ENTRUST

GLOBAL PERSONAL DATA PROTECTION POLICY

Document Version	1.2
Date	10-Sept-2020

Contents

1. Introduction

As a business and an employer, it is necessary for Entrust Corporation and its subsidiaries and affiliates (collectively, "Entrust" or the "Company") to collect, store and process personal data about our employees, contingent workers, customers, suppliers and other third parties with whom we engage to provide products or services on our behalf.

With the introduction of the European General Data Protection Regulation ("GDPR") on May 25, 2018 and other applicable laws governing data protection, we are subject to enhanced requirements regarding how we collect, use, and store personal data.

2. Purpose

The purpose of this policy is to help all of us comply with our legal obligations and enable individuals about whom we hold personal data to have confidence in us. This policy applies to all Entrust employees, contingent workers and third parties processing data on behalf of Entrust. Unless specified, this policy applies in all countries in which Entrust operates and/or conducts business.

3. Policy Requirements

3.1 Definitions

"Data Controller" means the entity that determines the purpose and means of Processing Personal Data.

"Data Processor" means the entity that Processes Personal Data on behalf of the Controller.

"Data Protection Laws" means all applicable data protection and data privacy laws and regulations, including but not limited to the EU General Data Protection Regulation (GDPR), Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) and the California Consumer Privacy Act (CCPA).

"Data Subject" means the identified or identifiable person or household to whom Personal Data relates.

"Data User" is a term used to describe any employee, consultant, independent contractor, intern, temporary worker or third party acting on Entrust's behalf (including data processors) whose work involves processing personal data for Entrust.

"Personal Data" shall have the meaning ascribed to "personally identifiable information," "personal information," "personal data" or equivalent terms as such terms are defined under Data Protection Laws.

"Personal Data Incident" shall have the meaning assigned by Data Protection Laws to the terms "security incident," "security breach" or "personal data breach" and shall include any situation in which Vendor becomes aware that Personal Data has been or is likely to have been

accessed, disclosed, altered, lost, destroyed or used by unauthorized persons, in an unauthorized manner.

"Processing" means any operation or set of operations that is performed on Personal Data, whether or not by automatic means, such as collection, recording, organization structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing also includes transferring or disclosing personal data to third parties.

"Special Category Data" is a subset of personal data and refers to information about an individual's race or ethnic origin, sex life or sexual orientation, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data (eye color, hair color, height, weight), medical history, or criminal convictions and offenses or related security measures.

3.2 Our Responsibility

Depending on the circumstances, Entrust may act as a data controller or a data processor. As a data controller, Entrust is responsible for establishing practices and policies in line with Data Protection Laws. It is equally important that Entrust be able to demonstrate compliance with these laws. The Company does this by:

- Implementing policies that enable the Company to comply with data protection laws such as this policy, policies around document retention and data security, and Entrust's privacy statements;
- Communicating and training employees, contingent workers and third parties acting on behalf of Entrust about data protection requirements;
- Investigating instances of non-compliance with Entrust data protection policies and taking appropriate remedial and/or disciplinary action;
- Investigating, remediating and, in some instances, providing notification of a Personal Data Incident;
- Conducting data processing impact assessments where required for new types of processing activities;
- Undertaking periodic internal audits of Entrust's data protection policies and procedures; and
- Considering data protection at the outset of new product design.

3.3 Processing Personal Data

Any personal data that the Company processes or that is processed on Entrust's behalf must:

- Be processed fairly, lawfully and in a transparent manner;
- Be processed only for specified, explicit and legitimate purposes;
- Be relevant and limited to what is necessary for the legitimate purpose(s) for which the data is processed;

- Be accurate and kept up to date ensuring, where reasonably possible, that inaccurate personal data is erased or rectified without delay;
- Not be kept any longer than is necessary to fulfill the purpose(s) for which the data was collected; and
- Be processed in a manner that ensures appropriate security of personal data, including protection against unauthorized or unlawful processing, accidental loss, destruction or damage.

3.4 Legal Grounds for Processing Personal Data

The Company may only process personal data if permitted to do so under Data Protection Laws. The following are the grounds Entrust relies upon to process personal data:

Where processing is necessary:

- For the performance of a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into a contract;
- For compliance with a legal obligation to which Entrust is subject; and/or
- To pursue Entrust's legitimate interests, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject.

In addition to these grounds, Entrust may also process personal data where the data subject has given consent to the processing for one or more specified purposes, provided that the consent is freely given, specific, informed and an unambiguous indication of the data subject's wishes. Where Entrust uses consent as the grounds for processing, a data subject has the right to withdraw consent at any time and for any reason.

Entrust may, on occasion, also need to process special categories of personal data for employees or contingent workers (e.g., where required by safe employment practices). When Entrust processes or uses a third party to process on its behalf special categories of personal data, Entrust will ensure, where applicable, that the following conditions are satisfied:

- Data subject has given explicit consent to the processing of the special category of personal data for one or more specified purposes;
- Processing is necessary for carrying out obligations under employment law, social security or social protection law, or a collective bargaining agreement;
- Processing is necessary for the purposes of preventive or occupational medicine, or for the assessment of the working capacity of an employee;
- Processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving consent;
- Processing relates to personal data which has been made public by the data subject; and/or
- Processing is necessary for establishing or defending legal claims.

3.5 Data Records Management

Entrust maintains a central record of the types of personal data the Company collects and why that data is collected. Entrust will only process personal data for the specific purpose(s) set forth in the central record or for any other purpose(s) specifically permitted Data Protection Laws. Entrust will notify data subjects of those purposes when data is first collected or, where not possible, as soon as possible thereafter.

Entrust will only process personal data to the extent required for the purposes provided to the data subject. This means that Entrust may not ask for, or record in its systems, more personal data than is needed. The Company has appropriate technical and organizational measures in place to ensure that personal data that is no longer needed is erased or destroyed.

The Company also employs reasonable measures to ensure that any personal data held is accurate and kept up to date. Entrust aims to check the accuracy of any personal data at the point of collection and at regular intervals afterwards. The Company will take all reasonable steps to erase, destroy or amend inaccurate or out-of-date data without undue delay and, in any event, within one month of a data subject's request (or for up to three months where there are specific reasons why one month is not possible).

3.6 Erasure or Destruction of Personal Data

Paper records that contain personal data must be shredded and disposed of securely when there is no longer a need to retain them. *Paper records containing personal data may not be disposed of in any other manner.*

When deleting electronic personal data, all possible steps should be taken to put the data in question beyond use. Where it is impossible to delete personal data altogether, reasonable steps must be taken to ensure the data is deleted to the fullest extent possible.

IT is responsible for destroying or erasing electronic equipment that contains personal data (e.g. laptops, desktops, company-owned mobile devices, and work data on BYOD devices).

3.7 Information Security

When the Company processes personal data, it takes reasonable measures to ensure data remains secure and is protected against unauthorized or unlawful processing, accidental loss, destruction or damage. Entrust does this by:

- Encrypting personal data where possible and appropriate;
- Ensuring the ongoing confidentiality, integrity, availability and resilience of systems and services used to process personal data;
- Ensuring the restoration of access to personal data in a timely manner in the event of a physical or technical incident; and
- Facilitating testing, assessment and evaluation of the effectiveness of technical and organizational measures for ensuring data security.

In assessing the appropriate level of security, Entrust considers the risks associated with the processing, in particular the risks of accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to the personal data that is processed.

Where Entrust engages third parties to process personal data on its behalf, such parties do so based on written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organizational measures to ensure data security. Personal data may not be shared with anyone outside of Entrust or authorized third parties.

Desks and cupboards are kept locked if they hold personal data or confidential information of any kind. Data users ensure that individual monitors/screens do not show personal data or confidential information to passers-by and that they log off from or lock their computers/tablets when left unattended.

3.8 Reporting a Personal Data Incident

A Personal Data Incident can happen in many ways, including:

- Loss of a mobile device or hard copy file which contains personal data (e.g., accidentally leaving a device behind on public transportation);
- Theft of a mobile device or hard copy file which contains personal data (e.g., stolen from a vehicle or home);
- Human error (e.g., an employee accidentally sending an email containing personal data to an unintended recipient, or accidentally altering or deleting personal data);
- Cyber-attack (e.g., opening an attachment to an email from an unknown third party that contains ransomware or other malware);
- Allowing unauthorized use/access (e.g., permitting an unauthorized third party to access secure areas of Entrust offices or systems);
- Unforeseen circumstances such as a fire or flood; or
- Where information is obtained from Entrust by a third party through deception.

Signs that a Personal Data Incident may have occurred include the following:

- Unusual log-in and/or excessive system activity, in particular with respect to active user accounts;
- Unusual remote access activity;
- The presence of spoof wireless (Wi-Fi) networks visible or accessible from Entrust's working environment;
- Equipment failure; and
- Hardware or software key-loggers connected to or installed on Entrust systems.

Colleagues who become aware of or have any reason to suspect that a Personal Data Incident has occurred or is about to occur must immediately contact the Entrust Security Operation Center by email at SOC@entrust.com and the Compliance Director at privacy@entrust.com.

3.9 Personal Data Incident Response Plan

In the event of an actual or imminent Personal Data Incident, Entrust takes quick action to minimize the impact of the incident and report the incident if required by law. In most cases, the response will involve:

- Investigating the incident to determine the nature, cause and extent of the damage or harm that may result;
- Implementing necessary steps to stop the incident from continuing or recurring, and limiting the harm to affected data subjects;
- Assessing whether there is an obligation to notify other parties (e.g., national data protection authorities, affected data subjects) and making those notifications. If there is an obligation to notify data protection authorities, reporting must usually occur within 72 hours of the Company, including any of its employees, becoming aware of the incident; and
- Recording information about the Personal Data Incident and the steps taken in response, including documentation that explains the decision to notify or not notify.

3.10 International Data Transfers and Transfers to Third Parties

Under the GDPR, Entrust may transfer personal data to countries outside the European Economic Area ("EEA") where there is an adequate level of protection in that country 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 the Intra-Group Data Transfer Agreement in order to ensure appropriate safeguards for the transfer of personal data outside the EEA, but within the Entrust group.

Companies outside of the Entrust group who process personal data for or on behalf of Entrust, for which Entrust acts as a data controller or data processor, must enter into a data processing agreement with Entrust to ensure appropriate safeguards for the transfer of personal data outside the EEA. That agreement contains language to ensure the third party has appropriate technical and organizational measures in place to comply with the GDPR and to ensure the protection of data subject rights.

Instances where Entrust transfers personal data to a country outside the EEA may include:

- The data subject has given their explicit consent to the proposed transfer after Entrust has informed them of any possible risks associated with such transfer (e.g., the absence in that country of equivalent safeguards);
- The transfer is necessary for the performance of a contract to which the data subject is a party or to take steps at the request of the data subject prior to entering into a contract;
- The transfer is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving consent; or
- The transfer is necessary for the establishment or defense of a legal claim.

For each transfer of data outside the EEA, Entrust will rely upon the Standard Contractual Clauses as defined by the European Commission (2001/497/EC, 2004/915/EC and 2010/87/EU). Note that a data transfer agreement is also required if transferring personal data outside of Canada.

3.11 Notifying Data Subjects

Entrust is required to provide information to data subjects about the processing of their personal data. This information is contained in the Company's Privacy Statement which is publicly available at www.entrust.com, and the Employee Privacy Statement which is available on the Entrust intranet. Such statements provide information about:

- The types of personal data Entrust processes;
- The purpose and legal basis for processing personal data;
- Whether personal data will be disclosed to any third parties in the course of processing;
- Whether personal data will be transferred outside of the EEA and Canada and, if so, what safeguards will be put in place;
- How long the personal data will be processed or, if not possible to determine, the criteria the Company will use to determine the processing period;
- How the data subject can obtain a copy of their personal data held by Entrust;
- Data subject's rights, including how to make a complaint;
- If the personal data must be processed in order to comply with a law or a contract, the possible consequences of the data subject failing to provide the data or objecting to processing; and
- The existence and details of any automated decision-making processes, where applicable.

If Entrust receives personal data about a data subject from a third party, the Company will also provide the data subject with information on:

- The type of personal data received from the third party; and
- The source of the data and whether it came from a publicly accessible source (e.g., a website accessible to the public).

3.12 Privacy by Design and Data Protection Impact Assessments

Data Protection Laws require Entrust to consider data protection during the development stages of a new product offering. In order to satisfy this obligation, Entrust must take steps to ensure data protection is part of the design process and personal data collection is minimized to the extent possible.

In some circumstances (namely, when processing would result in high risk to an individual's rights and freedoms), Entrust may be required to undertake a formal data protection impact assessment (DPIA) in relation to the processing of personal data. Such an assessment involves documenting the purposes for which the activity is carried out, how Entrust will comply with data

protection laws and how the Company will mitigate potential risks to individuals' privacy. If you believe a data protection impact assessment may be needed, contact the Compliance Director at privacy@entrust.com.

3.13 Data Subject Rights

If Entrust processes personal data, under Data Protection Laws the data subject may have the right to:

- Request information about the personal data held with respect to them;
- Have any inaccurate personal data about them corrected and incomplete personal data completed, subject to Entrust determining that the data is, in fact, inaccurate or incomplete;
- Object to Entrust processing their personal data where the Company is doing so in pursuit of its own legitimate interests. Entrust can continue processing the personal data notwithstanding an objection if the Company's legitimate interests outweigh those of the data subject, or if Entrust needs to do so for the establishment or defense of a legal claim;
- Ask Entrust to destroy personal data held with respect to the data subject. The Company can refuse this request if the personal data is still necessary for the purposes for which it is being processed and there is a legitimate basis for Entrust to continue processing;
- Ask Entrust to restrict the processing of their personal data to storage. This can only be requested if the accuracy of personal data has been contested and remains unverified; Entrust no longer requires the personal data, but the data subject needs it to establish or defend a legal claim; the data subject has objected to the processing of personal data; and Entrust is deciding whether its legitimate interests override the data subject's interests or if the processing is unlawful.

If a data subject exercises these rights and Entrust has disclosed the personal data in question to a third party, the Company will do its best to ensure that the third party also complies with the wishes of the data subject.

3.14 Data Subject Access Rights

Data subjects who wish to request information about the personal data Entrust holds about them may do so by submitting a Data Subject Access Request (DSAR). If colleagues receive a request directly (whether verbally or in writing), immediately forward details of the request to privacy@entrust.com.

3.15 Training

Entrust provides its employees and contingent workers with access to training about data protection responsibilities. This training occurs at onboarding and at regular intervals thereafter.

3.16 Data Protection Officer

Entrust's assigned GDPR representative is Anjali Doherty, Sr. Corporate Counsel (UK). Entrust Deutschland GmbH's assigned Data Protection Officer is the law firm of Kill & Wolff GmbH.

Entrust Corporation does not have an assigned Data Protection Officer. Oversight of the data privacy compliance program is handled by the Compliance Director, Jenny Carmichael, who is located at Entrust's headquarters in Shakopee, Minnesota, USA.

4. Compliance

All employees and contingent workers are expected to comply with this policy. Additionally, all business units must ensure they have appropriate local standards and procedures in place to comply with this policy and applicable data privacy legislation in their jurisdiction. Breaches of this policy will be taken seriously and may result in disciplinary action, up to and including termination. This policy may be updated or amended at any time.

5. Exceptions

There are no exceptions to this policy.

6. Ownership and Review

This policy is owned by the Chief Legal and Compliance Officer. This policy shall be reviewed on an annual basis. Changes to this document shall be in accordance with the ISMS Document and Records Control Standard.

6.1 Contact Information

Questions about this policy or complaints about the handling of personal data should be directed to the Compliance Director at privacy@entrust.com.