UPDATED JULY 2020

This document provides information about the privacy and security of the Salesforce Services which can help our customers to assess our security and privacy program, including by completing privacy impact assessments. It does not provide legal advice. We urge you to consult with your own legal counsel to familiarize yourself with the requirements that govern your specific situation. More information about privacy impact assessments can be found here.

Data Protection Impact Assessments & Salesforce Services

At Salesforce, trust is our #1 value, and nothing is more important than the success of our customers and the protection of their data. Salesforce enables our customers to build trusted relationships, putting their customers at the center of everything they do, including protecting individual privacy through compliance with global data protection laws.

Salesforce is committed to both complying with applicable data protection laws when providing services to our customers as a processor and to ensuring that our customers can continue to use our services while complying with the applicable data protection laws. Data protection law compliance requires a partnership between Salesforce and our customers in their use of our services. As part of our commitment to our customers, we've published this document to describe the features customers can use when responding to common requests using the Salesforce Services, and to assist our customers in completing their data protection impact assessment for the Salesforce Services. This document may also help you assess how Salesforce complies with its obligations under applicable data protection laws and customer agreements.

Table of Contents

Definitions

"**Customer**" has the meaning given to it in the MSA, available here.

"**Customer Data"** has the meaning given to it in the DPA available here.

"**DPA**" or "**Data Processing Addendum**" means Salesforce's Data Processing Addendum as amended from time to time, available here.

"**Infrastructure & Sub-processors Documentation**", available here by selecting the relevant Salesforce Service.

"**Personal Data"** has the meaning given to it in the DPA available here.

"**Salesforce Services**" (each a "**Salesforce Service**") has the meaning given to it in the DPA, available here.

“SPARC Documentation” means the Security, Privacy and Architecture Documentation, available here by selecting the relevant Salesforce Service.

All capitalised terms included in this document and not defined herein have the meanings given to them in the Data Processing Addendum, available here.

Security & Architecture

Data protection laws require organizations to use appropriate technical and organizational security measures to protect Personal Data against unauthorized processing and accidental disclosure, access, loss, destruction, or alteration. Salesforce has robust security and privacy programs in place that meet the highest standards in the industry. They enableSalesforce and its Customers to comply with a variety of data protection laws and regulations applicable to the Salesforce Services.

The Salesforce Services are operated in multi-tenant architecture that is designed to segregate and restrict access to Customer Data based on business needs. The architecture provides an effective logical data separation for different Customers via Customer-specific unique identifiers and allows Customer and user role-based access privileges. Additional data segregation is ensured by providing separate environments for different functions, especially for testing and production. Salesforce has implemented procedures designed to ensure that Customer Data is processed only as instructed by the Customer, throughout the entire chain of processing activities by Salesforce and its sub-processors.

Security Controls & Certifications

The Salesforce Services include a variety of security controls, policies and procedures, as further described in our Security, Privacy and Architecture Documentation. Salesforce has obtained multiple industry-standard third-party certifications and audit reports as described in the Security Privacy and Architecture Documentation.

Data Subject Rights

Data protection laws afford individuals whose Personal Data is processed certain rights, depending on where they are resident. These rights require companies to have systems in place to respond to and effectively address individual data subjects’ requests. For example, if an individual submits a request to have its Personal Data deleted and the relevant circumstances apply, companies must be equipped to find the relevant Personal Data linked to that individual and delete it.

More information about how the Salesforce Services enable Customers to handle Data Deletion, Consent Management, Restriction of Processing, Data Access and Portability within the Salesforce Services you can find here.

Provide a general description of the Salesforce Services

For a description of each Salesforce Service, please see the offerings listed on the Salesforce website.

Describe the Personal Data that will be used, stored, collected, disclosed or otherwise Processed on the Service

Salesforce Customers choose what data to submit to, and collect using, the Salesforce Services. The Personal Data processed will vary per Salesforce Service and the Customer's own use-case.

By way of illustration, please see the following examples:

Typical Personal Data processed within the Salesforce Services may include names, contact information and other information about prospects and customers.

Typical Personal Data processed in connection with Marketing Cloud may include information about the consumers who are part of the Customer's Marketing Cloud marketing campaigns (contact information, activity records, transaction records, etc.).

Similarly, for B2C Commerce, typical Personal Data processed may include information about the shoppers who visit the Customer's B2C Commerce-hosted website and create accounts or perform transactions (contact information, activity records, transaction records, etc.).

For Audience Studio, typical Personal Data processed may include data related to consumers' internet browsing activities (e.g., websites visited or advertisements viewed). This data is then tied to pseudonymous device identifiers such as cookies and mobile identifiers. Customers are prohibited from submitting Personal Data such as names, email addresses, or user names to the Audience Studio, other than pseudonymous personal data and IP addresses. In addition, as the Audience Studio adheres to the Network Advertising Initiative (NAI) Code of Conduct (https://www.networkadvertising.org/code-enforcement/code), the Audience Studio may not be used: (i) to associate pseudonymous non-personal identifiers with other personal data in violation of the NAI Code of Conduct; and/or (ii) to use cookies, web beacons, or other tracking mechanisms to collect or store personal data in violation of the NAI Code of Conduct.

Does the Personal Data include “special categories of Personal Data” (as defined under GDPR) or Personal Data related to criminal convictions or offences?

Salesforce Customers may be able to submit “special categories of Personal Data” to certain Salesforce Services as explained in and in accordance with the Security, Privacy and Architecture Documentation.)

Salesforce Customers are responsible for ensuring that submission of any special categories of Personal Data, where permitted, complies with applicable laws.

Does the Personal Data include financial account numbers, government identification numbers, or health information?

The Security, Privacy and Architecture Documentation sets out whether Customers may submit financial account numbers, government identification numbers, or health information for each respective Salesforce Service.

Salesforce Customers are responsible for ensuring that submission of such data, where permitted, complies with applicable laws and the contractual terms in place with Salesforce.

Are the individuals Data Subjects made aware of the details of the Processing of their Personal Data?

Salesforce provides self-service tools that Customers are able to use to interact with their own Data Subjects. Thus, Salesforce does not directly communicate with its Customers’ Data Subjects. Responsibility for making Data Subjects aware of Customers’ Processing of their Personal Data using the Salesforce Services rests with Customers .

To the extent Salesforce Processes Personal Data for its own purposes, the Salesforce Privacy Statement and other privacy-related documentation are publicly available here.

How is access to the Service managed?

Salesforce Customers can assign different levels of access to their users. The Salesforce Services also allow Customers to assign access permissions based on the user’s role. Salesforce’s Customer contracts restrict access by Salesforce’s personnel as further outlined below in the section “Can Salesforce personnel access Personal Data in the Service”.

To the extent Customers need Salesforce's assistance in managing Personal Data, Salesforce has committed to provide assistance as described in its Data Processing Addendum.

Can Salesforce personnel access Personal Data in the Service? If so, where are those personnel located and for what purpose do they need access?

Salesforce's Data Processing Addendum contains a contractual commitment by Salesforce that its personnel may access Personal Data only in accordance with Customer's documented instructions for specific purposes, including processing under the Data Processing Addendum, processing initiated by the Customer in using the Salesforce Services, and processing to comply with other instructions provided by the Customer. The locations of Salesforce's Affiliates that employ personnel who may access Personal Data for these purposes are available in the Infrastructure & Sub-processors Documentation.

Who will manage security?

Salesforce has policies and procedures in place to protect the security of the Salesforce Services. The security policies, procedures, and controls Salesforce makes available to Customers are described in the Security, Privacy and Architecture Documentation.

Salesforce Customers share responsibility for managing security. The Salesforce Services include a variety of security controls that a Salesforce Customer can configure; each Customer is responsible for configuring those security controls and for managing other aspects of Processing under its control such as the security of the Customer's end users' computers, and controlling access to its instances of the Salesforce Services.

Who is responsible for assuring proper use of the Personal Data?

Customers are responsible for using the Salesforce Services appropriately, including their Processing of Personal Data using the Salesforce Services. Salesforce's Data Processing Addendum provides that Salesforce is responsible for providing the Salesforce Services appropriately and contains a commitment from Salesforce to use the Personal Data only in accordance with Customer's documented instructions for specific purposes, including processing under the Data Processing Addendum, processing initiated by the Customer in using the Salesforce Services, and processing to comply with other instructions provided by the Customer.

How can requests from individual Data Subjects to access or correct their Personal Data be handled?

The Salesforce Services allow Customers to manage the Personal Data they maintain in the Salesforce Service, including in response to Data Subject requests. More details in respect of each Salesforce Service can be found in the Help Documentation, and specifically in the case of Audience Studio (formerly known as DMP) here.

To the extent a Customer needs Salesforce's assistance to respond to a Data Subject, Salesforce will provide assistance as described in its Data Processing Addendum.

Where will Personal Data be stored?

Salesforce's storage locations for Personal Data are described in the Infrastructure and Sub-processors Documentation.

Salesforce has a number of transfer mechanisms in place to support international transfers of Personal Data.

For example, with respect to transfers out of the EU, Salesforce offers three mechanisms to legally transfer Personal Data: (i) Binding Corporate Rules for Processors; (ii) the EU-US and Swiss-US Privacy Shield; and (iii) Standard Contractual Clauses.
For more information about these transfer mechanisms and which Salesforce Services will rely on which mechanism, please see the Salesforce's Data Processing Addendum and our FAQs.

For transfers of Personal Data submitted from the APEC region to Salesforce, regardless of where it is processed once submitted, Salesforce is certified under the Asia-Pacific Economic Cooperation (APEC) Privacy Recognition for Processors (PRP) System.

Describe the information flows for Personal Data for Salesforce Services.

The Salesforce Services are cloud-based platforms, and Customers can allow their users to access the Salesforce Services from virtually anywhere with an internet connection. For these reasons, Personal Data may flow to or from Salesforce from global locations, depending on where the Customer, its users, its consumers/other end users and its website visitors are located.

The locations of Salesforce and its Sub-processors are described in the Infrastructure and Sub-processors Documentation.

How are transfers across national borders accounted for? If a transfer takes place, what is the purpose of this transfer?

Salesforce's Data Processing Addendum, offers multiple transfer mechanisms for all Salesforce Services and includes an "order of precedence" clause in the event one mechanism is not or no longer applicable.

For more information about these transfer mechanisms and which Salesforce Services will rely on which mechanism, please see the Salesforce's Data Processing Addendum and our International Data Transfer FAQs.

The purpose of such a transfer could for example be to allow a Salesforce employee based in the United States providing customer support to a European customer.

How (and with whom) will Personal Data be shared?

Personal Data is shared with Salesforce and, if applicable, its Sub-processors, as described in the Infrastructure and Sub-processors Documentation.

Access by Salesforce and its Sub-processors is subject to the protections in the Data Processing Addendum and Salesforce maintains safeguards to prevent access except (a) to provide the Salesforce Service and prevent or address service or technical problems, (b) as compelled by law, and (c) as the Customer expressly permits in writing.

Which controls does Salesforce have in place with respect to Sub-processors?

As described in the Data Processing Addendum, Salesforce (i) takes responsibility for the actions of its Sub-processors; and (ii) has entered into a written agreements with each Sub-processor containing data protection obligations not less protective than those in our Customer agreements. In addition, all the data transfer mechanisms that Salesforce offers contain comprehensive obligations in respect of 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). 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 Subprocessor using the procedure set out in the Data Processing Addendum.

What contracts are in place to protect Personal Data submitted to the Service?

Protections for Personal Data are described in the Salesforce Customer's contract with Salesforce.

Contractual documents containing protections for Personal Data include (1) a master subscription agreement between Salesforce and the Customer; (the "Master Subscription Agreement" or "MSA") (2) Salesforce's Data Processing Addendum. Note that the SPARC Documentation & I&S Documentation form part of the MSA and DPA and so are also contractual commitments.

How does Salesforce respond to government requests to access Customer Data?

As explained in Salesforce's MSA, Salesforce will disclose Customer Data to a governmental entity only when required to do so by law, in response to a valid compelled disclosure request from a governmental entity.

It is rare for Salesforce to receive a government request for Customer Data. In the unusual circumstances where we do receive such a request, Salesforce follows a robust and comprehensive process whereby the Salesforce Legal Department reviews the request to determine if it is lawful, valid, and enforceable, and we notify our Customer of the request, to the extent permitted by law. Salesforce contractually guarantees to provide such notification in its Master Subscription Agreement available here and, to the extent applicable to the Salesforce Service in question, in its Salesforce Binding Corporate Rules for Processors. To review which Salesforce Services are covered by our Processor Binding Corporate Rules, please see here.

Please also see Salesforce's Principles for Government Requests for Customer Data for more information.

How are breach notifications addressed?

Salesforce has comprehensive procedures in place to notify Customers in the event of a data breach of its systems as managed by its Computer Security Incident Response Team (CSIRT). Salesforce commits contractually in its Data Processing Addendum to notifying Customers

"without undue delay" which is the standard of notification required for processors in accordance with applicable law. Salesforce has a formal Incident Management Process that guides the Salesforce Computer Security Incident Response Team (CSIRT) in investigation, management, communication, and resolution activities.

Salesforce will promptly notify the Customer in the event of any security breach of Salesforce Services resulting in an actual or reasonably suspected unauthorized disclosure of Customer Data. Notification may include phone contact by Salesforce Support, email to the Customer's administrator and Security Contact (if submitted by Customer), and public postings on trust.salesforce.com. Regular updates are provided to engaged parties until issue resolution. Incident tracking and resolution is documented and managed within an internal ticketing system.

Can Personal Data be encrypted?

Please see the Security, Privacy, and Architecture Documentation, for details on Salesforce Service encryption. Most Salesforce Services offer encryption in transit by default and several allow customers to encrypt some data at rest, for example by using Salesforce Shield.

How long is Personal Data retained?

Customers choose how long to retain Customer Data, including Personal Data, on the Salesforce Service. Unless otherwise specified in the Security, Privacy, and Architecture Documentation, Salesforce does not delete Customer Data, including Personal Data, during a subscription term, unless the Customer instructs Salesforce to do so. After a Customer's contract with Salesforce terminates, Salesforce deletes Customer Data, including Personal Data, in the manner described in the Security, Privacy and Architecture Documentation.

How is Personal Data deleted when it is no longer needed?

Unless otherwise specified in the Security, Privacy, and Architecture Documentation, upon request by the Customer, or after termination of a Customer's contract, Salesforce deletes the Customer's Personal Data in the manner described in the Security, Privacy and Architecture Documentation.

How are requests from individuals (or Data Subjects) to have their Personal Data deleted managed?

As described in Salesforce's Data Processing Addendum, Salesforce shall notify a Customer if it receives a request to exercise rights related to the Processing of Personal Data on Salesforce Services. The Salesforce Services provide functionality to enable the Customer to respond to

that request, but Salesforce's Data Processing Addendum also commits to provide reasonable assistance if needed.

More details in respect of each Salesforce Service can be found in the Help Documentation.

Has Salesforce appointed a Data Protection Officer?

Yes. Lindsey Finch is Salesforce's Data Protection Officer. She can be reached at privacy@salesforce.com.

Please provide an overview of how Salesforce incorporates the principles of "privacy by design" into its product development.

Salesforce works to incorporate privacy and data protection concepts from the inception of each new service or feature it offers. Product managers and engineers who design our products are trained at least annually on data protection. In addition, each Salesforce Service is supported by at least one product attorney knowledgeable about data protection and privacy, who reviews and advises on the product's functionality. Additionally, each product attorney is supported by a privacy attorney who specializes in data protection and privacy. The product release cycle also contains multiple checks where additional people can provide comments on the service or feature's protection of Personal Data. Finally, when a service or feature is released, it is described in the product documentation and release notes so that Customers can perform their own evaluations. Salesforce regularly considers input from its Customers when designing and refining product functionality.

Please provide details of how Salesforce is addressing its accountability and governance obligations under data privacy laws.

Salesforce commits to meeting its accountability and governance obligations under applicable law and will take all appropriate related measures. These measures include implementing appropriate technical and organizational security measures (more details available in the Security, Privacy and Architecture Documentation), undertaking privacy impact assessments (where appropriate) and maintaining records of processing, among others. Salesforce has appointed a data protection officer as is required by applicable law.

How does Salesforce audit compliance with data protection controls?

Salesforce's privacy and product lawyers work closely with Salesforce's product developers on Salesforce's 'privacy by design' privacy strategy to ensure that it meets all of our data protection obligations. Before any new service or feature is released (and throughout its development), it goes through a comprehensive privacy review to ensure it can meet Salesforce's rigorous privacy and security programme, as well as the contractual commitments we make to our Customers.

In order to ensure that our privacy commitments remain true over time, Salesforce has a comprehensive range of compliance and internal accountability measures to ensure we protect Personal Data where it is accessed, stored, or processed such as our internal policies and standards and employee training. Our internal audit team continually evaluates the performance of our internal governance, risk management and internal controls and all issues are dealt with in a proactive, timely manner.

Salesforce makes a number of contractual commitments to Customers in the Data Processing Addendum in relation to data protection and privacy controls. This includes sections on (i) data transfer mechanisms and (ii) the Security Privacy and Architecture and Infrastructure and Sub-processing' Documentation.

Salesforce's Processor Binding Corporate Rules require that we undertake an annual audit of our BCR commitments. Our Privacy Shield certification also involves annual internal and external (via TrustArc) reviews. Furthermore, Salesforce regularly performs its own audit of its obligations under the Standard Contractual Clauses to ensure Personal Data can be transferred adequately outside of the EU.

In addition, Salesforce's Sub-processors receive questionnaires that they must complete annually attesting to their privacy and security compliance.

Are Salesforce employees bound by confidentiality obligations?

Yes, Salesforce commits in its Data Processing Addendum to ensure that personnel have been appropriately trained, are reliable and enter into confidentiality agreements. Employees also regularly undergo data protection and privacy training, such as the European Union Privacy Law Basics Trailhead.