purchase);
- To provide, maintain, or troubleshoot access to our Websites;
- To monitor, evaluate, and improve the content, functionality and usability of our Websites (e.g., debugging, measuring website traffic, etc.);
- To investigate and prevent fraudulent or illegal activity or unauthorized access to our Websites;

- To communicate with you, including to respond to your inquiries, to provide you with effective customer service, and to invite you to participate in surveys and provide feedback to us;[1]
- To conduct internal research and development;
- To comply with applicable laws or regulations;
- For advertising and marketing purposes, including to contact you with personalized offers and other information we believe may be of interest to you;
- To deliver relevant advertising to you, and to audit, measure, and understand the effectiveness of advertising we serve to you and others;
- To ensure that content from our Websites is presented in the most effective manner for you and for your device.

We may aggregate or de-identify personal data collected via the Websites so that such information can no longer be linked to you or your device. We may use aggregated or de-identified information for any purpose, in our discretion.

Does Entrust Share And Disclose Personal Data?

We may share and disclose your personal data in certain circumstances, including:

- We may disclose or transfer your personal data to Entrust subsidiaries or affiliates.
- We may disclose or transfer your personal data as part of a potential or actual company merger, acquisition, sale of a portion of Entrust or our assets or as part of a bankruptcy proceeding or a business reorganization.
- We may share your personal data with third parties who provide services to us. Examples of third-party service providers (also known as “data processors”) include payment processing providers, credit reference agencies, website analytics and advertising companies, and service providers who operate, maintain and support our websites, products and services.
- We may disclose personal data to protect, enforce or defend our rights or those of others, or where we believe the disclosure is required by law.
- We may disclose personal data to prevent or investigate a possible crime, such as fraud or identity theft, or to protect the security of our Websites, products and services.

We may also share aggregated or de-identified information with third parties, in our discretion.

[1] Where Entrust communicates with you via SMS to provide customer service or support, we will obtain your consent prior to using this method of communication and that consent will not extend to any third parties.

Digital Advertising And Analytics

We may partner with ad networks and other ad serving providers ("Advertising Providers") that serve ads on behalf of us and others on non-affiliated platforms. Some of those ads may be personalized, meaning they are intended to be relevant to you based on information Advertising Providers collect about your use of our Websites and other websites or apps over time, often through the use of cookies or similar technologies, including information about relationships among different browsers and devices. This type of advertising is known as targeted advertising (also referred to as "cross-context behavioral advertising").

We may also work with third parties that collect data using cookies and similar technologies about your use of our Websites and other sites or apps over time for non-advertising purposes. Entrust uses Google Analytics and other third-party services to improve the performance of the Websites and for analytics or marketing purposes. For more information about how Google Analytics collects and uses data when you use the website, visit www.google.com/policies/privacy/partners, and to opt out of Google Analytics, visit tools.google.com/dlpage/gaoptout.

If you would like to opt out of Entrust's targeted advertising or analytics cookies, please visit our Cookie Policy and click on the "Cookie Settings" button. From there, you have the ability to adjust your cookie settings so that only strictly necessary cookies are activated.

How Long Do We Retain Personal Data?

We only retain personal data for as long as reasonably necessary for the purpose in which it was collected. For example, where your personal data is needed to provide you with access to our websites, online products or services, we retain your personal data for the period in which we are providing that access unless we are required by law to dispose of it earlier or to keep it longer. We also retain personal data as necessary to comply with our legal obligations, resolve disputes, pursue legitimate business interests, conduct audits, and protect or enforce our rights.

Protecting Your Personal Data

We use reasonable administrative, technical, and physical security measures to protect your personal data from loss, misuse, unauthorized access, disclosure, alteration, and destruction. These security measures are designed to provide a level of security appropriate to the risk of processing your personal data.

Where we have given you (or where you have chosen) a password which enables you to access certain parts of our Websites, you are responsible for keeping this password confidential. You should not share your password with anyone.

Unfortunately, the transmission of information via the internet is not completely secure. Although we will do our best to protect your personal data, we cannot guarantee the security of your data transmitted to our Websites or stored in our databases. Your transmissions are, therefore, at your own risk.

International Data Transfers

The personal data that we collect from you may be transferred to and/or stored at a destination on our servers or our third-party servers that is different from the location where it was collected. It may also be processed by staff who work for us or for one of our service providers in a location different from where the data was collected. We will only transfer your personal data as permitted by law. Certain privacy and data protection laws require data controllers to put in place safeguards to protect personal data transferred across borders. For more information about Entrust's compliance with data protection laws governing cross-border transfers of personal data, please review our Data Privacy FAQ page available here.

Who Is The Data Controller?

The data controller of the personal data we collect via the Websites is Entrust Corporation. For more information about when Entrust is the "data processor," please see the section titled "Entrust as a Service Provider" above.

What Rights Do You Have With Respect To Your Personal Data?

Certain states' and countries' data protection laws provide their residents with rights regarding businesses' use of their personal data, including the rights to know, access, correct, transfer, restrict the processing of (including specific restrictions that may pertain to the sale or sharing of personal information, the processing of sensitive information, and more), and delete personal data. Regardless of your state or country of residence, you can currently contact Entrust at any time using the instructions set out below to request that we:

- confirm whether we process your personal data;
- disclose the categories of personal data that we have collected about you;
- disclose the categories of sources from which we have collected your personal data;

- disclose our purpose(s) for collecting, disclosing, or selling your personal data;
- disclose the categories of personal data about you that we have sold, and the categories of recipients of such personal data;
- disclose the categories of personal data about you that we have disclosed to third parties for business purposes and the categories of recipients of such personal data;
- delete all or some of your personal data;
- change, update, or correct your personal data;
- disclose the specific pieces of personal data that we have collected about you and provide you with a copy of such personal data in a commonly used electronic format (or ask that it be provided in that format to a third party);
- stop selling your personal data and stop sharing or processing your personal data for purposes of targeted advertising (also known as "cross-context behavioral advertising").

We will consider and respond to your requests promptly, and otherwise in accordance with all applicable laws. Furthermore, if you choose to exercise your privacy rights or make the above requests, Entrust will not treat you in a discriminatory way, nor will you receive a lesser degree of service from Entrust.

If you are a California resident, please see the section titled "California Privacy Rights" below.

Instructions for submitting requests. You can make any of the above requests by either visiting our Data Subject Request Form available here, by emailing us at privacy@entrust.com using subject line "Data Subject Request" and clearly stating the request(s) you'd like to make, or by calling us toll-free at 1-888-563-9240.

In order to help ensure that your personal data is not disclosed to any person who does not have the right to receive it, and to help ensure your personal data is not mistakenly deleted or changed, Entrust will attempt to verify that you are the subject of the personal data you are requesting to access, delete, or correct. We may ask for your email address and about your relationship to Entrust (e.g., Website user, customer, vendor, employee, etc.). We will compare the information you provide to any information we may have in our possession in order to verify your identity. We may also contact you at the email address you've provided to request additional information in relation to your request. Entrust will

use the information collected through the request process only for verification purposes and responding to your request.

We will confirm receipt of your request within ten (10) business days. If you do not receive confirmation within the 10-day timeframe, please email us at privacy@entrust.com.

We endeavor to substantively respond to a verifiable request within 30 days of its receipt. If we require more time (up to another 30 days), we will contact you at the email address you provide.

Authorized Agent. You may also choose to authorize an agent to make the above requests or exercise your rights. If you use an agent, we will take measures to verify your agent's authorization to act on your behalf and we may require more information to ensure proper verification of both you and your agent's identity and authorization.

Please note that Entrust may not be able to respond to your request if we cannot verify your identity, or your agent's identity and authority to make the request, and confirm the personal data relates to you.

Appeals Procedure. You may appeal our decision to decline your request by emailing us at privacy@entrust.com using subject line "Data Subject Request Appeal" and clearly stating the decision(s) you wish to appeal. We will respond to your appeal within 30 days of our receipt of your email, which response will include an explanation of our decision. If you are dissatisfied with our decision on appeal, and you live in a jurisdictions that allows for individuals to =engage a regulatory authority regarding our decision, Entrust will provide a link to relevant regulatory authority's website in our response.Additionally, you can object to the processing of your personal data in some circumstances (e.g., where we don't have to process the information to meet a legitimate interest, contractual or other legal requirement). Your right to object to processing of your personal data may be limited in certain circumstances (e.g., where fulfilling your request would reveal personal data about another person or where you ask us to delete information which we are required by law to keep or have other compelling legitimate interests to keep such as for purposes of fraud prevention). As noted above, 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.

If we have collected and processed your personal data with your consent, then you can withdraw your consent at any time by contacting privacy@entrust.com. Withdrawing your consent will not affect the lawfulness of any processing we conducted prior to your withdrawal, nor will it affect processing of your personal data on lawful processing grounds other than consent.

We may send you direct marketing without requiring your consent to the extent permitted by applicable law; for example, where our marketing is based on other lawful grounds. To opt out of receiving marketing communications from Entrust, please click here, or click the "unsubscribe" link in the footer of any marketing email communication.

Children's Privacy

We do not knowingly collect personal data on individuals under 18 years of age on Entrust's Websites. Certain identity verification products may collect personal data of users under 18 years of age depending on how Entrust's business clients use our products and services. Details regarding processing of personal data of users under the age of 18 can be found in Entrust's product specific privacy notices.

External Websites

Our Websites may contain links to third-party websites. We do not control, and are not responsible for, the content or privacy practices of these other websites. Our provision of such links does not constitute our endorsement of these other websites, their content, their owners, or their practices. This Privacy Statement does not apply to third-party websites.

California Privacy Rights

This section contains disclosures required by the California Consumer Privacy Act, as amended by the Consumer Privacy Rights Act ("CCPA").

Personal Information We Collect. In the preceding 12 months, we collected the categories of personal information about California consumers set out in the section titled "What Personal Data Does Entrust Collect?" above, for the purposes described in the section titled "For What Purposes Do We Use the Information We Collect?" above.

Categories of Sources. We collected the above-mentioned personal information from the sources described in the section titled "What Personal Data Does Entrust Collect?".

Disclosing Personal Information for Business Purposes. We may disclose your personal information to a third party for the purposes set out in the section titled "Does Entrust Share and Disclose Personal Data?".

Sale and Sharing of Personal Information. We may share your personal information with third parties, including for purposes of cross-context behavioral advertising, which may constitute "selling" or "sharing" under the CCPA. Such sale or sharing does not include information about individuals we know are under age 16. In the preceding twelve (12) months, Entrust has sold or shared the categories of personal information listed below with the categories of third parties listed below. For more instructions to opt out of this sale or sharing, please see the section titled "What Rights Do You Have with Respect to Your Personal Data?" above or click on the "Do Not Sell or Share My Personal Information" button located in the footer of the Websites.

Categories of Personal Information	Shared with the following categories of third parties:
Personal and online identifiers (such as first and last name, email address, IP address, or unique online identifiers)	• Advertising/marketing companies • Advertising networks • Marketing data companies • Data analytics providers • Social networks
Internet or other electronic network activity information (such as browsing history, search history, and information regarding a consumer's interaction with an internet website)	
Professional or employment-related information	
Inferences drawn from the above information about your predicted characteristics and preferences	
Other information about you that is linked to the personal information above	

Sensitive Personal Information. We do not collect or use sensitive personal information other than financial account or debit or credit card information when you make a purchase online, which information is used only to process your payment for such purchase.

An Explanation of Your Rights. The CCPA provides consumers (California residents) with specific rights regarding their personal information. Please see the section titled "What Rights Do You Have With Respect to Your Personal Data?" above for an explanation of those rights and how you may exercise them.

Contact Us

If you have questions or concerns about this Privacy Statement or our handling of your personal data, please contact us at privacy@entrust.com or:

Entrust Corporation
Attention: Jenny Carmichael, VP of Compliance
1187 Park Place
Shakopee, MN 55379