GLOBAL PERSONAL DATA PROTECTION POLICY

Classification	Public
Document Version	2.0
Publication Date	26 February 2026

Contents

1. Introduction

Entrust Corporation and its subsidiaries (collectively, "Entrust" or the "Company") process Personal Data relating to our colleagues and to business contacts at our sales partners, suppliers, and customers in our role as a data controller. Entrust also Processes Personal Data relating to our customers' employees and end users in our role as a Data Processor. Where Entrust processes Personal Data, we do so in compliance with our legal and contractual obligations and with full transparency.

2. Purpose

This policy sets forth the requirements and elements of our global data privacy program which Entrust has established 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 by Entrust.

3. Definitions

"Data Controller" means the entity that determines the purpose and means of Processing Personal Data and has the same meaning ascribed to "PII 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 "PII 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), UK's Data Protection Act (DPA 2018), Switzerland's Federal Act on Data Protection (as implemented 1 September 2023) (FADP), Canada's Personal Information Protection and Electronic Documents Act (PIPEDA), Japan's Act on Protection of Personal Information (APPI), China's Personal Information Protection Law (PIPL), and US state privacy laws, in each case as may be amended, superseded, or replaced.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 "PII 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 from inside the EEA or UK to a country outside the EEA/UK that does not have an adequacy finding by the European Commission or Information Commissioner's Office.

"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" or "PII" 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 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, political opinions, religious or philosophical beliefs, or trade union membership, and the Processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

4. Personal Data Processing Core Principles

Entrust adheres to the following core principles when Processing Personal Data as a Data Controller:

- **Lawfulness and Adequacy**: We ensure Personal Data is collected for a lawful purpose and limited to what is relevant and necessary for that purpose.
- **Accuracy and Retention**: We keep our systems up to date, provide mechanisms to update 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 Personal Data Incidents if they do occur, including providing timely notifications as required.
- **Fairness and 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 provide mechanisms for data subjects to exercise rights they have with respect to their Personal Data under applicable law.

All Entrust colleagues are 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. Records of Processing

To ensure compliance with applicable data protection laws and to uphold our commitment to transparency and accountability, Entrust maintains a Record of Processing Activities (RoPA) in accordance with Article 30 of GDPR and other relevant privacy regulations. The RoPA includes all processing activities involving Personal Data as classified in accordance with Entrust's Data Classification & Handling Standard.

6. Lawfulness and Adequacy

6.1 Legal Bases for Processing Personal Data

When acting as a Data Controller, the Company only processes Personal Data as legally permitted. 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, 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 described in Section 4 above as part of its design and development of new or substantially modified product offerings and when onboarding vendor solutions where PII will be processed, including licensed in third party software applications. This "Privacy by Design" assessment is embedded in Entrust's development and vendor onboarding processes. Completion of the assessment requires review and approval by Entrust's Privacy and Information Security teams. 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 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 the Data Subject. Where a DPIA relates to Processing where Entrust is the Data Controller, it is reviewed by Entrust's Data Protection Officer who must approve the proposed Processing before it commences. DPIAs shall be reviewed and updated at least annually, or more frequently as necessary, to ensure continued compliance with applicable laws and regulations.

6.2.3 Data Transfer Impact Assessment (DTIA)

Where Entrust intends to transfer Personal Data from inside the European Economic Area (EEA) or United Kingdom (UK) to a country outside of the EEA or UK that does not benefit from an adequacy finding by the European Commission or UK Information Commissioner's Office, 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. Entrust will only proceed with the transfer where it concludes the risk posed by the transfer is acceptable. DTIAs shall be reviewed and updated at least annually, or more frequently as necessary, to ensure continued compliance with applicable laws and regulations.

6.2.4 Legitimate Interest Impact Assessment (LIIA)

Where Entrust acts as a Data Controller and 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 evaluating whether the Data Subject's interests, rights and freedoms outweigh or override the legitimate interest. Entrust will only proceed with the Processing on the basis of legitimate interest where the LIIA concludes that the legitimate interest is not so overridden.

6.2.5 Standards for Handling Sensitive and Special Category Data

In its role as a Data Controller, Entrust processes Sensitive Personal Data relating to 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.

6.2.6 Bulk Data Rule

Sensitive personal data, including human 'omic data, biometric identifiers, precise geolocation data, personal health data, personal financial data and certain personal identifiers of U.S. citizens, as well as U.S. government data including precise geolocation data for any area specifically designated as posing a heightened risk of exploitation (such as military installations, national security, defense or intelligence facilities, or worksites of federal national intelligence personnel) is subject to restrictions on export, transfer and access. Such data cannot be provided to any individual or entity located in or controlled by or acting at the direction of an individual or entity located in, a "country of concern". Currently, "countries of concern" are China (including Hong Kong and Macau), Cuba, Iran, North Korea, Russia and Venezuela.

While such transfer or access can be provided under certain circumstances, Entrust has determined that it will not engage in any transactions with countries of concern that involve sensitive U.S. personal data or U.S. government data. No such data should ever be transferred to a country of concern or a person or entity located in a country of concern, either by Entrust or anyone acting on Entrust's behalf.

6.3 Contractual Protections

6.3.1 Intra-Group Data Transfer Agreement (IGDTA)

Entrust Corporation and its subsidiaries enter into the Intra-Group Data Transfer Agreement to ensure that where Personal Data is shared within the Entrust group, this is covered by appropriate data sharing clauses (including controller – processor clauses as required by GDPR). The IGDTA also ensures there are appropriate safeguards in place (i.e. standard contractual clauses) for when the sharing of Personal Data within the Entrust group involves the transfer of Personal Data from inside the EEA/UK to a country outside of the EEA/UK that does not benefit from an adequacy finding by the European Commission or Information Commissioner's Office.

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 to its customers 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). Contracts with vendors and suppliers also include obligations to comply with the Bulk Data Rule.

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 when 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 Data Classification and 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 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 Entrust holds about them, including a copy of such information;
- 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 (DSR) 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.

9.5 Data Protection Officer

Unless otherwise indicated, Entrust's Data Protection Officer is:

Mishcon de Reya LLP
Africa House, 70 Kingsway, London, WC2B 6AH, United Kingdom
DPO@mishcon.com

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 Revision History

This policy is owned by the Director, Privacy and shall be reviewed on an annual basis.