Salesforce's Data Processing Addendum FAQ
Updated February 2024

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 protection of our customers' data.

We know you may have questions about the Data Processing Addendum ("**DPA**") that Salesforce offers to its customers. To help you develop a better understanding of the Salesforce DPA, we have created this FAQ to answer some of the most common questions we are asked. All defined terms used in this FAQ are as set out in the DPA.

General

a. Does Salesforce make a DPA available to its Customers?

Yes, Salesforce offers a DPA to its Customers here. The DPA is an agreement that sets out the legal framework under which Salesforce Processes Customer Data and Personal Data. The DPA covers all of Salesforce's services. The DPA is an addendum or exhibit to the Main Services Agreement ("**MSA**") between Salesforce and its Customer.

b. Why can my organization not use its own DPA?

The Salesforce DPA is specific to Salesforce's multi-tenant services and covers our processes in relation to these. For example, the DPA covers our processes around privacy related notifications, audits, certifications, security measures, and sub-processing activities, all of which are aligned to the way in which Salesforce's services and its multi-tenant infrastructure work. The Salesforce DPA is also drafted to seamlessly interoperate with the MSA and other relevant Salesforce Documentation.

c. What is the scope of the DPA?

Although the DPA uses certain terminology from specific laws, e.g. Controller and Processor from the GDPR, it covers Customers globally and sets out relevant legal obligations and commitments related to the processing of Customer Data and Personal Data.

d. Which Customer entities can be a party to the DPA?

The following entities can be a party to the DPA: (i) the entity that signs the MSA, (ii) its Authorized Affiliates who sign an Order Form, and (iii) other Authorized Affiliates that are subject to European laws and are entitled to use the contracted Salesforce services. The purpose of (iii) is to ensure that all Authorized Affiliates that use our services and that must comply with European requirements can benefit from the DPA, including the SCCs.

e. Does the DPA apply to my organization if we don't have offices in Europe?

Yes, the majority of the DPA applies to Customers regardless of their connection to the European Economic Area ("EEA"), Switzerland and the United Kingdom ("UK") (together, "Europe"). Most of the commitments in the DPA are general privacy-related commitments that are not specific to European laws.

f. What are Salesforce and the Customer's respective roles under the DPA?

Salesforce acts as the Processor with respect to Personal Data submitted by Customers to Salesforce's services. The Customer either acts as a Controller or a Processor of such Personal Data. This is set out in the DPA at Section 2.1 ("*Customer's Processing of Personal Data*").

It is for the Customer to determine whether it is acting as a Controller or a Processor in uploading Personal Data to the Salesforce services. In both scenarios, Salesforce acts as a Processor and Processes such Personal Data only in accordance with the Customer's documented instructions.

g. How do Customers execute the DPA?

Customers can download the DPA from our website, and then complete, sign and return the DPA to dataprocessingaddendum@salesforce.com. Further information on the execution of the DPA can be found in the "*How to execute this DPA*" section in the opening preamble of the DPA.

2. Data Subject Requests

How does Salesforce handle requests from Data Subjects?

If Salesforce receives a Data Subject Request from a Customer's customer or end user in respect of Personal Data for which Salesforce acts as a Processor, Salesforce will, to the extent legally permitted, ask the Data Subject to contact the Customer directly about the request. Salesforce will also, in accordance with the commitments set out in our DPA, promptly notify the Customer although we will not further respond to the Data Subject Request without the Customer's prior consent.

3. Sub-processors

a. Does Salesforce use Sub-processors?

An effective and efficient performance of Salesforce's services requires the use of Sub-processors. These Sub-processors can include Affiliates of Salesforce as well as third party organizations. Salesforce's use of Sub-processors may require the transfer of Customer Data to Sub-processors for purposes like hosting Customer Data, providing customer support, and ensuring the services are working properly. As described in the DPA, Salesforce takes responsibility for the actions of its Sub-processors.

Up-to-date information about the hosting locations for each service and the identities and the locations of Sub-processors can be found in the applicable Infrastructure and Sub-processor Documentation (available here).

b. How does Salesforce notify its Customers of new Sub-processors?

Customers may subscribe to notifications of new Sub-processors (see here). Salesforce will notify all subscribed Customers of a new Sub-processor before authorizing the new Sub-processor to process Customer Data. Customers may object to the intended use of a new Sub-processor using the procedure set out in the DPA.

4. Technical and Organizational Measures

What security measures are in place to protect Customer Data?

Salesforce maintains appropriate technical and organizational measures to protect Customer Data, as set forth in the applicable Security, Architecture and Privacy ("**SPARC**") Documentation

(available here).

Please also see Salesforce's dedicated Security page and our Compliance website detailing our compliance certifications and attestations.

5. Security Breach Notification

How would Salesforce notify its Customers in the event of a security breach?

Salesforce maintains security incident management policies and procedures, which are described in the applicable SPARC Documentation (available here). In Section 7 of the DPA (available here) Salesforce commits to notify Customers without undue delay after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data processed by Salesforce or its Sub-processors.

If your organization is impacted by a security breach, your organization's Security Contact(s) will be notified. Steps on how to create and maintain your Security Contact List are available here.

6. Government Access Requests

What happens if Salesforce receives a government access request in respect of Customer Data?

At Salesforce, trust is our number one value. The protection of our Customers' data is paramount, and we safeguard that data with a robust, comprehensive, and transparent privacy and security program. Our privacy and security program is designed to protect Customer Data against unauthorized access or disclosure.

Salesforce may on occasion receive a request from a government agency or law enforcement authority seeking access to data belonging to a Customer. Salesforce is not the owner of Customer Data and, accordingly, if we receive a government request for Customer Data, if permitted by law, we try to refer the request to the affected customer so that the Customer can work with the governmental agency directly to respond. We do not disclose Customer Data to government agencies unless compelled by law and we also challenge unlawful requests.

For more information on how Salesforce handles any such requests please see Salesforce's Transparency Report that also details the number of government access requests we receive, here.

7. Return and Deletion of Customer Data

What happens to Customer Data after termination or expiration of an agreement with Salesforce?

After termination or expiration of the agreement, Salesforce will return and delete all Customer Data in accordance with the procedures and timeframes specified in the applicable SPARC Documentation (available here). Until Customer Data is deleted or returned, Salesforce will

continue to comply with the DPA and its Schedules.

8. European Data Transfers

What transfer tools and frameworks does Salesforce offer in its DPA?

Salesforce offers various transfer tools and frameworks (collectively, "**transfer mechanisms**") to facilitate the free flow of personal data around the globe, which are incorporated into its DPA:

- **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 third countries that have not been deemed adequate by the relevant regulators.
- **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 were released in 2021.
- **EU-US Data Privacy Framework ("DPF") and its extensions**: the DPF reflects an agreement between the European Commission and the United States to foster trans-Atlantic data flows. EEA, Swiss and UK organizations are able to transfer personal data to US organizations certified under the DPF, without being subject to any further conditions or authorizations and without the need for any additional data protection safeguards.

For further information, please see our Data Transfer Mechanism FAQs, available here.

a. Which transfer mechanism prevails in the DPA: the BCRs or the SCCs?

The DPA does not contain an order of precedence for the transfer mechanisms available to Customers. For example, where both the SCCs and the BCRs apply to a particular service, Customers may choose either or to invoke the protections afforded by their transfer tool of choice. All Salesforce services are covered by the SCCs by default. If you wish to check whether the relevant Salesforce service is also covered by the BCRs, please see Appendix A of our BCRs.

Please note that, following the EU Commission's adequacy decision for the EU-US Data Privacy Framework and Salesforce's certification under the same, the DPF automatically applies to transfers of Personal Data outside of Europe to Salesforce Inc., without being subject to any further authorizations and without the need for any additional data protection safeguards.

b. Why does Schedule 1 to the DPA contain additional terms about the BCRs and SCCs?

Schedule 1 includes certain provisions to clarify how the BCRs are incorporated into the DPA. It also ensures that in the event of any conflict between the BCRs and the DPA, the BCRs will prevail.

Schedule 1 also incorporates the SCCs into the DPA and describes how the SCCs requirements around use of Sub-processors, audits, and data deletion certifications apply to Salesforce's services. Schedule 1 also stipulates that the SCCs will prevail over the DPA in the event of a conflict with the DPA.

c. How does the DPA address the *Schrems II* decision and associated EDPB Recommendations 01/2020?

The DPA contains the following commitments:

- **SCCs.** The DPA incorporates the SCCs, allowing Customers to apply the protections in the SCCs to Personal Data transferred outside of Europe.
- **DPF.** The DPA incorporates the EU-US Data Privacy Framework and its extensions for Personal Data transferred outside of Europe. The European Commission adopted its adequacy decision with respect to the DPF, following enhanced protections and redress for European individuals under US law in response to key issues raised by the CJEU in the Schrems II ruling.
- **Compliance with local laws.** Under the DPA, BCRs, and the 2021 SCCs, Salesforce commits that it has no reason to believe that any local laws applicable to Salesforce would prevent Salesforce from fulfilling its obligations under the DPA, BCRs or SCCs. Salesforce is obliged to notify Customers if it no longer believes that it can make this commitment and, if Salesforce cannot address the problem, Customers are then able to terminate the applicable Order Form(s).
- **Government access requests.** In addition to the commitments made in the BCRs and SCCs, the DPA further includes a government access request clause (clause 8) that requires Salesforce to notify Customers of any government access requests applying to Customer Data (including Personal Data), unless legally prohibited, and contains a number of commitments about how Salesforce handles such requests.
- **Security.** Salesforce commits to implement appropriate technical and organizational safeguards to protect Personal Data. Descriptions of specific safeguards for each of Salesforce's services are included in the SPARC Documentation for each service, available here.

If you would like information on how Salesforce deals with transfers of personal data more generally, please see Salesforce's Data Transfer Mechanism FAQs, available here.

Which Module of the SCCs applies to my relationship with Salesforce?

To provide Customers with maximum flexibility, Salesforce has incorporated both Module 2 (Controller to Processor) and Module 3 (Processor to Processor) of the SCCs into the DPA. It is for Customers to determine which Module applies to the circumstances of their processing and complete their records of processing accordingly; no amends to the DPA are required.

d. Why are the SCCs not attached to the DPA?

Given the length of the SCCs, Salesforce has chosen to incorporate the SCCs by reference into the DPA. A complete copy of the SCCs is set out here. Customers may execute the SCCs separately following the procedure set out in the DPA.

The UK addendum is also incorporated by reference and is available here.

e. How do Customers enter into the SCCs?

As mentioned above, Salesforce's DPA incorporates the SCCs by reference. For Customers with DPAs executed before September 24, 2021, Salesforce offers the following options:

1. Enter into the DPA, available here, which will replace the Customer's existing DPA in its entirety; or
2. Enter into the Amendment to Data Processing Addendum (SCC Amendment), available here, which replaces the existing SCCs and SCC specific terms with the SCCs and SCC-specific terms. The Customer's existing DPA will otherwise remain unaffected.

DPAs signed after September 2022 include the UK addendum. Customers with DPAs executed before September 2022 who wish to incorporate the UK addendum may choose to: (i) enter into a new DPA as per option (1) above; or (ii) enter into a UK Addendum Amendment, available here, which incorporates the UK addendum into their existing DPA (which will otherwise remain unaffected).

For both options, Customers can download the relevant agreement from our website, and complete, sign and return the agreement to dataprocessingaddendum@salesforce.com.

f. What if I have additional questions not answered in this FAQ?

If you have additional questions, please contact your Account Executive or open a case with the Salesforce customer support team via the Help & Training success community here.

g. Where can I find additional legal documentation and information about Salesforce's services?

- Salesforce's DPA can be found here.
- Salesforce's Amendment to the Data Processing Addendum (SCC Amendment) can be found here.
- Salesforce's MSA, which incorporates the DPA, can be found here.
- The Security Privacy and Architecture Documentation (**"SPARC**") detailing Salesforce's security measures, and the Infrastructure and Sub-processor Documentation listing Salesforce's Sub-processors, are available in the Trust and Compliance Documentation section here.
- Details on Salesforce's transfer mechanisms can be found in our Data Transfer Mechanism FAQs, here.
- Salesforce's Privacy website can be found here, and provides further information on Salesforce's Privacy programme as well as helpful references including white papers on key topics and documents providing information to assist customers with the completion of data protection impact assessments ("**DPIAs**").
- The Salesforce Compliance website detailing our compliance certifications and attestations can be found here.
- Salesforce also has a dedicated Security page which details best practices, training and

security advisories.

- Salesforce offers publicly available Trailhead modules that can be used to learn about relevant topics. The trail for European Privacy Laws can be found here and the trail for US Privacy Laws can be found here.