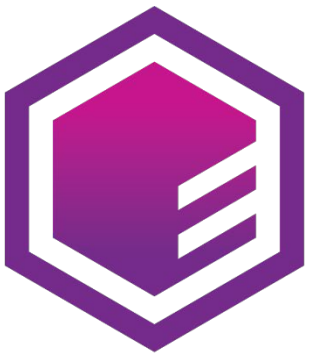

ENTRUST

DATA SUBJECT REQUEST (DSR) PROCEDURE

Document Version	1.9
Date	20-Nov-2025

Contents

1. Introduction

This procedure sets forth the process for complying with data subject requests (DSRs) under the EU's General Data Protection Regulation (GDPR) and other applicable data privacy laws and regulations (e.g., the California Consumer Privacy Act (CCPA), Canada's Personal Information Protection and Electronic Documents Act (PIPEDA), and the UK's Data Protection Act 2018 (DPA 2018), UK General Data Protection (UK GDPR) and Data Use and Access Act 2025 (DUAA).

2. Purpose

The purpose of this procedure is to help Entrust comply with its legal obligations and enable individuals about whom we hold personal data to have confidence in us as a data controller and processor. This procedure should be used by all Entrust Corporation ("Entrust" or "Company") employees, consultants, independent contractors, interns, or temporary workers in all countries in which Entrust operates and/or conducts business. For the purposes of the CCPA, this sets out our obligations as a "business" and a "service provider", as those terms are defined under the CCPA.

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 Laws refers to all personal data protection and privacy laws and regulations applicable to Entrust, including, but not limited to, GDPR, UK GDPR, DPA 2018, DUAA, PIPEDA, and US state privacy laws, in each case as may be amended, superseded, or replaced.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.

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

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.

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. This is sometimes referred to as "sensitive data".

4. Procedure Requirements

4.1 Data Subject Rights

There are lots of different Data Subject Rights, and the rights available vary depending on the jurisdiction in which the Data Subject is based. Requests may cover the following rights, particularly those subject to GDPR and UK GDPR:

Right to data access

This document focuses on the right of access. In many jurisdictions, including but not limited to California in the United States, Canada, the UK and the European Economic Area, Entrust, as a data controller, is required to take appropriate measures to provide data subjects with access to personal data it processes with respect to them.[1] Access should be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

Right to data erasure

Data subjects have the right to have their personal data erased (also known as the 'right to be forgotten'). The right only applies to data held at the time the request is received. It does not apply to data that may be created in the future. The right is not absolute and only applies in certain circumstances. For example, where we are required by law to process individuals' personal data, the right to erasure will not apply.

Right not to be subject to automatic decision-making

Individuals may have the right not to be subject to a decision when it is based on automated processing, and it produces an adverse legal effect or significantly affects the individual (also known as a 'qualifying significant decision').

[1] Entrust is only obligated to provide personal data collected in the 12 months before the request in the state of California. In relation to all other requests, the obligation is to provide personal data for the time period requested, or for a reasonable period if no period is specified.

We must ensure that in processes where automated processing takes place and may have an adverse effect, that individuals are able to obtain human intervention, express their point of view, obtain an explanation of the decision and challenge it. Human intervention must involve a close review of the decision process by someone who has the authority and competence to change the decision, and not a token review.

This right does not apply to profiling, or when a decision does not have an adverse legal or similarly significant effect on someone.

Right to object

Individuals have the right to object to the processing of their personal data at any time. This effectively allows individuals to stop or prevent Entrust from processing their personal data. An objection may be in relation to all the personal data we hold about an individual or only to certain information. It may also only relate to a particular purpose we are processing the data for.

Individuals have the absolute right to object to the processing of their personal data if it is for direct marketing purposes.

An individual must give specific reasons why they are objecting to the processing of their data. These reasons should be based upon their particular situation. There is no absolute right here, and Entrust can refuse to comply where:

- we demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or
- the processing is for the establishment, exercise or defence of legal claims.

Right to restrict processing

Individuals also have the right to restrict the processing of their personal data, defined as the ‘marking of stored personal data with the aim of limiting its processing for the future’.

When processing is restricted, Entrust will be permitted to store the personal data, but not further process it. Restriction could involve measures such as transferring data to a separate system or limiting the access through the use of passwords and other access controls.

For advice on dealing with all other data subject rights, please contact Entrust’s Data Protection Officer at DPO@mishcon.com.

4.2 Data Subject Access Rights

As outlined above, in many jurisdictions, data subjects have the right to access certain personal data that Entrust processes. The right varies by jurisdiction and below outlines some of the differences.

4.2.1 European Economic Area and UK

The data subject may also have the right to receive the following from Entrust if located in the European Economic Area or UK:

1. Confirmation as to whether Entrust processes personal data about the data subject
2. The purpose of the processing
3. The categories of personal data concerned
4. The recipients or categories of recipients to whom the personal data has been or will be disclosed
5. The period in which the personal data will be stored or, if not possible, the criteria used to determine that period
6. Information as to the source of personal data about the data subject held by Entrust (if not provided by the data subject)
7. Information about the existence of automated decision-making, including profiling, and meaningful information about the logic involved, as well as the significance and consequences of personal data processing
8. Information about safeguards Entrust has put in place where personal data is transferred to a third country (e.g., under the GDPR, a country that is not a signatory to the GDPR and has not received an adequacy decision from the European Commission)
9. Information about the right to lodge a complaint with the relevant supervisory authority
10. Transfer by Entrust of personal data held about the data subject to another data controller, designated by the data subject, where technically feasible, and where the personal data was obtained from the data subject and Entrust's processing was based on consent

4.2.2 California

The data subject may also have the right to receive the following from Entrust if located in California:

1. Confirmation as to whether Entrust processes personal data about the data subject
2. The purpose of the processing
3. The categories of personal data concerned

4. The recipients or categories of recipient to whom the personal data has been or will be disclosed
5. Information as to the source of personal data about the data subject held by Entrust (if not provided by the data subject)
6. The right to opt out of the "sale" by Entrust of personal data about the data subject, as "sale" is defined under the CCPA

4.2.3 Canada

Although not as prescriptive as the UK GDPR, GDPR and CCPA, PIPEDA has been interpreted to contain the same data subject rights. Thus, the aforementioned rights apply to those in Canada as well.

4.2.4 Other jurisdictions

For data subjects located in other jurisdictions, Entrust will provide the same information upon request and will review applicable data privacy legislation to determine whether different or additional rights apply to data subjects.

4.2.5 Considerations when responding to Data Subject Access Rights

Identity

As a data controller, Entrust may refuse to comply with a data subject's request if it cannot satisfy itself as to the identity of the data subject. Entrust will request only the information that is needed to confirm the data subject's identity and the information requested will be proportionate to the request (e.g., Entrust will go to greater lengths to confirm the data subject's identity where special category data is the subject of the request). See 4.3.3 for more information.

Fees

In the vast majority of cases, data subjects will have the right to access their personal data free of charge; however, in the rare case where the request is reasonably considered to be manifestly unfounded or excessive (e.g., due to the repetitive nature of the exceptionally broad scope of the request), Entrust may charge the data subject a reasonable fee taking into account the administrative costs of complying with the request or refuse to act on the request altogether. In practice this fee is not usually charged but Entrust can use its discretion to choose to charge. These fees would likely be for costs of printing if multiple printed copies of disclosure were requested.

Manifestly unfounded or manifestly excessive DSRs

The Director, Privacy will determine whether a request is manifestly unfounded or excessive and should be rejected or fulfilled subject to the payment of a fee by the data

subject. This must be done on a case-by-case basis. Some examples of manifestly unfounded or excessive DSRs in the EEA/UK include where:

- The individual clearly has no intention to exercise their right of access, such as where they offer to withdraw the DSR in return for a settlement agreement in an employment dispute.
- The request is malicious and is being used to harass the business with no real purpose other than to cause disruption, for example:
    - They explicitly state they intend to cause disruption.
    - They make unsubstantiated accusations against the business or specific employees.
    - They systematically send different requests to you as part of a campaign.

It may also be possible to reject a DSR where an individual repeatedly submits DSRs over a short timeframe. While each DSR must be considered individually, if there is a pattern of consistent requests within a relatively short timeframe it may be possible to reject on the grounds that the data subject's data has not changed sufficiently within the period.

Entrust may also refuse the request in full or in part where disclosure of third-party data is unavoidable, making use of redactions where necessary.

Decisions on refusing to respond to a DSR will be recorded in the DSR log.

For California residents, Entrust is not required to respond to DSRs more than twice for the same consumer in a 12-month period.

Entrust may also charge a reasonable fee based on administrative costs if the data subject requests more than one copy of the personal data held about them from Entrust.

Exemptions

There are other potential exemptions to the provision of access to certain types of data held on the data subject that may apply (e.g., Entrust cannot honor a request to discontinue processing the data subject’s personal data because it has a contractual or legal obligation to retain or process the personal data or where personal data of another individual is involved). Before responding to a data subject request, the Director, Privacy will determine whether there are any applicable exemptions that apply to the personal data that forms the subject of the request. For a complete list of available exemptions, see Appendix 1.

4.3 Procedure (Data Subject Request Process Flow)

See Appendix 2.

4.3.1 DSR Intake

Entrust's Privacy Statement can be accessed from the Company's website by clicking on "Privacy Statement" at the bottom of the homepage. It can also be found at https://www.entrust.com/legal-compliance/data-privacy under the Privacy Statement Tab. The Privacy Statement contains a link to the Data Subject Request Form. All data subjects are encouraged to complete this form when submitting a DSR. If a DSR is received through other means (e.g., in person, over the phone, through email, by letter), the data subject should be directed to this form as completion of the form will allow Entrust to respond faster and more efficiently to the request. If the data subject still does not wish to complete the form, the details of their request should be forwarded immediately to privacy@entrust.com.

Many data privacy regulations require companies to respond to DSRs within a prescribed period of time (e.g., 1 calendar month under the GDPR and UK GDPR unless the data controller can articulate valid reasons from a prescribed list for the delay to the data subject, in which case the period of time can be extended by 2 months, for 3 calendar months in total); thus, it is important that details of the request be forwarded as soon as they are received.

4.3.2 DSR Acknowledgement

Entrust Acting as Data Controller

If Entrust is acting as a data controller with respect to the personal data, the Director, Privacy will enter the date on which the DSR was received by Entrust in the DSR log and then acknowledge receipt of the DSR to the data subject in writing. This acknowledgment should be sent within one business day of the Director, Privacy receiving the request. The Director, Privacy will also ensure that any relevant third parties involved in processing the personal data are promptly notified of the DSR to facilitate compliance.

Entrust Acting as Data Processor

If Entrust is acting as a data processor on behalf of our customer as the data controller, Entrust will notify the data controller upon receipt of the request and assist the data controller in responding as required under relevant data privacy legislation and/or as agreed to in any Data Processing Agreement (DPA) with the data controller. Entrust will notify the data subject that Entrust is the data processor and that the request has been forwarded to the appropriate data controller for handling.

If Entrust is the data processor and uses sub processors in connection with the processing of the data subject's personal data, Entrust will notify the sub processor upon receipt of the request to enable the sub processor to act accordance with the Data Processing Agreement (DPA) that has been executed with Entrust.

4.3.3 Verify Data Subject Identity

The Director, Privacy will verify the identity of the data subject. This may involve reaching out to the data subject to provide proof of their identity. Where the data subject submits a request from their Entrust email account, no further verification will be required.

Entrust should first try to verify an individual's identity by asking the data subject to confirm certain key details about themselves held by Entrust (e.g., date of birth, first and last line of address, personal identification number, period of employment). Only if this is not possible should Entrust request a form of identification documentation that has been redacted to only display the name and/or address (e.g., driver's license, national identification card, passport) to verify the data subject. The Director, Privacy will notify the individual that until their identify has been verified, the clock pauses until we receive the required information.

Entrust will only request information needed to confirm the data subject's identity and the information requested will be proportionate to the request (e.g., Entrust will go to greater lengths to confirm the data subject's identity where special category data is the subject of the request). Once the data subject's identity has been verified, this will be noted in the DSR log and the copy of the identification will be destroyed.

For most Employee DSRs, provided the request comes from a familiar source (e.g. the Employee's Entrust email address) identity verification is unlikely to be required. For ex-employees or any external individual, it is more likely to be reasonable and necessary to confirm the identity of the individual. It may also be necessary to identify the individual if there is a concern about fraudulent or other suspicious activity.

If a request is received on behalf of another individual, we should confirm that the requestor has consent from the individual to make the request. The exception to this is where a request is received from a law firm, in this case we can assume the law firm has consent from the individual.

If the data subject's identity cannot be verified, the Director, Privacy will notify the data subject in writing that Entrust cannot comply with the request because it cannot verify the data subject's identity.

4.3.4 Review DSR and Determine Required Response

The Director, Privacy will review the nature and scope of the request and determine what actions need to be taken under applicable data privacy law, including whether the request should be rejected, because the request is manifestly unfounded or excessive or an exemption applies.

If the scope is very broad, the Director, Privacy will ask the data subject to clarify what personal data they are requesting and / or ask to limit the scope to a particular time frame or search terms.

If the decision is made to reject the request on this basis, the Director, Privacy will notify the data subject in writing, including why we are refusing their request and their right to make a complaint to their local regulator for data protection. The Director, Privacy will record this justification in the DSR log. The Director, Privacy will send further instructions to IT, if applicable, within three business days.

4.3.5 Locate Data Subject in Entrust Systems via Searches

Upon receipt of instructions from the Director, Privacy, IT will begin taking appropriate action with respect to the DSR, including searching Entrust's databases, systems, applications or other places where personal data about the data subject may be held using our IT DSAR Fulfillment For. Search terms might include:

- [first name + surname]
- [email address]
- [alternative first name + surname]
- [surname] / [first name] (if unique)
- [initials] (if referred to by initials)
- [identification number/employee number]

In circumstances where IT have reason to believe employees will hold the data subject's personal data on their personal device used for work purposes, IT will request they send copies of relevant records.

IT should complete its searches (coordinating with other departments as needed) and package (in secure form) a copy of all personal data held with respect to the data subject. While the default for packaging this information should be in electronic form, documents will be provided in paper form if requested by the data subject.

IT should then send the package of data to the Director, Privacy within 10 business days. If more time is needed, IT should notify the Director, Privacy in writing and provide an explanation for why the request cannot be completed within the prescribed timeframe. The Director, Privacy will notify the data subject of Entrust's reliance on the available right to extend the timeline for a response.

As part of its instructions, IT will be tasked with determining whether any of the personal data held with respect to the data subject has been sent to third parties for processing. If yes, IT should provide the Director, Privacy with a list of those third parties as well as a point of contact for each entity. IT will also determine whether any of the personal data

held with respect to the data subject has been sent outside of the country in which it was collected. If yes, IT should provide the Director, Privacy with a list of those countries. The Director, Privacy will notify the impacted third parties of the DSR to respond as appropriate to the data subject and consider the legal implications of any international transfers of data.

If IT does not locate personal data related to the data subject, the Director, Privacy will respond to the data subject in writing that based upon the information provided, Entrust has not identified any personal data Entrust holds with respect to the individual.

4.3.6 Review, Exemptions and Redactions

The Director, Privacy will review the information provided by IT to first remove any duplicate documents (for example, repeated parts of the same email chain) and irrelevant records (for example, records that only contain the data subject's name or email address and no other personal data), and second to remove any personal data that is exempt from disclosure. This includes personal data of anyone that is not the data subject making the request, including their email address and signature.

Where exemptions apply, particularly in relation to requests made from the UK or the EU which are subject to UK GDPR and EU GDPR, redactions should be applied to documents to prevent disclosure of this data. Redaction is a change to a document which prevents certain information from being extracted from the document. Redaction of digital files should be completed using Redaction software (for example, Adobe Acrobat) so that it is not possible for the data subject to remove the redaction and reveal the information underneath.

4.3.7 Respond to Data Subject

The Director, Privacy will respond to the data subject with all non-exempt personal data located as soon as possible along with an explanation as to why any portion of the request was denied or omitted from the response, if applicable. Depending on the nature of the request, the response may be provided orally, in writing or by electronic means.

4.3.8 Update DSR Log

The Director, Privacy will log all DSRs in the Data Subject Request log. A copy of the initial request, acknowledgment of the request and the response provided will be maintained in a restricted access folder maintained by Legal.

4.4 Assignment of Responsibilities

The Director, Privacy may delegate responsibilities under this procedure as appropriate.

5. Ownership and Review

This procedure is owned by the Director, Privacy and shall be reviewed and updated annually or as needed to reflect changes in applicable law.

5.1 Contact Information

Questions about this procedure should be directed to the Director, Privacy at privacy@entrust.com.