Job Applicant Privacy Statement

Last updated January 10, 2024

Entrust Corporation and any of its subsidiaries or affiliates ("Entrust") value and respect your privacy. This Job Applicant Privacy Statement sets forth how we will use any personal data we collect or that you provide to us as a job applicant. **We strongly encourage you to read this Job Applicant Privacy Statement in its entirety.**

When we refer to **personal data** (or "personal information") in this Job Applicant 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 from job applicants ("Applicant Information") is set forth below.

What personal data does Entrust collect from Job Applicants?

Information you provide to us

We may collect the following Applicant Information from you as a job applicant:

- Your name, address and contact details, including email address and telephone number, place of birth, date of birth, marital status, nationality, gender;
- Details of your qualifications, educational background, skills, experience, and employment history, including start and end dates with previous employers;
- Information about your entitlement to work;
- Information about your current level of remuneration, including benefit entitlements;

Depending on local law, we may also collect and process the following "special categories" of Applicant Information:

- Information about medical or health conditions, and whether you have a disability for which the organization needs to make reasonable accommodations during the recruitment process;
- Equal opportunity monitoring information, including information about your ethnic origin, sexual orientation and religion or belief;
- Information about your financial credit history and criminal record;
- In the United States, and depending on the role, you may be required to undergo drug screening and provide Entrust with your fingerprints.

Entrust may collect this information directly from you through application forms, CVs or resumes, passport or other identity documents such as your driver's license, correspondence with you or through interviews, meetings or other assessments.

Information we collect

Entrust may also collect Applicant Information about you from third parties such as former employers and employment background check providers, depending on local law. We will only collect this information once a job offer has been made to you. Before we conduct these checks, we will generally inform you that we are doing so to obtain your consent, and to let you know what information will be collected, from whom the information will be collected, and what we will do with the information. However, that is not always possible in all circumstances (for example, where informing you in advance could amount to an offense or otherwise prejudice others).

For what purposes do we use the employment information we collect?

Where applicable law requires us to have lawful basis for processing Applicant Information, we only process Applicant Information 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 need to process Applicant Information to manage the recruitment process, assess and confirm a candidate's suitability for employment, and decide whom to offer a job. Entrust also needs Applicant Information to respond to and defend against legal claims should any arise in the context of the job application process.

In some cases, we need to process Applicant Information to ensure compliance with our legal obligations. For example, we are required to check a successful applicant's eligibility to work in the country in which they are applying before employment starts. We may also be legally required to collect information about an applicant's disability to determine whether reasonable accommodations need to be made for that individual.

Entrust also has a legitimate interest in processing Applicant Information during the recruitment process to follow safe employment practices. For example, we may seek information about criminal convictions and offenses where local law allows.

Does Entrust share and disclose employment information?

Entrust may share and disclose Employment Information in the following limited circumstances:

- **Corporate Affiliates.** Applicant Information may be shared internally with other Entrust affiliates, including Human Resources and Talent Acquisition, interviewers involved in the recruitment process, managers in the business area with the vacancy, and IT staff if access to the data is necessary for the performance of their roles. These Entrust affiliates are permitted to use Applicant Information in a manner consistent with this Job Applicant Privacy Statement.
- **Third Party Service Providers.** Entrust will not share your Applicant Information with third parties unless your application for employment is successful and we extend an offer of employment. Entrust may then share your Applicant Information with third-party vendors, consultants, or other service providers. These third-parties process Applicant Information pursuant to Entrust's instructions and solely for the purpose and under the security measures indicated in the agreements we sign with them. These third-party vendors may be responsible for pre-employment references and background checks, criminal records checks, and financial credit checks. Entrust currently uses HireRight with servers to perform background checks, with servers in the US, as well as servers in the EU for positions in APAC and EMEA.
- **Former Employers.** Once an offer of employment has been made and accepted, Entrust may provide your Applicant Information to your former employers for purposes of obtaining references and verifying prior employment.

How long do we retain applicant information?

If your application for employment is unsuccessful, we will hold your Applicant Information on file after the conclusion of the recruitment process in order to build a talent database for potential future recruitment activities. You may withdraw your consent at any time, at which point your Applicant Information will be deleted.

If you are located in the European Economic Area (EEA), we will hold your Applicant Information on file for 24 months after the conclusion of the recruitment process in order to build a talent database for potential future recruitment activities. At the end of the applicable period, or once you withdraw your consent, your Applicant Information will be deleted.

If your application for employment is successful, Applicant Information gathered during the recruitment process will be transferred to your personnel file and retained in line with our Employee Privacy Statement.

How do we protect your applicant information?
Entrust is an ISO 27001 and 27701 certified organization and uses appropriate technical, organizational, and administrative security measures to protect your Applicant Information from loss, misuse, unauthorized access, disclosure, alteration, and destruction. We also ensure we have Data Processing Agreements (DPAs) in place with all third party vendors to whom we transfer personal data. These security measures are designed to provide a level of security appropriate to the risk of processing your Applicant Information.

Storage and international data transfers
The Applicant Information 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 suppliers in a location different from where the data was collected. We will only transfer your Applicant Information as permitted by law. Certain privacy and data protection laws require data controllers to put in place safeguards to protect Applicant Information transferred across borders. To comply with this requirement, Entrust utilizes the standard contractual clauses recommended by the relevant data privacy regulators for all international transfers of data (both internally and to third-party vendors) to provide adequate safeguards for Applicant Information.

Entrust digitally stores application information on Workday, a third party platform with servers in the US.

Who is the data controller?
Entrust Corporation is the entity acting as the data controller of your Applicant Information.

What rights do you have with respect to your applicant information?
Depending upon the applicable data protection law in your country of residency, you may in some circumstances have the right to ask Entrust for information relating to Applicant Information about you we control and process; to correct, delete, or restrict any active processing of your Applicant Information; and to obtain a copy of your Applicant Information in a structured, machine-readable format.

Additionally, you can object to the processing of your Applicant Information 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 your Applicant Information may be limited in certain circumstances (e.g., where fulfilling your request would reveal Applicant Information 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).

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 Entrust has collected and processed your Applicant Information 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 Applicant Information on lawful processing grounds other than consent.

What if you do not provide Applicant Information?

You are under no statutory or contractual obligation to provide Applicant Information to Entrust during the recruitment process. If, however, you do not provide the information, we may not be able to process your application or consider you for employment.

Amendments to this Job Applicant Privacy Statement

We reserve the right to amend this Job Applicant Privacy Statement from time to time as our business, laws, regulations, and industry standards evolve. Any changes are effective immediately following the posting of such changes on https://www.entrust.com/legal-compliance/data-privacy. We encourage you to review this statement from time to time to stay informed. Please note that any subsequent application for employment with Entrust following changes to the Job Applicant Privacy Statement will be subject to the revised Job Applicant Privacy Statement.

Other notices

This Job Applicant Privacy Statement is not intended to replace other notices provided by Entrust in accordance with national and local laws and regulations. In the event of any conflict between this Statement and other notices required by local law, the notices

required by local law will prevail. This Job Applicant Privacy Statement applies to the processing of Applicant Information by or on behalf of Entrust anywhere in the world.

Contact us

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

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

To exercise your data subject rights, please use our online form. We will do our best to answer your questions and address your concerns. If you are still not satisfied, you may lodge a complaint with your national data protection supervisory authority. The European Data Protection authorities can be found here. The UK Information Commissioner's Office (ICO) can be found here. The Office of the Privacy Commissioner of Canada can be found here. The Cyberspace Administration of China (CAC) can be found here.