Salesforce's Agentforce Privacy FAQ
Published: June 2025

This document is provided for informational purposes only. It is not intended to provide legal advice. Salesforce urges its Customers to consult with their own legal counsel to familiarize themselves with the requirements that govern their specific situations. This information is provided as of the date of document publication, and may not account for changes after the date of publication. For further information on our privacy practices, please see other resources on the Privacy website available here.

This document serves as a Customer facing frequently asked questions (FAQ) resource regarding Salesforce's Agentforce offering and its privacy implications. Please note that this FAQ does not apply to Salesforce's Bring-Your-Own LLM offering; for more information, see below.

For the definitions of capitalized terms used in this FAQ, please refer to Salesforce's Data Processing Addendum (DPA).

Table of Contents

What is Agentforce?

When we talk about Agentforce, we're talking about the Salesforce platform for creating, customizing, and deploying autonomous AI agents (Agents). Agentforce enables businesses to build, deploy, and manage Agents to automate tasks and enhance productivity across various functions like sales, service, marketing, and commerce.

Agentforce is built on the Salesforce platform which integrates the Einstein Trust Layer. The Einstein Trust Layer is a set of agreements, security technology, and data and privacy controls used to keep Customers and their data safe while exploring generative AI solutions. For more information, see the Einstein Trust Layer Documentation. Please note that data masking is currently disabled for Agentforce; more information is set out here.

What are Agents?

Agents are goal-oriented, autonomous AI assistants that perform tasks and business interactions. They can initiate and complete a sequence of tasks, handle natural language conversations, and securely provide relevant answers drawn from business data. Some Agent types are best at assisting and collaborating with a Salesforce user in the flow of work. Other types can also act on behalf of a user or Customer, based on the use cases and guardrails that

an admin specifies (in respect of which, see below). For more information, see Agentforce Help Documentation.

How does Agentforce interoperate with other Salesforce Services?

Agentforce is the agentic layer of the deeply unified Salesforce platform and is designed to be integrated with existing Salesforce Services, such as Sales and Service Cloud. In addition, Customers connect Agentforce to their existing Data Cloud org which enables Customers to utilise retrieval-augmented generation (RAG) and ground responses in relevant structured and unstructured data that Customers upload to their Data Cloud org. The concepts of RAG and grounding are explained in more detail below.

Does the information in this FAQ apply when Customers decide to use their own LLM i.e. "bring your own" LLM (BYO LLM)?

The questions in this FAQ do not apply to BYO LLM. By way of background, Salesforce offers Einstein 1 Studio Model Builder in Data Cloud which allows Customers to bring their own Large Language Models (LLM) for use within custom prompt builder templates.

Salesforce Customers can also leverage their own LLM relationships within the Salesforce ecosystem. In that case, the LLM provider they choose to use is a Non-SFDC Application (not a SFDC Sub-processor) and the Customer is required to comply with its own contract with the LLM provider. More information on BYO LLM is available in Salesforce's Bring Your Own Large Language Model in Einstein 1 Studio blogpost.

Personal Data Processed by Agentforce

Does Agentforce process Personal Data?
As with all Salesforce Services, the scope of Personal Data processed by Agentforce is determined by the Customer. It depends on the Personal Data that Customers choose to upload or submit to the Services, as well as the particular use case.

Some examples of data that Customers may upload or submit to the Services and process using Agentforce include Personal Data disclosed by users during the course of conversations with the Agent and any Personal Data uploaded to Data Cloud for the purpose of grounding Agent responses. We have explained grounding in more detail below.

Agentforce & Salesforce's Data Processing Addendum

Is Agentforce covered by Salesforce's Data Processing Addendum (DPA)?
Yes, anything branded as Agentforce, as listed in the Einstein Platform Security, Privacy and Architecture (SPARC) Documentation (including Agentforce Assistant, Agentforce SDR, Agentforce Sales Coach and Agentforce Service Agent), is covered by the definition of Services in Salesforce's Main Services Agreement (MSA) which incorporates Salesforce's DPA.

Agentforce & Sub-processors

Where can I find details of the Sub-processors that Agentforce uses?
The list of the Sub-processors used by Agentforce is available in the Einstein Generative AI Services section of Salesforce's Infrastructure and Sub-processors Documentation applicable to the relevant Service.

Agentforce and Third-Party LLMs

Does Agentforce use third-party LLMs?
Yes, Salesforce uses a number of third-party LLMs as part of Agentforce. Salesforce has a zero data retention policy in place which ensures any third-party LLMs used by Salesforce do not retain Customer Data or use it for model training.

Why is OpenAI the only third-party LLM listed in the Infrastructure & Sub-processors Documentation?
There are many ways that Salesforce works with third-party LLMs as part of Agentforce. In some cases e.g. OpenAI, Customer Data is sent to OpenAI directly and OpenAI is Salesforce's Sub-processor. In other cases, such as Anthropic which is hosted on AWS and OpenAI which is hosted on Microsoft Azure, the models are out-of-the-box and hosted on third-party infrastructure. As Customer Data is not sent to OpenAI or Anthropic in these scenarios, but to the hosting provider, the hosting provider is Salesforce's Sub-processor.

In all of these scenarios, Salesforce has a zero data retention policy in place which ensures any third-party LLMs used by Salesforce do not retain Customer Data nor use it for model training.

More information on Sub-processors can be found in the Einstein Generative AI Services section of the Infrastructure & Subprocessors Documentation. Customers who would like information on which third-party LLM is used by their specific implementation of Agentforce should contact their Account Executive.

Does Salesforce have Data Processing Agreements in place with third-party LLMs?
Yes, Salesforce has data processing agreements in place with third-party LLMs that are Sub-processors which contain obligations that are no less protective than those Salesforce puts in place with its Customers. Where LLMs are hosted by third parties (e.g. Anthropic on AWS or Open AI on Azure), Customer Data is not sent to the LLM provider but to the hosting provider; in this case, Salesforce has data processing agreements in place with the applicable hosting provider.

Agentforce and Data Storage

Is Customer Data stored in Agentforce?

Customer Data is not stored in Agentforce. Agentforce is the agentic layer of the Salesforce platform and is integrated with underlying Salesforce Services, such as Sales and Service Cloud. Customers also have the option to integrate Agentforce with Data Cloud and upload structured and unstructured data to Data Cloud which can be used for RAG and grounding. Therefore, whilst Agentforce processes Customer Data, any Customer Data is stored in the underlying Salesforce Services.

What are the data retention and deletion rules applicable to Agentforce?
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.

Do third-party LLMs retain Customer Data?
Salesforce operates a zero data retention policy which ensures that the third-party LLM providers it currently uses do not retain Customer Data (including any Personal Data contained in Customer Data) nor use it to train or improve their models.

Agentforce and Model Training

Is Customer Data used to train generative AI models?
Salesforce operates a zero data retention policy which ensures no Customer Data is retained or used for model training by third-party LLMs.

In addition, Salesforce does not currently use Customer Data to train generative AI models. To the extent that Salesforce decides to train generative AI models on Customer Data in the future, the Product Terms (available in the Product Terms Directory) applicable to products that a Customer may have purchased on an Order Form expressly require Customers to opt-in to such training. For more information on our Product Terms, please see the Product Terms Directory where Customers can search the applicable terms based on the Services on their Order Form(s). For additional information, Customers may contact their account executive.

Agentforce & Data Transfer Mechanisms

How does Salesforce legalize transfers of Personal Data for Customers using Agentforce?
Salesforce has a robust privacy program that meets the highest standards in the industry and, as part of that program, we offer Customers various transfer tools and frameworks, including in respect of Agentforce, to facilitate the free flow of Personal Data globally.

These include: (i) EU and UK Binding Corporate Rules ("BCRs") for processors; (ii) Standard Contractual Clauses; (iii) certification to the Data Privacy Frameworks (EU-US, Swiss-US, and UK Extension), and (iv) the APEC Privacy Framework (CBPRs and PRPs), together with robust supplementary measures where required. Details on these transfer mechanisms are available in Salesforce's Data Transfer Mechanisms FAQ.

Is Agentforce covered by the SCCs?
Yes. All Salesforce Services - including Agentforce - are covered by the EU Standard Contractual Clauses (SCC) incorporated in our DPA (see above).

Is Agentforce covered by the BCRs?
Yes, see above. Agentforce is expressly listed in Appendix A - Services to which the Salesforce Processor BCR apply.

Agentforce & Data Subject Rights

How can Customers fulfil data subject rights in respect of Agentforce?
As Agentforce does not store Customer Data (see above section on Agentforce and Data Storage), data subject requests must be exercised in respect of the underlying Service in which the Customer Data is stored. For more information on fulfilling data subject rights, please see Salesforce's Data Protection and Privacy Documentation.

Agentforce & Security

What technical and organizational security measures does Salesforce offer in respect of Agentforce?
Trust and customer success are core values for Salesforce. Providing a robust security and privacy program that carefully considers data protection matters across Salesforce Services, including Agentforce is critical to both.

The Einstein Platform Security, Privacy and Architecture (SPARC) describes Agentforce's security- and privacy-related audits and certifications, and applicable administrative, technical, and physical controls.

In addition to the information set out in the SPARC, Agentforce uses the Einstein Trust Layer. The Einstein Trust Layer includes a range of additional built-in privacy and security controls that apply to Agentforce, like bias detection, prompt scrutiny, secure data retrieval, and auditing features. Please note that data masking is currently disabled for Agentforce to improve performance and accuracy of agents. Further information is available in the Data Masking in Agentforce Documentation.

The Einstein Trust Layer ensures that features such as dynamic grounding and policies such as zero data retention apply when Customers use Agentforce (see "Agentforce & Data Retention" and "Agentforce & Privacy by Design" below.) Further information is available in the Einstein Trust Layer Documentation.

Are there any Agentforce specific security certifications?
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.

Agentforce & Privacy by Design

How can Customers use Agentforce to demonstrate privacy by design?
Agentforce can be used by Customers to demonstrate privacy by design. For example:

- **Transparency:** Agents can be configured to present an organization's privacy statement to individuals at the first point of contact, provide "just-in-time" notices if at any point further Personal Data is collected from individuals, and provide up-to-date and relevant information on how to exercise data subject rights on request. Agents could also be configured to help consumers better understand a company's privacy policies by creating a conversational interface for them to ask questions, demystifying complex legal jargon, and fostering transparency with the brand.

In addition, although Customer assumes all responsibility for Agent output, Agentforce has certain features which facilitate compliance with data minimisation and accuracy:

- **Data minimisation:** Agentforce uses retrieval-augmented generation (RAG) to help assist Customers with data minimisation. RAG is a feature that allows for relevant, contextual and customer-specific agent responses without the need to use Customer Data to train generative AI models. It gives LLMs the ability to retrieve information from a knowledge base or other data sources and incorporate that information into the responses they generate, rather than relying solely on the data on which the LLM was trained. To use RAG effectively, Customers must upload their most relevant and up-to-date structured and unstructured data to Data Cloud. By following this process, Customers can also ensure that Agents are producing outputs that contain and are grounded only on necessary information.
- **Accuracy:** RAG helps Customers ensure that Agent responses are accurate. Customers can select both structured and unstructured data sources to upload to Data Cloud which ensures that off-the-shelf LLMs which are trained on data which may not be specific to Customer's business are able to ground the output in up-to-date information reflecting Customer's evolving business practices.

Please find more information on this topic in our blogpost AI Agents Will Enhance — Not Impair — Privacy. Here's How.

Where can Customers find materials to help with an Agentforce data protection impact assessment (DPIA)?
Should Customers wish - depending on their use case - to complete a DPIA on Agentforce, Salesforce makes a DPIA covering all Salesforce Services, including Agentforce, available here.

Agentforce and Automated Decision-Making

Are all Agents fully autonomous?
Salesforce provides its Services in accordance with Customer instructions. Customers determine how Agentforce is used and implemented and different Agents allow for different levels of autonomy.

Customers can also configure Agent “guardrails” to ensure that Agents can only deal with specific topics. For example, Customers can define the conditions under which an Agent refers or “escalates” a conversation to a human agent, as further set out here. When Customers assign topics to an Agent, they also specify the instructions an Agent can follow and the actions an Agent can take in relation to that topic. By defining topics, actions and instructions, Customers narrow down the actions and data relevant to a given use case, set the context and define how their Agent behaves. For more information on topics, actions and instructions, please see Agent Topics.