UPDATED JUNE 2025

Data Protection Impact Assessments & Salesforce Services

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, and to complete their own data protection impact assessments, should such assessments be required. It does not provide legal advice. We urge Customers to consult with their own legal counsel to familiarize themselves with the requirements that govern their specific situation. More information about data protection impact assessments can be found here.

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 enable Salesforce 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.

In addition, for Agentforce: Agentforce runs within the Einstein Trust Layer, a framework designed to ensure secure and responsible use of AI, which includes a range of specific privacy and security controls that apply to Agentforce. The Einstein Trust Layer features controls like secure data retrieval, dynamic grounding, data masking, prompt defense, toxicity scoring, audit trails and a zero data retention policy with third party LLMs. Further information on the Einstein Trust Layer is available here.

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.

Agentforce maintains several industry-standard attestations—including SOC 2 Type II, ISO 27001, PCI DSS, HIPAA, IRAP, and FedRAMP High—with additional frameworks being added on an ongoing basis. For the complete and most up-to-date list of certifications, please see here for a complete list of certifications.

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 their 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.

It is important to note that while Salesforce provides the platform and tools, the responsibility for complying with data subject rights lies with the Customer as the data controller. They must configure the Salesforce Services - including Agentforce - in a way that aligns with their data privacy obligations and allows them to effectively respond to data subject requests.The Salesforce Services allow Customers to manage the Personal Data they maintain in the Salesforce Services, including in response to data subject requests.

In respect of Agentforce: Agentforce is designed to be integrated with existing Salesforce Services, such as Sales Cloud, Service Cloud and Data Cloud. Agentforce does not store Customer Data so data subject requests must be exercised in respect of the underlying Service in which the Customer Data is stored. 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.

More information about how the Salesforce Services enable Customers to handle data subject rights such as data deletion, consent management, restriction of processing, data access and portability within the Salesforce Services is available in the Help Documentation.

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 Agentforce, this processes Personal Data related to the end-users interacting with AI agents, such as their queries (i.e. prompts), conversations with the agent, and instructions for task completion. The specific types and extent of Personal Data processed will vary based on the Salesforce Customer's specific use cases, the AI agents they build, the data sources they choose to upload to Data Cloud, and the interactions users have with these agents.

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. For Agentforce specifically, please see the Einstein Platform Security, Privacy and Architecture Documentation (SPARC) available here.

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. For Agentforce specifically, please see the Einstein Platform Security, Privacy and Architecture Documentation (SPARC) available here.

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 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 as a controller for its own purposes, the Salesforce Privacy Statement and other privacy-related documentation are publicly available here.

How is access to the Services 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. For Agentforce specifically, please see the Einstein Platform Security, Privacy and Architecture Documentation (SPARC) available here.

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.

Where will Personal Data be stored?

Salesforce's storage locations for Personal Data are described in the Infrastructure and Sub-processors Documentation. For Customers opting for the Hyperforce EU Operating Zone (EUOZ), Salesforce provides customer and technical support within the EU, as well as storage of Customer Data in the EU.

Salesforce has a number of transfer mechanisms and frameworks in place to support international transfers of Personal Data. For example, with respect to transfers out of the EU, UK and Switzerland, Salesforce offers multiple transfer tools and frameworks to facilitate the free flow of personal data around the globe: (i) EU and UK Binding Corporate Rules for Processors (BCRs); (ii) certification to the Data Privacy Framework (DPF), namely the EU-US DPF, UK Extension to the EU-US DPF and Swiss-US DPF; and (iii) Standard Contractual Clauses (SCC).

For more information about these transfer mechanisms, 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. For Customers on the Hyperforce EUOZ, Salesforce provides in-region customer and technical support to meet enhanced EU data residency and privacy commitments and to contain global data flows.

The locations of Salesforce and its Sub-processors are described in the Infrastructure and Sub-processors Documentation. For Agentforce specifically, please see the Einstein Generative AI Services section of 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 tools and frameworks for all Salesforce Services, including Agentforce.

For more information, please see the Salesforce's Data Processing Addendum and our International Data Transfer FAQs.

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.

Agentforce may use third party Large Language Model (LLM) providers to process Personal Data. However, the Einstein Trust Layer and the zero data retention policy ensures that no Customer Data is retained or used for model training by third party model providers. For Agentforce, please see the Einstein Generative AI Services section of the Infrastructure and Sub-processors Documentation.

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 agreement 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.

For Agentforce, Salesforce employs the Einstein Trust Layer which includes a zero data retention policy. This means that any Customer Data is not stored or used to improve third-party LLMs. For more information on the Einstein Trust Layer, please see here.

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 and DPA, 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. Where we do receive such a request, Salesforce follows a robust and comprehensive process which is described in Salesforce's Transparency Report. Every request for Customer Data that Salesforce receives is carefully reviewed, consistent with the laws in the relevant jurisdiction(s), to ensure the requesting public authority is entitled to the data sought with the type of process utilized. Where Salesforce believes a request is invalid or unlawful, it will challenge it.

Salesforce offers its Customers various contractual commitments in its MSA (including its DPA). More precisely, these commitments can be found in (i) section 7 "Confidentiality" of Salesforce's MSA, (ii) section 8 "Government Requests" of Salesforce's DPA, clause 15 of the EU Standard Contractual Clauses and the Salesforce Processor Binding Corporate Rules. Namely, Salesforce commits to (1) notify an affected Customer of any legally binding and valid request for its data, unless Salesforce is explicitly prohibited from doing so by law, (2) try to get any notification restriction waived, (3) refer the requesting public authority to the affected Customer where possible, (4) not to disclose Customer Data to public authorities unless compelled by law, (5) challenge or reject unlawful requests and (6) not to provide any public authority with encryption keys or any other way to break encryption and not to build back doors into our products.

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. For Agentforce specifically, please see the Einstein Platform Security, Privacy and Architecture Documentation (SPARC) available here. 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, which enables Customers to use external key management, “bring your own key,” and cache-only keys. Notably, the external key management capability allows Customers to store and manage encryption keys with local EU providers, thereby further limiting Salesforce’s ability to access Customer Data in the clear.

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. As Agentforce does not store Customer Data, please refer to the retention and deletion rules of the underlying Service per the applicable 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. As Agentforce does not store Customer Data, please refer to the retention and deletion rules of the underlying Service per the applicable 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. Please also see the section on “Data Subject Rights” above.

As Agentforce does not store Customer Data (see above section on Agentforce and data storage / processing), data subject requests must be exercised in respect of the underlying Service in which the Customer Data is stored.

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" and "privacy by default" into its product development.

Salesforce assists Customers in implementing appropriate technical and organizational measures to comply with data protection principles and facilitate compliance with the requirements set up by Salesforce's Processor Binding Corporate Rules in practice, such as 'privacy by design' and 'privacy by default'.

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 and each product attorney is supported by a privacy attorney who specializes in data protection and privacy. Salesforce also has a specialist AI Legal team who provide on-hand expert support and in-depth knowledge on the privacy implications of using both predictive and generative AI. 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.

Salesforce is committed to its compliance with EU laws and operating in accordance with EU values by adhering to the EU's highest trust standards and by championing responsible and ethical AI. This includes the EU Cloud Code of Conduct, of which Salesforce was a founding member and under which Salesforce Services as listed here are verified compliant.

How does Salesforce audit compliance with data protection controls?

While Customers in their controller capacity need to audit their own compliance with data protection controls, Salesforce's privacy and product lawyers work closely with Salesforce's product developers on Salesforce's 'privacy by design' and 'privacy by default' privacy strategy. 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 program, as well as the contractual commitments we make to our Customers.

In addition, Salesforce has a comprehensive range of compliance and internal accountability measures to ensure we protect Personal Data in line with law applicable to Salesforce as a processor and the commitments we make to our Customers, such as internal policies, 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 as well as Salesforce's EU Cloud Code of Conduct require that we undertake an annual audit of our BCR and CoC commitments. Our EU-US Data Privacy Framework (DPF) and its extensions certifications also involve 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, UK and Switzerland.

In addition, Salesforce may conduct Sub-processor audits to ensure compliance with the terms set out in our agreements with those third parties.

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. All employees are required to complete annual Privacy & AI compliance training. Additionally, employees in designated roles must complete annual data-handler training to help ensure they understand the confidential nature of the data they may process and their associated responsibilities. There are also optional privacy trainings available such as the European Union Privacy Law Basics Trailhead.