



USTENTR

DATA SUBJECT ACCESS REQUEST (DSAR) PROCEDURE

| | |
|------------------|-------------|
| Document Version | 1.3 |
| Date | 12-Apr-2021 |

| Document Properties | |
|-----------------------|---|
| Property | Description |
| Circulation | Internal and external use |
| Classification | Public (Appendices and Internally Linked Documents are Proprietary) |
| Document Owner | Jenny Carmichael, Compliance Director |
| Next Scheduled Review | Periodic review as needed |

| Revision History | | | |
|------------------|--------------|------------------------|------------|
| Version | Date | Description of Changes | Revised By |
| 1.0 | 08-July-2019 | Initial version | |

Contents

| | |
|---|----|
| 1. Introduction..... | 4 |
| 2. Purpose..... | 4 |
| 3. Procedure Requirements..... | 4 |
| 3.1 Definitions..... | 4 |
| 3.2 Data Subject Rights..... | 5 |
| 3.2.1 Limitations on Data Subject Rights..... | 6 |
| 3.3 Procedure (Data Subject Access Request Process Flow)..... | 7 |
| 3.3.1 DSAR Intake..... | 7 |
| 3.3.2 DSAR Acknowledgement..... | 7 |
| 3.3.3 Verify Data Subject Identity..... | 8 |
| 3.3.4 Locate Data Subject in Entrust Systems..... | 8 |
| 3.3.5 Review DSAR and Determine Required Response..... | 8 |
| 3.3.6 Identify Complexity of Search and Third Party Processors..... | 9 |
| 3.3.7 Respond to Data Subject..... | 9 |
| 3.3.8 Update DSAR Log..... | 9 |
| 3.4 Assignment of Responsibilities..... | 9 |
| 4. Ownership and Review..... | 10 |
| 4.1 Contact Information..... | 10 |
| 5. Appendices..... | 10 |

1. Introduction

This procedure sets forth the process for complying with data subject access requests (“DSARs”) 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).

2. Purpose

The purpose of this procedure 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 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. Procedure Requirements

3.1 Definitions

Data Controller means the entity that determines the purpose and means of processing personal data and is synonymous with “PII controller” as defined in ISO 27701.

Data Processor means the entity that processes personal data on behalf of the data controller and is synonymous with “PII processor” as defined in ISO 27701.

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 and is synonymous with “data principal” as defined in ISO 27701.

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 and in ISO 27701.

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.

9. Transfer by Entrust of the personal data held about the data subject to another data controller as specified 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.

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.

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

3.2.1 Limitations on Data Subject Rights

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).

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 or 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. The Compliance Director 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. Entrust may also refuse the request in full or in part where disclosure of third party data is unavoidable. For California residents, Entrust is not required to respond to DSARs 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. 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 an access request, the Compliance Director 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.

3.3 Procedure (Data Subject Access Request Process Flow)

See Appendix 2.

3.3.1 DSAR 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 Privacy Management Form](#). All data subjects are encouraged to complete this form when submitting a DSAR. If a DSAR 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 within a prescribed period of time to DSARs (e.g., 30 days under the GDPR unless the data processor can articulate reasons for the delay to the data subject); thus, it is important that details of the request be forwarded as soon as they are received.

3.3.2 DSAR Acknowledgement

The Compliance Director will log the date on which the DSAR was received by Entrust, and then acknowledge receipt of the DSAR to the data subject in writing. This acknowledgement should be sent within one business day of the Compliance Director receiving the request.

Note: If Entrust is the data processor and not 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

4. Ownership and Review

This procedure is owned by the Compliance Director and shall be reviewed and updated on a periodic basis.

4.1 Contact Information

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

5. Appendices

PROPRIETARY