Financial Services and Data Protection FAQ

Frequently Asked Questions (FAQs)

Overview

This document is provided to assist in answering questions raised by customers when evaluating Salesforce’s online services. This document is a broad overview of Salesforce services that may or may not apply to a customer’s use cases. This document is not legal advice. Salesforce urges its customers to consult with their own counsel to familiarize themselves with the supervisory and data security requirements that govern their specific situations. This information is provided as of the date of document publication, and may not account for service changes after the date of publication.

What does Salesforce offer?

Salesforce is the leading provider of enterprise cloud computing technologies. ‘Cloud computing’ is a broad term but generally denotes a range of IT services provided in various formats through social, mobile and open technologies.

Salesforce enables companies to place their customers at the heart of their business and engage with them in new and powerful ways. Salesforce services include customer relationship management (CRM), collaboration, and social media monitoring for businesses of all sizes. Salesforce also provides platforms to build and run business applications without having to invest in new software, hardware, or related infrastructure. More information on the types of products and services that Salesforce offers can be found on the Salesforce website.

How does Salesforce deliver its services?

Salesforce generally delivers its services via the Internet. Customers log into Salesforce’s services through a website using unique usernames and passwords. Salesforce’s services allow for various additional authentication methods that may be activated by customers, as appropriate to their needs, such as two-factor authentication and IP range restrictions. We also serve our customers through what is known in the industry as cloud-based services architecture, which is designed for security, efficiency, availability, scalability, and rapid innovation.
How can Salesforce help with contractual compliance?

Salesforce offers its customers a comprehensive security and privacy framework underpinned by its Data Processing Addendum (‘DPA’). Salesforce maintains appropriate technical and organizational measures to protect Customer Data (as defined in the DPA), as set forth in the applicable Security Privacy and Architecture Documentation available here (select relevant service).

How does Salesforce support customer due diligence and ongoing review?

Salesforce is committed to supporting customer diligence by offering customers a strong compliance framework and advanced tools and security measures that may allow customers to evaluate, meet, and demonstrate compliance with applicable legal and regulatory requirements.

Conducting due diligence and ongoing review involves gaining a clear understanding of Salesforce technology and its underlying architecture. Salesforce offers its customers audit rights as well as third party certifications and audit reports in the DPA. In addition to the information and resources linked to in this FAQs (including under “Security” below), additional resources and consultation may be available upon discussion with your Account Executive. Salesforce will not interpret regulations for your particular circumstances, or interact directly with your regulator on your behalf.

How does Salesforce secure Customer Data?

Salesforce has implemented an array of technical and administrative security measures to help protect our services and Customer Data. Salesforce’s technical security measures include protections against system vulnerabilities, logical separation of Customer Data, robust network security, encryption of data in transmission, and options for encryption of data at rest. Salesforce’s administrative security measures include limiting access to Customer Data to those personnel who require such access to perform their current job functions (see “Data use limitation” below), comprehensive security policies regarding the handling of Customer Data, and robust security training and awareness programs.

Salesforce offers its customers controllable features that permit them to configure the security settings of their respective instances of the Salesforce services as individual customers deem appropriate for the sensitivity of their Customer Data.

Where can a customer get details of Salesforce’s security controls?

Specific security controls to protect Customer Data are set out in the applicable SPARC Documentation available here by selecting the relevant service.

Please also see Salesforce’s:

- Compliance website detailing our compliance certifications and attestations
- Salesforce Security Guide, detailing customer-controllable security features of Salesforce services (including encryption)
- Security Compliance Documentation Portal
- Help & Training Portal
- Security page
For Service availability, please see the Salesforce Trust website, which displays real-time information about service availability and performance.

Security Health Check: This standard Salesforce feature analyzes your Salesforce org’s security settings against a default or custom baseline. It provides a score and specific recommendations. Create your own compliance-specific baseline. Refer to the Help & Training article titled Security Health Check for additional information.

Where does Salesforce store data submitted by customers?

Salesforce hosts Salesforce’s services in a number of data centers. Up-to-date information about the hosting locations for each service that Salesforce offers can be found in the applicable Infrastructure and Sub-processor Documentation available here by selecting the relevant service.

Does Salesforce use third-party service providers to provide services to customers?

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 for reasons like providing customer support and ensuring the services are working properly. As described in our contracts, Salesforce takes responsibility for the actions of its Sub-processors.

Up-to-date information about the hosting locations for each service that Salesforce offers and the 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.

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.

Under what circumstances does Salesforce access or use data submitted by customers?

Salesforce provides contractual assurance to its customers that the data customers submit to Salesforce’s services will be kept confidential and not accessed by Salesforce except under narrow circumstances. As set out in the DPA, Salesforce processes Customer Data on behalf of customers and only in accordance with their documented instructions for limited purposes: (i) processing under the Agreement; (ii) processing initiated by customer users in using the Services; and (iii) processing to comply with other customer instructions.

How does Salesforce segregate one customer’s data from the data of other customers in its environment?

Salesforce serves its customers through what is known as “multi-tenant” application architecture, designed for security, efficiency, availability, and rapid innovation. A multi-tenant application is one that can be accessed and used by many users simultaneously, with logical separation of data in hardware and
software. The logical separation of data allows each Salesforce customer to view only their “instance” of Salesforce’s services and their associated data. Salesforce’s multi-tenant architecture is analogous to that used to provide online banking and brokerage services (which can also be accessed and used by thousands of users simultaneously through the logical – not physical – separation of data).

**Does Salesforce have business continuity and disaster recovery plans?**

Salesforce has a formally documented global Business Continuity and Disaster Recovery Program. Salesforce has Certified Business Continuity Planners on staff and has retained the services of leading consultants to assist in the ongoing development of Business Continuity and Disaster Recovery plans and procedures. This program is overseen by senior management for each of the key functional areas within Salesforce, and is supported by executive leadership at the highest level. A summary of the Salesforce Business Continuity Plan can be found in the applicable SPARC Documentation available [here](#) by selecting the relevant service.

**How and when will Salesforce return data upon termination of the service agreement?**

Salesforce’s customers always have access to their data. In addition, at the end of the agreement, Salesforce returns data to its customers as per the contractual commitments set forth in the applicable SPARC Documentation. Information about the return and deletion of Customer Data can be found in the SPARC Documentation available [here](#) by selecting the relevant service.

**Where can information about Salesforce’s privacy program be found?**

See Salesforce’s Privacy website [here](#).

This site includes helpful information on topics such as Salesforce’s DPA, data transfer mechanisms and our EU General Data Protection Regulation resources which also include documentation to support a customer’s Data Protection Impact Assessments.