Data Processing Addendum (DPA) FAQ

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? 05
BODY OF THE DPA

8. What is the scope of the DPA?

9. Which customer entities can be a party to the DPA?

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

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

12. What are Salesforce’s and the customer’s respective roles under the DPA?

13. How does Salesforce handle requests of data subjects?

14. Does Salesforce use Sub-processors?

15. How does Salesforce notify its customers of new Sub-processors?

16. What security measures are in place to protect Customer Data?

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

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

TRANSFER MECHANISMS

19. How does Salesforce help its customers to legalize the transfer of Personal Data outside of the European Economic Area (EEA)

20. What are BCRs, Privacy Shield, and the European Commission Standard Contractual Clauses?

21. To which services do the BCRs, Privacy Shield and the Standard Contractual Clauses apply?

22. Why does Schedule 1 to the DPA contain additional terms about the available transfer mechanism

23. Who approved Salesforce’s BCRs?

24. Have Salesforce’s BCRs ever been updated?

25. Which types of data transfers can be legalized by the BCRs?

26. What other transfer mechanisms are available if BCRs do not apply?

27. What steps does my company need to take to benefit from the Privacy Shield framework?

28. What steps has Salesforce taken to prepare for Brexit (the UK’s departure from the European Union)?
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 three transfer mechanisms that Salesforce offers to its customers: Binding Corporate Rules for Processors (“BCRs”); the EU-U.S. and Swiss-U.S. Privacy Shield (“Privacy Shield”); 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 and Salesforce sign a DPA at the same time the customer and Salesforce execute a 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 that you consult with your legal advisor to assess the potential impact that 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 three transfer mechanisms that Salesforce offers its European customers: (i) BCRs; (ii) the Privacy Shield; and (iii) 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.
3. 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).

15. How does Salesforce notify its customers of new Sub-processors?
Customers may subscribe to notifications of new Sub-processors for each service (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.
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

19. How does Salesforce help its customers to legalize the transfer of Personal Data outside of the European Economic Area (EEA)?

Salesforce has three transfer mechanisms incorporated into its data processing addendum (“DPA”). More information about each is available at the following links:

- The full text of Salesforce's BCRs can be found here.
- Salesforce's notice of certification to the EU-US and Swiss-US Privacy Shield frameworks can be found here.
- A copy of the controller to processor EU Standard Contractual Clauses can be found at Schedule 3 of our DPA, available here.

The DPA sets out of the scope of applicability of these transfer mechanisms through an order of precedence clause.

20. What are BCRs, Privacy Shield, and the European Commission Standard Contractual Clauses?

BCRs are company-specific, group-wide data protection policies approved by European data protection authorities to facilitate international transfers of personal data from the EEA to other countries. Obtaining BCRs requires intensive consultation with European data protection authorities, who approve them based on strict privacy principles. Salesforce was the first top 10 software company in the world to achieve approval for its processor BCRs. BCRs are seen as the “gold standard” of transfer mechanisms given the rigorous approval process. Additional information about BCRs can be found on the European Commission's website.

The EU-U.S. Privacy Shield framework was designed by the U.S. Department of Commerce and the European Commission to provide U.S companies with a mechanism to comply with European data protection requirements when receiving personal data from the EU. The framework was later adopted by the rest of the EEA, and the U.S. reached a similar agreement with Switzerland; as a result, the Privacy Shield framework now applies throughout the EEA and Switzerland. To certify, U.S. companies may submit certifications committing to comply with the EU-U.S. or the Swiss-U.S. Privacy Shield frameworks. Certified companies must undertake annual verification to demonstrate compliance, and compliance is subject to oversight and enforcement by the U.S. Federal Trade Commission. Additional information on the Privacy Shield is available on the official Privacy Shield website.
21. To which services do the BCRs, Privacy Shield and the EU Standard Contractual Clauses apply?

The BCRs apply to the Salesforce's services listed in Appendix A to the BCRs available [here](#). The Privacy Shield applies to the services that are listed in Salesforce’s Privacy Shield notice of certification available [here](#). Schedule 3 of the [DPA](#) contains the list of services that are covered by our EU Standard Contractual Clauses.

22. Why does Schedule 1 to the DPA contain additional terms about the available transfer mechanisms?

Schedule 1 includes certain provisions to incorporate the BCRs into the DPA, and to make the provision of the BCRs enforceable between Salesforce and its customers. This procedure was endorsed by European data protection authorities during Salesforce’s BCR approval process. 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 Privacy Shield framework into the DPA and imposes an obligation on Salesforce to ensure that Salesforce maintains its self-certifications to and compliance with the Privacy Shield frameworks.

Finally, Schedule 1 incorporates the EU Standard Contractual Clauses into the DPA and describes how the clauses’ requirements around use of sub-processors, audits, and data deletion certifications apply to Salesforce's cloud services. Schedule 1 also stipulates that the EU Standard Contractual Clauses will prevail over the DPA in the event of a conflict with the DPA.

23. Who approved Salesforce’s BCRs?

Salesforce received approval for its BCRs for processors 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 EU 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 EEA member states of Iceland, Liechtenstein, and Norway, were part of the approval process.

24. Have Salesforce’s BCRs ever been updated?
Salesforce has updated its Binding Corporate Rules twice since 2015.

In November 2018, Salesforce updated its BCRs to (i) bring them in line with the GDPR (the previous version was adopted under the EU Data Protection Directive) and (ii) expand the BCRs to new services. This GDPR update was required by November 2018 under Salesforce’s annual BCR reporting to the CNIL and did not need to be completed by May 2018, when the GDPR took effect.

In November 2019, Salesforce updated its BCRs to include additional new services. We also made updates to Sections 5 and 6 and Appendix A of the BCRs to make the BCRs more applicable to Salesforce’s services generally. Salesforce has notified CNIL of this further update under Salesforce’s annual BCR reporting to the CNIL.

No service previously covered by the BCRs was removed during these updates. For more information on what services are now covered by our BCRs, see Appendix A to the BCRs, which is available here.

25. Which types of data transfers can be legalized by the BCRs?
The BCRs legalize three categories of data transfers. First, transfers of Personal Data from customers to members of the Salesforce Group. Second, transfers between members of the Salesforce Group. Third, transfers from members of the Salesforce Group to third-party Sub-processors if these third-parties signed appropriate back-to-back agreements with Salesforce.

26. What other transfer mechanisms are available if BCRs do not apply?
Two additional transfer mechanisms, the Privacy Shield and EU Standard Contractual Clauses, are incorporated in the DPA. Each mechanism provides another method for customers to legalize the transfer of their Personal Data to Salesforce’s services.

27. What steps does my company need to take to benefit from the Privacy Shield certification?
Customers using services that are not within the scope of the Salesforce BCRs may take advantage of Salesforce’s Privacy Shield certification. Privacy Shield applies automatically to all services that are within the scope of Salesforce’s Privacy Shield certification.
Please find additional details on Salesforce's Privacy Shield Certification in Salesforce's Notice of Certification, available [here](#).

28. **What steps has Salesforce taken to prepare for Brexit (the UK’s departure from the European Union)?**

Irrespective of the outcome of the ongoing Brexit negotiations, Salesforce remains committed to the success of our customers and employees in the UK and the rest of the EU.

We are closely monitoring the negotiations between the UK government and the European Union regarding the details of their future relationship. As the details become clear, we will take appropriate measures to ensure that our customers can continue to use our services in compliance with both EU and UK laws.

As part of this preparation, Salesforce’s internal Brexit Working Group is looking at possible scenarios, with special attention on areas important to our customers and our business like data transfer restrictions. While we hope that an agreement will allow unhindered delivery of services across the UK and EU, we are also planning for other scenarios to ensure that our customers can continue to use our services without interruption or inconvenience.

The success of our customers is our top priority, and if the outcome of the Brexit negotiations requires any change in the way in which we deliver our services, we will work to enable those changes with minimal disruption and with as much notice to customers as possible.