ENTRUST CORPORATION

Compliance with EU Transfer Requirements for Personal Data

ENTRUST

Table of Contents

Introduction

Entrust Corporation is dedicated to its role as a trusted partner and data processor and is committed to supporting our customers' privacy compliance efforts. The cross-border transfer of European personal data has become more complex as a result of the *Schrems II* Ruling. This whitepaper provides Entrust customers with information about how Entrust follows the recommendations of the European Data Protection Board ("EDPB") to help ensure adequate protection of personal data leaving the European Economic Area ("EEA").

This document is a summary and is for reference purposes only. This document does not modify any terms of your individual agreement with Entrust. Entrust assumes no liability arising from your use of the information contained in this document.

Schrems II Ruling & EDPB Recommendations

Schrems II Ruling

On July 16, 2020, the Court of Justice of the European Union ("CJEU") invalidated the EU-U.S. Privacy Shield framework but upheld the validity of the European Commission's standard contractual clauses ("SCCs") as a cross-border transfer mechanism for personal data leaving the European Economic Area ("EEA") in the widely-publicized *Schrems II* decision. While the SCCs remain valid, organizations that currently rely on them must consider whether, with regard to the nature of the personal data, the purpose and context of the processing, and the country of destination, there is an "adequate level of protection" for the personal data as required by European Union ("EU") law. Where that is not the case, organizations should consider what additional safeguards may be implemented to ensure there is an "adequate level of protection."

Entrust has never relied on the EU-U.S. Privacy Shield framework. Entrust relies instead on the SCCs for transfer of personal data, and these SCCs are specifically included in our standard **Data Processing Addenda** ("DPAs") with customers, vendors and partners. The revised SCCs were issued and came into force on June 27, 2021, and Entrust has incorporated these new SCCs into our DPAs.

European Data Protection Board Recommendations

Further to the *Schrems II* ruling, the **European Data Protection Board** ("EDPB") published **recommendations** on supplemental measures companies should implement to ensure adequate protection of personal data leaving the EU. While the EDPB recommendations are non-binding, Entrust has used the EDPB recommendations to evaluate our transfers of personal data. The EDPB recommends data exporters follow six steps in assessing their data transfers and determining if supplementary measures are needed:

1. **Map all transfers of personal data to third countries.** Assess whether the personal data being transferred is limited to only what is necessary.
2. **Verify the transfer mechanism that will be used.** In the absence of an adequacy decision, an Article 46 General Data Protection Regulation ("GDPR") transfer mechanism should be used.
3. If the data exporter is relying on an Article 46 GDPR transfer mechanism (such as SCCs), **asses whether the mechanism is effective with the particular circumstances of the transfer**. This assessment should take into consideration whether there is anything in the law and/or practices of the third country that may impinge on the effectiveness of the appropriate safeguards of the transfer mechanism.
4. **Identify and adopt any supplementary measures**, including but not limited to contractual, technical, and organizational measures, that "are necessary to bring the level of protection of the data transferred up to the EU standard of essential equivalence."
5. **Take formal procedural steps** adopting any needed supplementary measures that are required.
6. **Re-evaluate**, when appropriate, the level of protection for personal data transferred to third countries. This re-evaluation should include monitoring any developments that may affect the transfers.

Implementation of EDPB Recommendations

Step One: Map all transfers of personal data to third countries

Personal data transferred outside of the EEA in connection with Entrust products

Entrust may transfer personal data out of the EEA for processing depending on the product/service in question. For specific information regarding the types of personal data collected by Entrust products/services and international data transfers of that personal data, please review the applicable **product privacy notice**.

Sub-processors

Entrust's **sub-processor list** is published on the **Data Privacy** section of **Entrust's website**. The sub-processor list identifies each sub-processor, its location, and the purpose of processing. Entrust performs thorough information security reviews on and executes a GDPR-compliant DPA with all of its sub-processors. Entrust updates the sub-processor list on an ongoing basis as new products, and new versions of existing products, are developed and notifies affected customers before changes are made to this list.

Step Two: Verify the transfer mechanism that will be used

Entrust relies on the following transfer mechanisms for personal data originating from the EEA:

Adequacy Findings

The European Commission, the UK government, and the Swiss Federal Data Protection and Information Commissioner each have the authority to determine whether a country outside of its respective jurisdiction has an adequate level of data protection. Personal data can be transferred to a country that has been declared "adequate" without any further transfer mechanism or transfer risk assessment required.

Standard Contractual Clauses

Entrust also relies on the European Commission's Standard Contractual Clauses (Commission Decision 2021/914 of June 2021) to transfer personal data to Entrust and its sub-processors. The implementation of the 2021 SCCs is reflected in our current **DPAs**.

Step Three: Assess the effectiveness of the transfer mechanism

Clause 14(a) of the 2021 SCCs requires both data exporters and importers to "warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the importer, including any requirements to disclose personal data or measures authorizing access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses."

In its *Schrems II* decision, the CJEU was principally concerned with the ability of U.S. law enforcement to reach EU personal data through mechanisms such as Foreign Intelligence Surveillance Act ("FISA") Section 702 and other intelligence gathering activities under Executive Order ("EO") 12333, or "no notification" orders under the Electronic Communications Privacy Act ("ECPA"), authorized by a court, which allow for records requests to electronic communications service providers and generally do not permit immediate notification to the data subject of the existence of the order. The U.S. Department of Commerce published its **formal response** to the decision in September 2020 to specifically address questions and concerns about the use of these mechanisms to reach personal data. We encourage customers to read this whitepaper. Entrust has assessed whether it has reason to believe that the FISA Section 702 and EO 12333 measures would prevent Entrust from fulfilling its obligations under the SCCs. Specifically, with regard to Entrust products, we engaged expert legal counsel to advise on the applicability and reach of these mechanisms to obtain personal data we process on behalf of our customers in the United States.

FISA Section 702

Review of documents issued by U.S. government authorities provides no reason to believe the U.S. government uses FISA Section 702 to target private enterprises nor does it target EEA governments with Section 702 data collection.

EO 12333

EO 12333 does not permit the U.S. government to compel private parties to disclose information, and therefore the government's principal means of collection are voluntary cooperation and technical collection when private party assistance is not needed.

ECPA

The ECPA regulates when Electronic Communications Service Providers ("ECS") and Remote Computing Service Providers ("RCS") may or must disclose user or subscriber records and communications to law enforcement agencies. An ECS or RCS can be subject to subpoenas, court orders, and court-issued ECPA warrants. However, any of these forms of legal process must be either issued by a court or otherwise subject to judicial oversight.

Risk Assessment

While Entrust qualifies as an ESC for customers purchasing our Identity and Access Management products, Entrust has concluded that it has no reason to believe that FISA Section 702, EO 12333, or the ECPA would prevent Entrust from fulfilling its obligations under the SCCs in the specific circumstances of the transfers involved with its products and services. Entrust has based this conclusion on an assessment of the type of personal data processed by Entrust, review of relevant public documents and statements issued by U.S. government authorities, and in consultation with external counsel. Overall, Entrust is unlikely to receive such a request for customer personal data under FISA 702, EO 12333, or the ECPA.

Implementation of EDPB Recommendations

Step Four: Identify and adopt any supplementary measures

This step is only required if the assessment of the effectiveness of the transfer mechanism indicates that supplementary measures should be taken. Entrust's assessment concludes that customer personal data is protected to the relevant standard. Entrust has implemented robust privacy and security measures for our customers including the following:

Entrust prioritizes protecting customer data by:

- **Implementing Privacy by Design into the development of our products and services**
- **Requiring our vendors and sub-processors to meet our data security and privacy standards**
- **Regularly conducting data mapping and data protection impact assessments**
- **Maintaining a comprehensive record retention schedule and purging data in accordance with it**
- **Providing customers instant access to our data privacy resources on our website**

Technical and organizational measures

Entrust implements robust organizational measures to protect transferred personal data including information security, asset management, physical and environmental security, access control, security incident management, and business continuity management.

Entrust's corporate information security management system ("ISMS") is ISO 27001 compliant. Additionally, Entrust maintains compliance certifications to various other information security standards and frameworks, depending on the product, service, and geographic location.

For more information about Entrust's technical and organizational security measures, please see Annex II to the Standard Contractual Clauses in our **Customer DPA**.

Contractual measures

Entrust has updated its **DPAs** to include the 2021 SCCs and makes strong contractual commitments about the measures we take to protect customer personal data in our standard product terms and conditions and agreements with customers.

Unless required by law, Entrust will not disclose or provide access to customer data to law enforcement. If Entrust is compelled to disclose or provide access to customer data to law enforcement, Entrust will promptly notify the customer and provide a copy of the demand unless Entrust is legally prohibited from doing so.

Implementation of EDPB Recommendations

Step Five: Take formal procedural steps adopting needed supplementary measures

This step is only required if the assessment of the effectiveness of the transfer mechanism indicates that supplementary measure should be taken. Entrust's assessment did not indicate supplementary measures should be taken, and therefore, there are not any formal procedural steps needed. In terms of contractual measures, Entrust publishes its **DPA** with the 2021 SCCs included for all new customers and customers who want to upgrade to the new SCCs.

Step Six: Re-evaluate

As the data privacy regulatory and legislative landscape continues to evolve, Entrust's Privacy team is closely monitoring these developments to ensure that we anticipate, identify, and are prepared to respond to changes. Entrust has updated its **DPAs** and will continue to do so as needed. We also regularly update our **sub-processor list** and **data privacy resources**.

Contact Us

For questions about this whitepaper, please contact **privacy@entrust.com**. For more information about Entrust Corporation's data privacy program, please click **here**.