



Data Processing Addendum (DPA) Frequently Asked Questions:

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 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 outlined the most common questions asked. All defined terms used in this FAQ are as set out in Salesforce’s DPA.

This document does not provide legal advice and the information we present may not take into account future changes in laws and regulations. We urge you to consult with your own legal counsel to familiarize yourself with the requirements that govern your specific situation.

Detailed explanations of how we process Personal Data are available on our [Privacy Website](#).

General

1. Does Salesforce make a DPA available to its customers?	03
2. Does the DPA take GDPR into account?	03
3. Why can my organization not use its own DPA?	03
4. How do customers incorporate Salesforce’s DPA into their existing Salesforce contract?	03
5. What happens if my organization does not sign the DPA?	04
6. Where can I find additional legal documentation and information about Salesforce’s services?	04
7. What if I have additional questions not answered in this FAQ?	04

Body of the DPA

8. What is the scope of the DPA?	05
9. Which customer entities can be a party to the DPA?	05
10. Does the DPA apply to my organization if we don’t have offices in the EU?	05
11. What is contained in the schedules to the DPA?	05



12. What are Salesforce's and the customer's respective roles under the DPA?	06
13. How does Salesforce handle requests of data subjects?	06
14. Does Salesforce use Sub-processors?	06
15. How does Salesforce notify its customers of new Sub-processors?	06
16. What security measures are in place to protect Customer Data?	07
17. How would Salesforce notify its customers in the event of a security breach?	07
18. What happens to Customer Data after termination or expiration of an agreement with Salesforce?	07

Transfer Mechanisms

Please see 'Salesforce's International Transfers of Personal Data FAQs'.	07
--	----



General

1. Does Salesforce make a DPA available to its customers?

Yes, Salesforce offers a DPA to its customers: the document can be found [here](#). The DPA is an agreement that sets out the legal framework under which Salesforce processes Personal Data. The DPA covers all of the services provided by Salesforce. The DPA is an addendum or exhibit to the Master Subscription Agreement (“MSA”) between Salesforce and our customer, and forms part of the customer agreement.

2. Does the DPA take GDPR into account?

Yes, Salesforce’s current DPA includes provisions to assist customers with their GDPR compliance. Customers who signed earlier versions of our DPA, or who entered into an MSA without a DPA, can sign our current DPA at any time. For existing customers with DPAs, the current DPA only adds to what a customer already has and does not replace any comparable or additional rights featured in their existing DPA (see the DPA section ‘How this DPA Applies’).

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

The Salesforce DPA is specific to Salesforce’s multi-tenant services and covers the specific processes and procedures in relation to, for example, specific notifications related to privacy; 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 also clearly identifies which Salesforce services are covered by each of the two transfer mechanisms that Salesforce offers to its customers: Binding Corporate Rules for Processors (“BCRs”) and the Standard Contractual Clauses. More information about these mechanisms is available in the ‘Transfer Mechanisms’ section below.

The Salesforce DPA is also drafted to seamlessly interoperate with the MSA and other relevant Salesforce documentation.

4. How do customers incorporate Salesforce’s DPA into their existing Salesforce contract?

Salesforce’s online DPA is pre-signed by Salesforce. Where a customer is signing Salesforce’s online DPA, the customer may 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 Section “How to execute this DPA” in the opening preamble of the DPA.



Where a customer signs a DPA as part of their MSA or order form, the customer will **not** need to sign again or return the DPA to dataprocessingaddendum@salesforce.com.

5. What happens if my organization does not sign the DPA?

Salesforce recommends you consult with your legal advisor to assess the potential impact your decision not to sign the DPA may have on your particular situation.

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

- Salesforce's DPA 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](#) by selecting the relevant service.
 - Details and associated documentation about Salesforce's transfer mechanisms can be found in the 'Transfer Mechanism' section below.
 - 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](#).
-



7. 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](#).

Body of the DPA

8. What is the scope of the DPA?

Although the DPA uses specific terminology based on EU data protection laws and regulations (e.g. controller, processor, etc.), it covers all jurisdictions and also applies to non-EU customers. The DPA sets out relevant legal obligations and commitments related to the processing of Customer Data and Personal Data.

9. 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 Affiliates who sign an Order Form, and (iii) other customer Affiliates that are subject to European laws and regulations and are entitled to use the contracted Salesforce services. The purpose of (iii) is to ensure that all affiliates that use our services and that must comply with European requirements can benefit from the DPA and the Standard Contractual Clauses.

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

Yes, the majority of the DPA applies to customers, regardless of their connection to the EU. Most of the commitments in the DPA are general privacy related commitments which are not specific to EU laws.

11. What is contained in the schedules to the DPA?

The DPA includes three schedules:

1. Schedule 1 contains clarifications relating to the two transfer mechanisms that Salesforce offers its European customers: (i) BCRs; and (ii) the Standard Contractual Clauses (controller to processor).
2. Schedule 2 provides specific details of the types of data and the categories of data subjects involved in the processing activity.



- Schedule 3 contains the Standard Contractual Clauses (controller to processor) that apply to Salesforce's services. This schedule also contains appendixes detailing data processing (Appendix 1) and incorporating the Security, Privacy and Architecture Documentation (Appendix 2), as well as details about the product-specific applicability of the Standard Contractual Clauses (Appendix 3).
-

12. What are Salesforce's 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, and the customer acts as the Controller. This means that Salesforce's customers uniquely determine what Personal Data is submitted to and processed by Salesforce's services, and that Salesforce processes Personal Data only in accordance with the customer's documented instructions. This is set out in the DPA at Section 2.1 ("Roles of the Parties").

13. How does Salesforce handle requests of data subjects?

If Salesforce receives a data subject request from a customer's customer, Salesforce is the Processor, and we will, to the extent that applicable legislation does not prohibit Salesforce from doing so, promptly suggest that the data subject contact the customer (i.e. the Controller) directly about the request. Salesforce will not further respond to a data subject request without the customer's prior consent.

14. 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 that Salesforce offers and the identities and the locations of Sub-processors can be found in the applicable Infrastructure and Sub-processor Documentation (available [here](#) by selecting the relevant service).



16. 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 SPARC Documentation (available [here](#) by selecting the relevant service). Please also see Salesforce's dedicated [Security page](#) and our [Compliance website](#) detailing our compliance certifications and attestations.

17. How would Salesforce notify its customers in the event of a security breach?

Salesforce maintains security incident management policies and procedures, which are specified in the applicable SPARC Documentation (available [here](#) by selecting the relevant service). Salesforce commits to notifying its 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.

18. 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](#) by selecting the relevant service).

Transfer Mechanisms

Please see '[Salesforce's International Transfers of Data FAQs](#)'.
