DATA PROCESSING ADDENDUM (DPA) - FREQUENTLY ASKED QUESTIONS

Updated January 2019

At Salesforce, nothing is more important to our company than the privacy of our customers' data. The protection of our customers' data is of the utmost importance, and given our commitment to trust, we safeguard Customer Data with a robust, comprehensive and fully transparent privacy program. Detailed explanations of how we process Personal Data are available on our Privacy Website.

Additionally, we publish a General Data Protection Regulation ("**GDPR**") Website, outlining our approach to the regulation, explaining how we help support our customers on their GDPR compliance journey, and championing the new opportunities that have resulted from the GDPR. Our GDPR-ready Data Processing Addendum is available on this website in addition to numerous other resources.

This FAQ provides you with information about the commitments Salesforce makes in respect of our Personal Data processed on behalf of our Customers as set out in Salesforce's Data Processing Addendum.

All defined terms used in this FAQ are as set out in Salesforce's Data Processing Addendum ("DPA").

GENERAL

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

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 is Salesforce's and the customer's role under the DPA?**
13. **How does Salesforce handle requests of data subjects?**
14. **Does Salesforce make use of Sub-processors?**
15. **How does Salesforce notify its customers of new Sub-processors?**
16. **Which security measures are in place to protect Customer Data?**
17. **How does 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 European Personal Data outside of the EU?**
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 comprise additional terms in respect of the available transfer mechanisms?**
23. **Who approved Salesforce's BCRs?**
24. **Why were Salesforce's BCRs updated and what were the major changes that resulted as part of the BCR update?**
25. **Which types of data transfers can be legalized by the BCRs?**
26. **What other transfer mechanisms are available if BCRs do not cover the transfer of Personal Data?**
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 available a DPA 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 Customer 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 organisation 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 e.g. specific notifications related to privacy, audits, certifications, security measures and sub-processing activities 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") or the Standard Contractual Clauses, see more information in the 'Transfer Mechanisms' section below.

Moreover, the Salesforce DPA is drafted in such a way that it seamlessly interoperates with the MSA and other relevant documentation, including the Security Privacy and Architecture Documentation (**"**SPARC") detailing Salesforce's security measures and the Infrastructure and Sub-processor Lists.

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

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 is signing a DPA which forms an exhibit to their written MSA (and which is not an online click-through MSA), the DPA will be signed separately as part of that MSA and such customer will **not** need to sign and 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 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 GDPR website can be found here, and details the GDPR enhancements made to Salesforce products 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.
- Publicly available Trailheads which provide learning about European Privacy Laws can be found here and 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 alternatively 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 all 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) its Affiliates that are entitled to use the contracted Salesforce services but are not captured by (i) and (ii), to the extent such Affiliate meets the definition of an "Authorized Affiliate" as set out in the DPA. The purpose of (iii) is to ensure that customer Affiliates that are subject to European data protection laws and that are using Salesforce's services but who are not captured by (i) or (ii) above can nonetheless be a party to 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 five 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 outlines what services are covered by the BCRs.
3. Schedule 3 sets out what services are covered by the EU-U.S. and Swiss-U.S. Privacy Shield.
4. Schedule 4 provides specific details of the types of data and the categories of data subjects involved in the processing activity.
5. Schedule 5 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 is Salesforce's and the customer's role under the DPA?

Salesforce acts as the Processor with respect to Personal Data submitted by customers to Salesforce's services, whilst 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 in our capacity as Controller, we will respond to it. If Salesforce receives a data subject request from a customer's customer (ie a User of the services, to whom a customer has provided a User login), Salesforce is the Processor, and we will, to the extent that applicable legislation does not prohibit Salesforce from doing so, promptly inform the customer's customer to contact the customer (i.e. the Controller) directly about any request relating to his/her Personal Data. Salesforce will not further respond to a data subject request without the customer's prior consent.

14. Does Salesforce make use of 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 the hosting of Customer Data and related infrastructure support, or to provide customer support and to ensure the services are working properly. Importantly, as per the Sub-processor section of the DPA, Salesforce remains liable for its Sub-processors to the same extent Salesforce would be liable for its own activity under the DPA.

Up-to-date information about the hosting locations for each service that Salesforce offers and the identity and the location of Sub-processors with potential access to Customer Data 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 in connection with the provision of the applicable services. 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 does Salesforce notify its customers in the event of a security breach?

Salesforce maintains security incident management policies and procedures 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/or delete all Customer Data in accordance with the procedures and timeframes specified in the applicable SPARC Documentation available here by selecting the relevant service. Salesforce's data deletion procedures are an integral part of Salesforce's measures to protect Customer Data.

TRANSFER MECHANISMS

19. How does Salesforce help its customers to legalize the transfer of European Personal Data outside of the EU?

Salesforce has three transfer mechanisms incorporated into its DPA to ensure the legal transfer of our customer's Personal Data outside of the EU. These are: Binding Corporate Rules ("BCRs") for processors, the EU-U.S. and Swiss-U.S. Privacy Shield ("Privacy Shield"), and the European Commission's standard contractual clauses ("Standard Contractual Clauses").

- Salesforce's BCRs can be found here.
- Salesforce's notice of certification to the EU-U.S. and Swiss-U.S. Privacy Shield can be found here.
- A copy of the controller to processor Standard Contractual Clauses can be found at Schedule 5 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 transfers of Personal Data from the EU to other countries. BCRs are based on strict privacy principles established by European data protection authorities and require intensive consultation with European data protection authorities. Salesforce was the first top 10 software company in the world to achieve approval for its 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 Privacy Shield is a framework designed by the U.S. Department of Commerce and the European Commission (or the Swiss Federal Data Protection and Information Commissioner) to provide companies with a mechanism to comply with European (or Swiss) data protection requirements when transferring Personal Data from the EU (or Switzerland) to the U.S. Companies may self-certify to comply with the EU-U.S. or the Swiss-U.S. Privacy Shield frameworks, 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.

The EU Standard Contractual Clauses are legal contracts entered into between contracting parties who are transferring Personal Data from the EU to other countries located outside the EU. The Standard Contractual Clauses were drafted and approved by the European

Commission. You can find additional information on Standard Contractual Clauses on the official website of the European Commission.

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

Please refer to Schedules 2, 3 and 5 of the DPA for a comprehensive overview of the services each transfer mechanism applies to. The body of the DPA also sets forth the order of precedence.

22. Why does Schedule 1 to the DPA comprise additional terms in respect of 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 the 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 contains clarifying wording in respect of the Standard Contractual Clauses. The main purpose is to effectively incorporate the text of the Standard Contractual Clauses into the DPA, which is attached in full to the DPA in Schedule 5. There are also some commercial terms related to the use of sub-processors, audits, requesting a certification of data deletion, and lastly, stipulating that the Standard Contractual Clauses will prevail to the extent there is a conflict with the DPA.

23. Who approved Salesforce's BCRs?

Salesforce has received approval for its BCRs for processors from the 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 Article 29 Working Party, all European data protection authorities in addition to the data protection authorities of European Economic Area member states of Iceland, Liechtenstein, and Norway, were part of the approval process. This means the Salesforce's BCRs are officially recognized across the EU and European Economic Area.

24. Why were Salesforce's BCRs updated and what were the major changes that resulted as part of the BCR update?

Salesforce has updated its Binding Corporate Rules to align them with the GDPR and to further enhance the robust privacy protections offered by Salesforce to its customers. We have also taken the opportunity to onboard new services (Financial Services Cloud, Health Cloud and Einstein Analytics) onto our BCRs.

Salesforce notified the French data protection authority (CNIL) of these updates in November 2018 as part of its annual update to the CNIL.

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

The BCRs approved by the European data protection authorities enable customers to rely on the BCRs to justify the transfer of Personal Data to members of the Salesforce Group located in countries which do not provide adequate Personal Data protection. Second, the BCRs provide a framework to legitimize transfers between members of the Salesforce Group which have all adopted the BCRs. Third, the BCRs are an approved legal basis for data transfers from members of the Salesforce Group to external third party Sub-processors as part of the BCR framework.

26. What other transfer mechanisms are available if BCRs do not cover the transfer of Personal Data?

As stated above, the Privacy Shield and Standard Contractual Clauses are incorporated in the DPA in the event that transfers of Personal Data are not legalized by the BCRs. This can happen in the following circumstance: Some of Salesforce's services are not (yet) covered by the BCRs. Data transfers for such services are either covered by Salesforce's Privacy Shield or by the Standard Contractual Clauses. If a service is not covered by BCRs or the Privacy Shield, the Standard Contractual Clauses can be relied upon to legalize transfers of data outside the EU.

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

Customers using services not within the scope of the Salesforce BCRs, may take advantage of Salesforce's certification under the Privacy Shield. The Privacy Shield framework applies automatically to services within the scope of Salesforce's certification, which are listed within Schedule 3 of the DPA. The Standard Contractual Clauses are incorporated into Salesforce's DPA for the situations where Privacy Shield is not applicable.

Please find additional details on Salesforce's Privacy Shield Certification in Salesforce's Notice of Certification under the Privacy Shield framework as published 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 Europe.

We are closely monitoring the negotiations between the UK government and the European Union regarding the detail 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, and for Salesforce overall, business will continue as usual and will remain focused on our customers' success.

As part of this preparation Salesforce's internal Brexit Working Group is looking at all the possible scenarios, focusing on a number of areas, including data transfer and free movement of citizens across borders. Whilst we are hopeful that a settlement will be reached that allows unhindered delivery of services across the UK and EU, both during any transition period and beyond, Salesforce is developing plans for every scenario to ensure that our customers can continue to use our services without interruption or inconvenience.

The success of our Ohana is our number one priority, and should the outcome of the Brexit negotiations require any changes to the way in which we deliver our services to our customers, our priority will be to enable such changes with minimal disruption and with as much notice as possible.