ENTRUST

# GLOBAL PERSONAL DATA PROTECTION POLICY

| | |
|---|---|
| Document Version | 1.6 |
| Date | 5-Sept-2023 |

**Contents**

## 1. Introduction

Entrust Corporation and its subsidiaries and affiliates (collectively, “Entrust” or the “Company”) process personal data belonging to our colleagues, contingent workers, partners, suppliers, and customers in our role as a data controller, and personal data belonging to our customers and their end users in our role as a data processor. Where Entrust processes personal data, we do so in compliance with our legal, contractual, and ethical obligations and with full transparency.

## 2. Purpose

This policy sets forth the requirements and elements of our global data privacy program to ensure we comply with relevant legal and contractual obligations as well as certification and audit requirements. This policy applies globally to all personal data processing performed directly by Entrust and indirectly by third parties processing personal data on our behalf.

## 3. Definitions

**“Data Controller”** means the entity that determines the purpose and means of processing personal data and has the same meaning ascribed to “Personally Identifiable Information Controller” under ISO 27701.

**“Data Processor”** means the entity that processes personal data on behalf of the data controller and has the same meaning ascribed to “Personally Identifiable Information Processor” under ISO 27701.

**"Data Protection Impact Assessment”** refers to a documented analysis by a data controller or data processor assessing privacy risks where processing is likely to result in a high risk to the rights and freedoms of the data subject.

“**Data Protection Laws**” refers to all personal data protection and privacy laws and regulations applicable to Entrust, including, but not limited to, the EU General Data Protection Regulation (GDPR), UK General Data Protection Regulation (UK GDPR), Canada’s Personal Information Protection and Electronic Documents Act (PIPEDA), and US state privacy laws, in each case as may be amended, superseded, or replaced.

**“Data Subject”** means the identified or identifiable person or household to whom personal data relates and has the same meaning ascribed to “Personally Identifiable Information Principal” under ISO 27701.

**“Data Transfer Impact Assessment”** refers to a documented analysis by a data controller or data processor of the impact and security implications of a transfer of personal data to a country outside the European Economic Area (i.e., countries covered by the GDPR) that does not have an adequacy finding by the European Commission.

**“Legitimate Interest Impact Assessment”** refers to a documented analysis by a data controller or data processor as to whether legitimate interest can be used as the legal basis for processing personal data. The assessment includes a three-prong test analyzing whether the personal data

processing is in pursuit of a legitimate interest, whether it is necessary for that pursuit, and whether the data subject's interests override the legitimate interest.

**"Personal Data"** has the meaning ascribed to "personally identifiable information," "personal information," or equivalent terms as such terms are defined under data protection laws.

**"Personal Data Incident"** has the meaning ascribed to "security incident," "security breach" or "personal data breach" or equivalent terms as such terms are defined under data protection laws and includes any situation in which Entrust 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 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.

**"Sensitive Personal Data"** is a subset of personal data and refers to information about a data subject that if lost, compromised, accessed, or improperly disclosed could result in harm, embarrassment, inconvenience, or unfairness to the data subject and is therefore subject to heightened protection.

**"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 (e.g., eye color, hair color, height, weight), medical history, or criminal convictions and offenses.

## 4. Personal Data Processing Core Principles

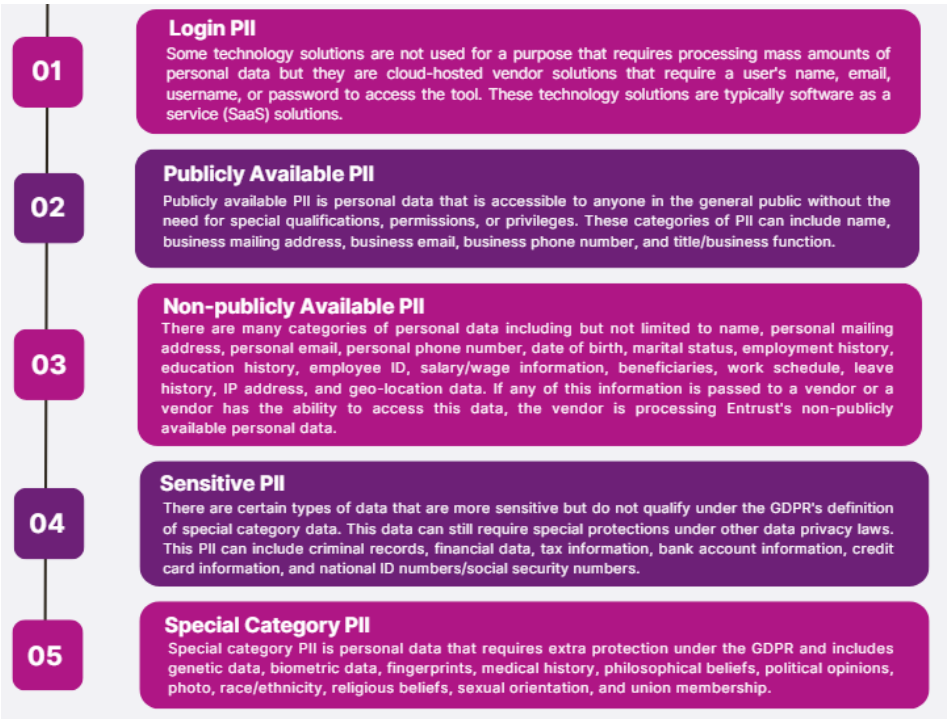
Entrust adheres to the following core principles when processing personal data:

- **Lawfulness and Adequacy**: We ensure personal data is collected for a lawful purpose and relevant and necessary for that purpose.
- **Accuracy and Retention**: We keep our systems up to date, provide mechanisms to update or delete inaccurate personal data and do not retain personal data longer than necessary to fulfill the lawful purpose for processing.
- **Confidentiality and Integrity**: We ensure personal data remains secure and protected during processing but respond swiftly and appropriately to security incidents and data breaches if they do occur, including providing timely notifications as required.
- **Transparency**: We adequately inform data subjects when we process their personal data. We are clear about why we need it, how we will use it and how it will be handled and protected.

We are all responsible for appropriately processing and safeguarding personal data and understand that failure to do so has the potential not only to undermine customer confidence in Entrust, but to result in significant fines and penalties for the Company.

## 5. Data Classification

Entrust maintains a central record of its processing activities. All personal data is classified into one of the following categories:




## 6. Lawfulness and Adequacy

### 6.1 Legal Bases for Processing Personal Data

The Company only processes personal data as legally permitted and with appropriate notice to the data subject. Entrust principally relies on the following legal bases for processing:

- Performance of a contract;
- Compliance with legal obligations, including but not limited to, lawful requests from law enforcement;
- Legitimate interest, except where such interest is overridden by the interests or fundamental rights and freedoms of the data subject; and
- Consent.

Where consent is the legal basis for processing (e.g., for marketing purposes), Entrust ensures that consent is freely given, specific, informed and an unambiguous indication of the data subject's wishes. The data subject has the right to withdraw consent at any time for any reason.

## 6.2 Privacy Assessments

### 6.2.1 Privacy by Design Assessment

Entrust evaluates personal data processing against the core principles as part of its design and development of new or substantially modified product offerings and when onboarding vendor cloud-hosted solutions, including licensed in third party software applications. The Privacy by Design assessment is embedded in Entrust's development and vendor onboarding processes and reviewed by Compliance and Information Security. Development may not move forward without approval.

### 6.2.2 Data Protection Impact Assessment (DPIA)

When contemplated personal data processing poses a high risk to an individual's rights and freedoms, Entrust completes a formal DPIA to document and assess the purpose for the processing, how Entrust will comply with relevant data protection laws and how the Company will mitigate potential risks to data subject rights.

### 6.2.3 Data Transfer Impact Assessment (DTIA)

Where Entrust intends to transfer personal data to a country outside of the European Economic Area (EEA) that does not benefit from an adequacy finding by the European Commission, Entrust completes a formal DTIA to analyze the impact and security implications of the transfer, particularly where the laws of the receiving country could allow its government access to the personal data being transferred.

### 6.2.4 Legitimate Interest Impact Assessment (LIIA)

Where Entrust relies on legitimate interest as the legal basis for processing personal data, the Company completes a formal LIIA to document and assess the legitimate interest, determine whether the processing is necessary, and evaluate whether data subject rights outweigh the legitimate interest.

### 6.2.5 Standards for Handling Sensitive and Special Category Data

In its role as a data controller, Entrust processes sensitive personal information on behalf of colleagues across various business systems and some limited special category data on a voluntary basis and as permitted by local law. Appropriate controls are in place and outlined in applicable DPIAs, the Access Control Standard for Sensitive and Special Category Data and enhanced privacy training mandated for colleagues handling this sensitive and special category data.

## 6.3 Contractual Protections

### 6.3.1 Intra-Group Data Transfer Agreement (IGDTA)

Companies within the Entrust group (i.e., all corporate entities and subsidiaries) enter into the Intra-Group Data Transfer Agreement to ensure appropriate safeguards are in place for the transfer of personal data out of the EEA but within the Entrust group to a country that does not benefit from an adequacy finding by the European Commission.

### 6.3.2 Data Processing Agreement (DPA)

Companies outside of the Entrust group who process personal data for or on behalf of Entrust are required to enter into a Data Processing Agreement with Entrust to ensure the third party (e.g., vendor, supplier, channel partner) has appropriate technical and organizational measures in place to comply with relevant data protection laws. Entrust makes equivalent commitments where it acts as a data processor through a standard customer DPA.

### 6.3.3 General Privacy Provisions

Contractual language around privacy is also built into standard agreements with customers, suppliers, and partners as well as in Entrust's standard Non-Disclosure Agreement (NDA).

## 7. Accuracy and Retention

## 7.1 Records Management

The global records management program ensures that a retention period is formally defined for processing personal data to ensure it is kept only for as long as it is needed, and that personal data is erased, destroyed, or anonymized at the end of the assigned retention period. The Global Records Management Policy sets forth handling requirements for all records, not just those containing personal data, and the accompanying Records Retention Schedule defines the retention period for each type of record maintained by the Company.

## 7.2 Storage and Backup of Personal Data

Entrust stores and backs up personal data across multiple server locations directly and indirectly managed by the Company. IT and relevant vendors (for non-IT managed, cloud-hosted applications) are provided with standard guidance around the proper handling of personal data on these servers, including with respect to storage and backups.

Entrust does not remove copies of personal data from its backup media and servers at the end of the retention period where doing so would be commercially impracticable; however, personal data retained by Entrust in this manner is protected by the same security standards protecting the personal data while in use and the personal data remains subject to confidentiality and may not be accessed except as required by applicable law.

## 7.3 Erasure or Destruction of Personal Data

The Global Records Management Policy and Information Classification Handling Standard set forth the requirements for appropriately handling records of all types at the end of their prescribed retention period. In particular, the following principles apply with respect to records containing personal data:

- Personal data should not be copied except as necessary to accomplish the specified purpose for processing and any copies made should retain any original confidential or proprietary markings.
- Paper records must be shredded and disposed of securely when there is no longer a need to retain them and may not be disposed of in any other manner.
- Personal data in electronic format should be deleted or anonymized once it is no longer needed.
- 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 Bring Your Own Device (BYOD) devices) in accordance with relevant Information Security policies and standards.

# 8. Confidentiality and Integrity

## 8.1 Information Security

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

- Encrypting personal data at rest and in transit where required by law or contract and additionally as commercially practicable;
- Ensuring the ongoing confidentiality, integrity, availability and resilience of systems and services used to process personal data through formalized business recovery and disaster recovery plans that are routinely tested or exercised;
- Ensuring the restoration of access to personal data in a timely manner in the event of a physical or technical incident;
- Periodically testing, assessing, and evaluating the effectiveness of technical and organizational measures in place to secure personal data;
- Enforcing physical security standards are in place requiring that desks and cupboards be kept locked if they hold personal data, individual monitors/screens not allow for personal data to be visible to passers-by and electronic devices (e.g., computers, tablets) are locked or logged off the Company's systems when left unattended.

In assessing appropriate security controls, Entrust considers the risks associated with the processing, in particular the risk 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 from Entrust and subject to contractual provisions (e.g., DPA) to appropriately handle the personal data and implement appropriate technical and organizational measures that are at least equivalent to Entrust's own security requirements. Personal data is not shared outside of Entrust without these mechanisms in place. Various security tools (e.g., DLP) are in place to ensure personal data does not leave the organization without authorization.

## 8.2 Testing

Personal data may not be used in any Entrust testing environments without a formal security exception approved in advance. All testing environments must adhere to the current standards and controls in place for production environments and all personal data approved for use in testing environments must be removed without delay once testing has been completed. Further details are outlined in the Secure-Software Development Life Cycle (S-SDLC).

## 8.3 Reporting a Personal Data Incident

A personal data incident can take many forms including, but not limited to:

- Loss of a mobile device or hard copy file containing personal data (e.g., accidentally leaving a device behind on public transportation);
- Theft of a mobile device or hard copy file containing personal data;
- Human error (e.g., a colleague 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);
- Physical destruction and loss (e.g., fire or flood); or
- Information is obtained from Entrust by a third party through deception (e.g., phishing or smishing attacks).

A personal data incident may have occurred if there is:

- Unusual log-in and/or excessive system activity 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; or
- 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 may have occurred or is about to occur must immediately contact Entrust's Security Operations Center at SOC@entrust.com.

## 8.4 Personal Data Incident Response

In the event of an actual or imminent personal data incident, Entrust will implement its incident response and handling procedures maintained by Information Security to minimize the impact of the incident and notify regulators, data subjects and/or other parties as legally and/or contractually required. A response will typically involve the following:

- Investigating the incident to determine the nature, cause and extent of the damage or harm that has or 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, contractual parties) and making those notifications in a timely manner; and
- Recording information about the personal data incident and steps taken in response, including documenting decisions to notify or not notify regulators or affected parties.

# 9. Transparency

Entrust provides transparency with respect to its global data privacy program through robust internal and external landing pages.

## 9.1 Privacy Notices

Entrust provides notice to data subjects about the processing of their personal data in its role as both a data controller and data processor. This information is available through Entrust's various privacy notices for web users, job applicants and colleagues as well as through its individual product privacy notices available here. Such notices provide information about:

- The types of personal data Entrust processes;
- The purpose and legal basis for the processing;
- Third parties used for processing, if applicable;
- Location and duration of processing;
- Any cross-border transfers of personal data;
- Duration of processing;
- Data subject rights; and
- Details of any artificial intelligence/automated decision-making processes

## 9.2 Training

Entrust provides colleagues with mandatory, annual training about data protection responsibilities. The Introduction to Data Privacy Training occurs at onboarding and annually thereafter. In addition to the all-colleague Introduction to Data Privacy Training, Entrust mandates annual completion of the Enhanced Data Privacy Training by colleagues who handle sensitive and special category data as well as the Privacy by Design Training by colleagues who play a role in the development and design of software product and service offerings. Entrust continues to develop and deploy additional function-specific privacy trainings as needed.

## 9.3 Data Subject Rights

Where Entrust processes personal data, data subjects have certain rights under data protection laws. Although these rights vary by jurisdiction, data subjects generally 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;
- Object to Entrust's 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 legal reasons;
- 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 legal basis for Entrust to continue processing;
- Ask Entrust to restrict the processing of their personal data to storage under certain circumstances.

Entrust will assess a data subject's rights under data protection laws on a case-by-case basis and follow the Data Subject Request Procedure in determining how to fulfill a request. In general, Entrust will use a data subject's rights under the EU GDPR as a baseline for fulfilling all requests and apply additional rights available under data protection laws applicable to the data subject to the extent those are more favorable to the data subject. 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.

Data subjects who wish to request information about the personal data Entrust holds about them should do so through submission of a formal Data Subject Request (DSR). If colleagues receive a request directly (whether verbally or in writing), the request should immediately be forwarded to privacy@entrust.com.

## 9.4 Supervisory Authorities

Contact information for relevant data supervisory authorities varies by location. The list of European Data Protection Board authorities can be found here. The United Kingdom (UK) Information Commissioner's Office (ICO) can be found here. The Office of the Privacy Commissioner of Canada can be found here.

## 10. Compliance

All colleagues 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.

## 11. Exceptions

There are no exceptions to this policy.

## 12. Ownership and Review

This policy is owned by the Chief Legal and Compliance Officer and shall be reviewed on an annual basis.

## 12.1 Contact Information

Questions about this policy or Entrust's handling of personal data can be directed to privacy@entrust.com.