Japan Financial Services and Data Protection FAQ
Questions and Answers for Salesforce Customers

Published: September 2020

This document is provided to assist in answering questions raised by customers when evaluating Salesforce's online services. This document is not legal advice. Salesforce urges its customers to consult with their own counsel to familiarize themselves with the supervisory and data protection 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.

Defined/capitalised terms are included in the table at the end of this FAQ.

Nothing is more important than the trusted relationship between Salesforce, its customers, and everyone in the Salesforce ecosystem. Salesforce earns the trust of its stakeholders through transparency, security, privacy, compliance and performance. We are trusted advisors, and we deliver the most trusted infrastructure in the industry.

Trust.Salesforce.com is the Salesforce community's home for real-time information on system availability, performance, security and compliance. Having trust at the foundation of our culture is how we maintain our pace of innovation and deep customer and stakeholder relationships at scale.

Salesforce is committed to supporting our customers on their financial services compliance journeys and we have created this FAQ in support of that effort. We recognise that each of our customers will have differing compliance requirements depending on the characteristics of their specific financial institution, their particular business model, and the way in which they use our services.

We encourage our customers to evaluate how their use of our services, given our comprehensive security and privacy program, contractual commitments, and the controls available within our services, enable them to meet, and demonstrate compliance with applicable rules and regulations. We also engage with regulators to better understand sectoral rules and regulations, which allows Salesforce to build solutions and develop features to better support our customers' independent compliance efforts.

You can see here how our services have successfully been used by some of the largest financial institutions across the globe.

WHAT DOES SALESFORCE OFFER?

Salesforce is one of the leading providers 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, blockchain and open technologies. Salesforce operates as a SaaS and PaaS provider of cloud services.

Salesforce is the #1 customer relationship management solution allowing companies to connect to their customers in a whole new way. It's single integrated platform gives all your departments — including marketing, sales, commerce, and service — a single, shared view of every customer, made smarter by the use of artificial intelligence. The Salesforce platform also allows companies to build and run business applications without having to invest in new software, hardware, or related infrastructure. More information about the services that Salesforce offers can be found on the Salesforce website.

COUNTRY SPECIFIC RULES AND REGULATIONS FOR JAPAN

1. Can financial institutions use Salesforce?

Yes. Financial institutions are permitted to use cloud services in Japan, provided they comply with applicable rules and regulations, such as those described below.

2. Who is the financial regulator?

The Financial Services Agency of Japan (the "JFSA") is the major regulator.

3. What rules and regulations could apply to financial institutions using Salesforce?

The use of Salesforce cloud services by a financial institution would amount to outsourcing insofar as any Salesforce cloud services are a service that would otherwise be undertaken by the financial institution itself.

There is no unified single outsourcing rule which applies to all financial institutions. The specific rules applicable to outsourcing vary depending on the type of regulated business/financial institution.

Mandatory law:

Banks

· Article 12-2, Paragraph 2 of the Banking Act

· Article 13-6-5 and Article 13-6-8, Paragraph 1 of the Ordinance for Enforcement of the Banking Act

Insurance Companies

· Article 100-2 of the Insurance Business Act

· Article 53-8 and Article 53-11 of the Ordinance for Enforcement of the Insurance Business Act

Trust Business Operators

· Article 22 of the Trust Business Act

· Article 40, Paragraph 6 of the Regulation for Enforcement of the Trust Business Act

Fund Transfer Service Providers (FTSPs)

· Article 50 of the Payment Services Act

· Article 27 of the Cabinet Office Order on FTSPs

Crypto-assets Exchange Service Providers (CESPs)

· Article 63-9 of the Payment Services Act

· Article 13 of the Cabinet Office Order on VCESPs

Money Lending Business Operators (MLBOs)

· Article 10-2 and 10-5 of the Ordinance for Enforcement of the Money Lending Business Act

JFSA Guidance:

· III-3-3-4 of the Comprehensive Guidelines for Supervision of Major Banks, etc. (the "Banking Guidelines")

· II-4-5-2 and II-5-1-2 of the Comprehensive Guidelines for Supervision of Insurance Companies, etc. (the "Insurance Business Guidelines")

· III-4-5, III-5-4 and III-5-5(4) of the Comprehensive Guidelines for Supervision of TBOs, etc. (the "Trust Business Guidelines")

· I-2-3-3-1 of the Administrative Guidelines No.3 (for FTSPs) (the "FTSP Guidelines")

· II-2-3-3-2 of the Administrative Guidelines No.3 (for CESPs) (the "CESP Guidelines")

· II-2-3 of the Comprehensive Guidelines for Supervision of MLBOs (the "MLBO Guidelines")

· III-2-4 and III-2-7 (2) of the Comprehensive Guidelines for FIBOs, etc. (the "FIBO Guidelines")

· Policy towards strengthening Cybersecurity in the Financial field

FISC Guidance:

The guidelines/standards published by Financial Industry Information System (FISC) can be voluntarily observed, including among others:

"Safety Measures Standards/commentary for Computer Systems of Financial Institutions"

4. What are the key data privacy considerations for financial institutions using Salesforce?

See the Regional Privacy Laws section of our privacy website, which includes information and tools to help enable our customer's success.

KEY RESOURCES

1. Security

How does Salesforce secure Customer Data?

We strongly encourage customers to follow security best practices and use available tools to strengthen the security of their Salesforce instance. Security does not start and end with Salesforce -- it is a trusted partnership with our customers.

As set forth in more detail in our SPARC Documentation, Salesforce has implemented technical and administrative security measures designed to 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, 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.

For more information on the application security features Salesforce provides, please refer to this help article on Protecting Your Salesforce Organization.

Where can a customer get details of Salesforce's security and compliance controls?

- Salesforce's Compliance website details our audit/compliance certifications and attestations, e.g. ISO and SOC. This compliance website can be filtered by country and industry.
- Salesforce offers its customers a comprehensive security and privacy framework which is contractually underpinned by the Salesforce DPA. In our DPA, Salesforce contractually commits to maintain appropriate technical and organizational measures designed to protect Customer Data, as set forth in the applicable SPARC Documentation, available here by selecting the relevant service.
- The Salesforce Security Guide details customer-controllable security features of Salesforce services (including encryption)
- Our trust.salesforce.com website shows real-time information on system performance and security.
- The Salesforce Shield for Financial Services white paper contains further information on additional security measures such as encryption of data, monitoring and access controls.
- The External Security Assessments in the Trust and Compliance Documentation contain attestations of penetration tests and security assessments performed by third parties for certain Salesforce services.
- 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. Refer to the Help and Training article titled Security Health Check for additional information.

- Additional resources can be found on the Help and Training Portal and Security page.

Under what circumstances does Salesforce access or use Customer Data

Salesforce provides contractual assurance to its customers that Salesforce has measures in place designed to maintain the confidentiality of Customer Data and to prevent access to that data by Salesforce, except under specified 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 customer's agreement with Salesforce for the purchase of online services; (ii) processing initiated by customers' users in using Salesforce's 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 is designed to allow 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).

How does Salesforce handle Customer Data incidents?

Customer Data incident, management and notification is addressed at Section 7 of the DPA.

2. Due diligence, ongoing review and audit

How does Salesforce support customer due diligence, ongoing review and audit?

Salesforce is committed to offering customers a strong compliance framework and advanced tools and security measures. When conducting due diligence and ongoing review, customers should gain a clear understanding of Salesforce's technology and its underlying architecture, and then evaluate how, using Salesforce's framework, tools and measures, customers may meet and demonstrate compliance with applicable rules and regulations. The following resources can support customers in this regard:

- Salesforce offers its customers audit rights in the DPA and SPARC Documentation.
- Salesforce's Compliance website details our compliance certifications and attestations. Also, our trust.salesforce.com website shows real-time information on system availability and performance.
- Additional resources and consultation may be available upon discussion with your Account Executive. Please note, Salesforce cannot provide legal advice and will not interpret regulations for customers' own particular circumstances.
- Further corporate information about Salesforce can be found in the company overview, as well as the "About Us" section on the Salesforce website.

Where can information about Salesforce's compliance programs be found?

Please see Salesforce's Compliance Center website detailing our audit/compliance certifications and attestations, e.g., ISO and SOC. This compliance website can be filtered on a country and industry basis.

3. Data location and subcontractors

Where does Salesforce store Customer Data?

Salesforce operates its services and stores Customer Data in a number of locations. Up-to-date information about the storage 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 DPA, Salesforce is liable for the acts and omissions of its Sub-processors and has entered into a written agreement with each Sub-processor containing data protection obligations not less protective than those in the DPA with respect to the protection of Customer Data.

Up-to-date information about the identity and the location 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 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.

4. Business continuity and disaster recovery

Does Salesforce have business continuity and disaster recovery plans?

Salesforce has a formally documented global business continuity and disaster recovery program. As part of this, Salesforce has staff who are certified business continuity planners and Salesforce employs 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 (as well as information about data replication, reliability and disaster recovery) can be found in the applicable SPARC Documentation available here by selecting the relevant service.

Salesforce maintains a disaster recovery plan that supports a robust business continuity strategy for the production services and platforms as described on the Disaster Recovery and BCP website.

5. Termination

How and when will Salesforce return Customer Data upon termination of the service agreement?

Salesforce's customers own their Customer Data and the services are designed to always give customers access to it. In addition, at the end of the agreement, Salesforce returns Customer Data to its customers as per the contractual commitments set forth in the applicable agreement and 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.

6. Privacy

Where can information about Salesforce's privacy programme be found?

The protection of our customers' data is paramount, and Salesforce is committed to helping our customers on their global compliance journeys in our role as trusted advisor. Our customers trust us to help them build meaningful relationships with their own customers, and Salesforce's top priority is the security and privacy of the data that we are entrusted to protect.

We have five privacy principles that highlight our commitment and focus on trust: customer control, security, transparency, compliance and partnership. Our privacy website includes global privacy information, resources and tools (such as Salesforce's DPA, International Data Transfers FAQ and documentation to support data protection impact assessments) to help enable our customers' success.

7. Government access to Customer Data

How does Salesforce handle government requests for access to Customer Data, also known as compelled disclosure requests?

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

8. What if I have further questions?

We continue to make your success our top priority. If you have any questions, please contact your Account Executive. Salesforce has invested in a dedicated team, the 'Financial Institutions Resource Support Team' ("**FIRST**") which comprises subject-matter experts from Salesforce's Privacy, Legal, Security, Government Affairs, Technology Compliance, Product and Financial Industries Team, who can help support adoption of Salesforce's services in this regulated landscape.

Defined terms

Customer Data	Electronic data and information submitted by or for a customer to the Salesforce services, as defined in the DPA
DPA	Salesforce's Data Processing Addendum, which forms part of the Master Subscription Agreement or other written or electronic agreement between Salesforce and each of its customers for the purchase of online services
financial institution	The entity (bank, broker-dealer, insurer and fund manager) to which the financial rules and regulations apply
FAQ	Frequently asked questions
PaaS	Platform as a Service
rules and regulations	Any applicable rules, legal requirements, guidance, or similar
SaaS	Software as a Service
SPARC Documentation	Security, Privacy and Architecture documentation
Sub-processor	Any processor engaged by Salesforce or a member of the Salesforce Group (this can include affiliates of Salesforce as well as third party organizations) that may have access to Personal Data (as defined in the DPA).