Job Applicant Privacy Statement

Last updated February 21, 2022

Entrust Corporation ("Entrust") values and respects 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.

Personal data is information that identifies you, either alone or in combination with other information available to Entrust (e.g., your name or email address). 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 personal data from you as a job applicant:

- Your name, address and contact details, including email address and telephone number, date of birth, marital status, nationality, gender;
- Details of your qualifications, 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 data:

- Information about medical or health conditions, and whether or not 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 personal data 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 inform you that we are doing so in order 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.

How do we use the applicant information we collect?

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 in order 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 we comply 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 in order 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 applicant information?

Entrust may share and disclose Applicant 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.

- **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.

Entrust will never sell, rent or lease your personal data to a third party.

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, personal data 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 uses appropriate technical, organizational and administrative 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.

Storage and 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 suppliers in a location different from where the data was collected. By submitting your personal data, you agree to this transfer, storage or processing. 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. To comply with this requirement, Entrust has put in place agreements that include the standard contractual clauses recommended by the European Commission to provide adequate safeguards for personal data.

Entrust digitally stores applicant materials on Workday, a third-party platform with servers in the US.

Who is the data controller?

For residents of countries in the European Economic Area (EEA), please refer to the following table to identify the Entrust entity acting as data controller of your personal data.

Country	Data Controller	Address
Czech Republic	Entrust Security Solutions UK Limited	Forum 3, Solent Business Park, Whiteley, Fareham, PO15 7FH, England
Denmark	Entrust Denmark A/S	Park Alle 350D, 2605 Brøndbyvester, Denmark
France	Entrust France S.A.S	ZAC des Châtelliers, 200 rue Léonard de Vinci, Semoy-45404 Fleury les Aubrais Cedex, France
Germany	Entrust Deutschland GmbH	Lütticher Strasse 132, 40547 Düsseldorf, Germany
Spain	Entrust Solutions Spain, S.L.U.	Parque Empresarial la Finca, Paseo Club Deportivo

		1 bl 3, 28223 Pozuelo de Alarcón, Madrid, Spain
United Kingdom	Entrust Security Solutions UK Limited	Forum 3, Solent Business Park, Whiteley, Fareham, PO15 7FH, England
	Entrust (Europe) Limited	6th Floor, Abbey Gardens, Abbey Street, Reading RG1 3BA, United Kingdom
	nCipher Security Limited	One Station Square, Cambridge CB1 2GA, United Kingdom
	Nu-Type Limited	Weycroft Avenue, Millwey Rise, Axminster, Devon EX13 5HU, United Kingdom

For non-EEA residents, you may obtain this information by contacting your recruiter.

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 have the right to ask Entrust for information relating to personal data about you we control and process; to correct, delete, or restrict any active processing of your personal data; and to obtain a copy of your personal data in a structured, machine readable format.

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 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).

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 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.

What if you do not provide applicant information?

You are under no statutory or contractual obligation to provide personal data 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 www.entrust.com. 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 personal data, please contact us at privacy@entrust.com. To opt-out of receiving information about Entrust job opportunities, please click here. To submit a Data Subject Access Request, 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.