Salesforce's Data Transfer Mechanisms FAQ

Updated: April 2025

This document is provided for informational purposes only. It is not intended to provide legal advice. Salesforce urges its customers to consult with their own legal counsel to familiarize themselves with the requirements that govern their specific situations. This information is provided as of the date of document publication, and may not account for changes after the date of publication. For further information on our privacy practices, please see other resources on the Privacy website available here.

At Salesforce, trust is our #1 value. Nothing is more important than the success of our customers and the privacy of our customers' data. We have a robust privacy program that meets the highest standards in the industry and, as part of that program, we offer various transfer tools and frameworks, each of which, by itself, is sufficient to legalize transfers, facilitating the free flow of personal data around the globe. These include: (i) EU and UK Binding Corporate Rules ("BCRs") for processors; (ii) Standard Contractual Clauses; (iii) certification to the Data Privacy Frameworks (EU-US, Swiss-US, and UK Extension), and (iv) the APEC Privacy Framework (CBPRs and PRPs), together with robust supplementary measures where required.

If you have questions specifically relating to our data processing addendum ("**DPA**"), please see our DPA FAQ.

Table of Contents

DATA TRANSFERS

a. How can personal data be transferred globally?

Salesforce offers its services globally, and use of our services involves transfers of personal data. For example, customers can log in to our services and manage their data from anywhere in the world.

Under certain global privacy laws, including those of Europe, personal data cannot be transferred to other destinations unless (i) the importing country has been deemed adequate, or (ii) the data exporter has appropriate safeguards in place to ensure that the personal data transferred is subject to an adequate level of data protection.

b. What is adequacy?

Various global privacy authorities have the power to determine whether a country outside of its respective jurisdiction has an adequate level of data protection. The effect of an adequacy decision is that personal data can be transferred from the jurisdiction in question to the adequate jurisdiction and/or to an entity deemed as adequate without any further transfer mechanism being necessary.

c. How does Salesforce legalize, and also help its customers legalize, transfers of personal data outside of Europe?

Salesforce certified to the **EU-US Data Privacy Framework**, meaning that the US has "adequacy" status for transfers via our services and such transfers can be handled in the same way as intra-EU transmissions of data (see below more for information).

Salesforce offers the following transfer mechanisms as "appropriate safeguards" to legitimize cross-border data transfers to non-adequate countries:

- EU and UK **Binding Corporate Rules for processors ("BCRs"):** these are company-specific, group-wide data protection policies approved by either the EU data protection authorities or the UK's Information Commissioner's Office (ICO) to facilitate international transfers of personal data from the European Economic Area or the UK to organizations that are located in third countries that have not been deemed adequate by the relevant regulators. For more information, see "*What are BCRs?*" below.

- **Standard Contractual Clauses ("SCCs")**: legal contracts entered into between contracting parties who are transferring personal data to third countries. The most recent set of SCCs are those pursuant to Regulation 2016/679 and were released in 2021 ("**2021 SCCs**"). For more information, see "*What are the Standard Contractual Clauses?*" below.

Salesforce also has additional technical, organizational and contractual measures in place as described in its Transfer Impact Assessment.

Salesforce is in the unique position of being able to offer these transfer mechanisms to its customers, each of which is, by itself, sufficient to legalize transfers of personal data outside of the UK or the European Economic Area. Salesforce has both sets of BCRs and the 2021 SCCs incorporated into its Data Processing Addendum ("**DPA**").

For further information:

- Salesforce's EU and UK BCRs can be found here.
- A full copy of the 2021 SCCs is available here.
- A copy of the Salesforce DPA can be found here.

TRANSFER TOOLS & FRAMEWORKS

BCRs

a. What are BCRs?

BCRs are company-specific, group-wide data protection policies approved by data protection authorities to facilitate international transfers of personal data to countries that have not otherwise been deemed adequate. Obtaining BCRs requires intensive consultation with data protection authorities, who approve them based on strict privacy principles.

Salesforce has both EU and UK BCRs for transfers out of the EU and the UK, respectively. BCRs are seen as the "gold standard" of transfer mechanisms because of the rigorous approval process. Salesforce was the first top 10 software company in the world to achieve approval for

its processor EU BCRs. The protections offered by EU BCRs also extend to Switzerland. Customers established in Switzerland that process personal data in accordance with Swiss local laws will benefit from the undertakings that Salesforce makes in the BCRs.

Salesforce was also one of the first six companies in the UK to receive approval for its UK BCRs, which apply to customer transfers from the UK or where the customer has contractually specified that UK data protection laws apply.

b. Who approved Salesforce's BCRs?

- **EU BCRs:** Salesforce received approval for its EU BCRs from European data protection authorities in November 2015. The French data protection authority, known as the CNIL, served as Salesforce's lead authority, and the Dutch and Bavarian data protection authorities served as co-lead authorities. In accordance with requirements established by European data protection authorities as part of the former Article 29 Working Party (now the European Data Protection Board under the GDPR), EU data protection authorities as well as the data protection authorities of Iceland, Liechtenstein, and Norway, were part of the approval process.

- **UK BCRs:** Salesforce received approval for its UK BCRs in January 2023 from the UK's data protection authority, the Information Commissioner's Office (ICO).

c. To which services do the Salesforce BCRs apply?

To check which services the BCRs apply to please see Appendix A of the relevant set of the BCRs.

STANDARD CONTRACTUAL CLAUSES

a. What are the Standard Contractual Clauses?

The Standard Contractual Clauses are legal contracts entered into between contracting parties who are transferring European personal data internationally. The original controller to processor Standard Contractual Clauses were drafted and approved by the European Commission in 2010. In June 2021, the European Commission published the 2021 SCCs.

A copy of the 2021 SCCs is available here and you can also find additional information on the 2021 SCCs on the official website of the European Commission.

b. To which services do the 2021 SCCs apply?

The 2021 SCCs apply to all services provided by Salesforce.

c. How does Salesforce legalize transfers from the UK post-Brexit?

The Salesforce DPA incorporates the international data transfer addendum to the European Commission's standard contractual clauses for international data transfers ("**UK addendum**") to legalize transfers of UK personal data to non-adequate countries using the 2021 SCCs. The UK addendum is incorporated by reference and is available here. Additionally, as of July, 24, 2023, Salesforce certified our commitment to comply with the UK Extension to the EU-US Data Privacy Framework for transfers of personal data from the UK (and Gibraltar).

EU-US DATA PRIVACY FRAMEWORK AND CORRESPONDING EXECUTIVE ORDER

a. What is the EU-US Data Privacy Framework?

The EU-US Data Privacy Framework ("**DPF**") reflects an agreement between the European Commission and the United States executive branch to foster trans-Atlantic data flows. Under the EU-US DPF, President Biden issued the Executive Order on Enhancing Safeguards for United States Signals Intelligence Activities ("**Executive Order**"), which provides additional safeguards and redress for European individuals whose personal data is potentially affected by US surveillance activities. Specifically, it provides binding safeguards that limit access to data collected by US surveillance activities, establishes an independent and impartial redress mechanism, and enhances US oversight of surveillance intelligence.

b. What is the practical effect of the EU-US DPF and Executive Order?

On July 10 2023, the European Commission adopted its adequacy decision with respect to the EU-US DPF. The adequacy decision concludes that the US ensures an adequate level of protection, compared to that of the EU, for personal data transferred from the EU to US organizations certified under the EU-US DPF. As a result, organizations from the European Economic Area are able to transfer personal data to US organizations certified under the EU-US DPF, without being subject to any further conditions or authorizations and without the need for any additional data protection safeguards (i.e., transfers can be handled in the same way as intra-EU transfers).

c. What is Salesforce's certification status?

As of July 17, 2023, Salesforce certified to the EU-US DPF, meaning that the US has "adequacy" status for transfers via our services and such transfers can be handled in the same way as intra-EU transmissions of data; no transfer mechanism or additional data protections are required. Salesforce has also certified our commitment to comply with the Swiss-US DPF and, as mentioned above, the UK Extension to the EU-US DPF. You can find additional details about Salesforce's participation in our Notice of Certification.

d. What is the current status of the EU-US DPF?

We understand that recent developments have resurfaced concerns about international data transfers, in particular the stability of the EU-US DPF. The EU-US DPF and its extensions remain valid and can continue to be relied upon by customers to transfer their personal data to the US in Salesforce's services.

In November 2024, the European Commission delivered its first review of the adequacy decision of the EU-US DPF after its first year in effect, and ultimately concluded that US authorities have put in place the necessary structures and procedures to ensure that the framework functions effectively. Further, the Executive Order, which strengthens the privacy and civil liberties safeguards governing US surveillance activities and serves as the basis for the abovementioned adequacy decision, is still in full effect. This means that the EU-US DPF continues to be a valid international data transfer tool.

Salesforce welcomes the European Commission's continued support of the EU-US DPF and we remain committed to continue to meet and exceed the requirements of the framework. As the Norwegian Data Protection Authority clarified, an "adequacy decision remains in force until it is revoked by the European Commission or the Court of Justice of the European Union." Thus, any changes to US law or its independent agencies would not automatically result in the lapse or revocation of the adequacy decision.

APEC PRIVACY FRAMEWORK (CBPRs and PRPs)

a. What is the APEC Privacy Framework?

The Asia-Pacific Economic Cooperation ("APEC") is a regional economic forum established in 1989, aimed at increasing prosperity for the region by promoting balanced, inclusive, sustainable, innovative and secure growth and accelerating regional economic integration.
As part of this Cooperation, the APEC Privacy Framework was adopted. The framework sets out a series of non-binding principles and implementation guidelines to ensure continued trade and economic growth and, in particular, the free flow of data.

The APEC Privacy Framework provides for two different systems and certifications to facilitate cross-border transfers:

1. APEC Cross Border Privacy Rules ("**CBPR**"), to which controllers can certify, i.e. in respect of data processed by companies for their own purposes.

2. APEC Privacy Recognition for Processors ("**PRP**") System, to which processors of personal data can certify, i.e., in respect of data processed on another company's behalf. Generally, Salesforce acts as a processor in respect of its services to customers (as controllers).

Both certifications not only demonstrate a commitment to the APEC Privacy Framework, but also provide a transfer mechanism which allows personal data to be transferred across country borders.

b. What does Salesforce's APEC CBPR and PRP certifications mean in practice?

Salesforce has obtained certification for both the APEC CBPR (for our data controller practices) and the APEC PRP System (for our data processor practices). These certifications demonstrate

our adherence to the APEC framework of accountability for the entire scope of our processing activities, meaning that Salesforce effectively implements the level of protections set out by the APEC CBPR and PRP frameworks. In effect, customers can use Salesforce to transfer customer personal data in accordance with the rules set forth in the APEC Privacy Framework (i.e., it operates as a "transfer mechanism" in certain APEC jurisdictions). More information can be found here.

OTHER

a. Do the BCRs apply to third-party sub-processors?

The BCRs apply only to transfers to and within the Salesforce group. Salesforce therefore relies on SCCs to transfer personal data to third-party sub-processors that are located in third countries. However, the BCRs do contain certain commitments about Salesforce's use of sub-processors, including an obligation to execute a data processing agreement with third-party sub-processors.

b. Does Salesforce have back-to-back agreements with third-party sub-processors?

Yes, Salesforce has data processing agreements in place with its third-party sub-processors. In addition, Salesforce is obliged under both sets of BCRs and SCCs, as well as the Data Privacy Framework, to ensure that, in respect of personal data transferred to third countries, the obligations set out in the SCCs are likewise put in place with sub-processors.

c. What is a Transfer Impact Assessment and is my organization required to perform one?

A Transfer Impact Assessment ("TIA") is an analysis used for transfers of personal data between the EU and third countries that are based on SCCs or BCRs. The purpose of this exercise is to determine whether there is anything in the law and/or practices in force of the third country that may impinge on the effectiveness of the appropriate safeguards of the transfer tools you are relying on, in the context of your specific transfer.

All EU-based data exporters (be they controllers or processors) have a legal obligation to conduct a TIA for transfers to the US that are based on SCCs or BCRs. For transfers based on the EU-US DPF, there is no requirement to conduct a TIA or, as mentioned above, implement additional data protection safeguards.

d. What supplementary measures does Salesforce have in place?

Salesforce offers a host of robust technical, contractual and organizational measures that it offers to support transfers of personal data out of Europe. These measures are discussed in detail in the TIA Whitepaper, including encryption, polymorphic storage of data, and Transparency Reports.

e. What if I have additional questions?

Please reach out to your dedicated Account Executive who will be able to help with any follow up questions that you may have.