JAPAN PRIVACY LAWS - FREQUENTLY ASKED QUESTIONS
July 2024

This document is provided for informational purposes. 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.

At Salesforce, trust is our #1 value, which makes the protection of our customers' data paramount. We know that many organizations in Japan have questions about their obligations under the Act on the Protection of Personal Information ("**APPI**"). To help you better understand how the APPI applies to your organization and its potential use of Salesforce's online services, we have outlined below the most commonly asked questions.

1. The Act on the Protection of Personal Information

a. What is the APPI?

The APPI was first enacted in 2003 and came into force in 2005. It has been amended a few times, most recently in April 2022. This most recent amendment was made to generally align more closely with other global privacy laws, such as the European Union's General Data Protection Regulation ("**GDPR**"). In 2019, Japan and the EU deemed one another's laws to be "adequate", meaning that the legal protections to individuals were essentially equivalent to each other. These adequacy decisions allow for the free flow of personal data between these jurisdictions. Japan has also recognized the United Kingdom as being an adequate jurisdiction. Additional information about the current APPI can be found below.

b. What are the main provisions of the APPI?

The APPI addresses a number of significant areas:

1. Establishment of the Personal Information Protection Commission (Art.59(1))

The APPI establishes the Personal Information Protection Commission ("**PPC**") as the governmental organization in charge of enforcing and providing guidance on the APPI. The PPC aims to provide one-stop service relating to the protection of personal information, although it still delegates its power to other authorities in particular cases, especially in special industrial sectors such as the medical, financial, and telecommunication industries. The PPC has issued implementation rules, and guidelines based upon the APPI ("**Guidelines**").

2. Definition of Personal Information (Art.2(1))

Personal information is defined as information about living individuals, where such information is capable of identifying the individual, whether by name, date of birth or other characteristics contained in the data.

3. Special care-required personal information (Sensitive personal information) (Art.2(3))

In most cases, a business operator is prohibited from obtaining sensitive personal information such as race, religion or medical history without the prior consent of the individual to whom personal information relates.

4. Definition of Pseudonymized Information (Art.2(5))

Pseudonymized Information is defined as information regarding a living person which is produced from processing personal information in a manner so that it cannot identify a specific individual unless combined with other information.

5. Definition of Anonymized Information (Art.2(6))

Pseudonymized Information is defined as information regarding a living person which is produced from processing personal information in a manner so that it is not possible to identify a specific individual.

6. Definition of Personally Referrable Information (Art.2(7))

Personally Referrable Information is defined as information relating to a living person which does not fall under personal information, pseudonymized information or anonymized information.

7. Definition of Retained Personal Data (Art.16(4))

Retained personal data is defined as personal data that a business operator has the authority to disclose; correct, add or delete; cease the use of or erase; or suspend its provision to a third party.

8. Purpose of use (Art.17, 18, 21)

A business operator should ordinarily handle personal information only for the purposes disclosed to the data subject. If the business operator wishes to use personal information in a different way, it is generally required to obtain consent from the data subject for that additional processing.

9. Penalty for the misuse of personal information (Chapter 7)

Misuse or theft of personal information by individuals who are involved in the handling of personal information may be subject to criminal penalties.

10. Transfer of personal data to and from third parties (Art.27, 30)

Business operators generally must obtain consent from a data subject to transfer personal data to third parties unless an exception applies, such as an “entrustment” of personal data to a data processor. If a business operator transfers personal data to a third party subject to an opt-out arrangement, prior notification to the PPC is necessary. Opt-out arrangements cannot be used to transfer Special care-required information.

A business operator that receives personal data from a third party generally must confirm how the personal data was obtained and retain a record related to the transfer for a certain period.

11. Limitation on cross-border transfer of personal data (Art.28)

When transferring personal data to a third party located outside of Japan (excluding the countries in the EEA and the UK) a business operator is generally required to obtain additional specific consent of the data subject unless such cross-border transfer meets certain exemptions in accordance with the APPI. Nevertheless, consent is not required in some circumstances, as further described below in “Does the APPI permit the cross-border transfer of personal data?”.

c. What are “business operators”, what are "service providers", and when are they subject to the APPI?

The APPI regulates "business operators" (i.e., private businesses) that use personal data databases for their business purposes.

When a business operator entrusts a service provider (referred to in the Guidelines as a "Trustee") to handle personal data on its behalf, Article 22 of the APPI requires that the business operator exercises "necessary and appropriate supervision" over the service provider to ensure the security of such data. The level of supervision required is not specified in the APPI, but according to the Guidelines, this requires the business operator to select appropriate service providers, enter a contract which contains the service provider's security obligations, and monitor the manner of data handling by the service provider.

Between Salesforce and its customers, the customers are business operators and Salesforce is a service provider of the customer. Salesforce’s customer contract contains robust security obligations, and Salesforce offers its customers multiple methods to monitor its data handling, including functionality in the user interface; its public Trust website; and numerous third-party audits and certifications as described in Salesforce’s Trust and Compliance Documentation, among others.

d. Does the APPI permit the cross-border transfer of personal data?

Yes. The APPI permits the cross-border transfer of personal data if certain requirements are met. If a business operator transfers personal data to a third-party located outside of Japan, the business operator will generally be required to obtain data subjects' prior consent for this transfer unless one of the following exemptions apply:

(i) the transfer is to a country that the PPC regards as “adequate”, meaning that the data protection laws and regulations are equivalent to the APPI. As previously noted, adequate jurisdictions are currently limited to European Economic Area member states and the United Kingdom;

(ii) the transfer is to a recipient that has put into place a personal data handling system

that complies with the standards necessary for continuous implementation of measures equivalent to those required under the APPI ("**Continuous Implementation System**"); or

(iii) the transfer is to a recipient certified based upon an international framework ("**Certification**") regarding the handling of personal data. Under the Guidelines, the only acceptable international framework is the APEC Privacy Framework's Cross Border Privacy Rules ("**CBPR**") System.

e. How does Salesforce help customers comply with the APPI cross-border transfer requirements?

Salesforce has been certified under both the APEC CBPR system and the APEC Privacy Framework's Privacy Recognition for Processors ("**PRP**") System. These certifications enable customers to rely on the Certification exemption set out in clause (iii) above. For more information on our APEC CBPR and PRP certifications, please see our APEC CBPR and PRP FAQ here.

Salesforce also complies with multiple international frameworks regarding the processing and handling of personal data. It has also implemented Binding Corporate Rules, approved by EU data protection authorities, being the "gold standard" of European data transfer mechanisms.

In addition, Salesforce offers customers robust contractual, organizational and technical measures which also demonstrate a Continuous Implementation System for the processing of personal data outside of Japan. As such, customers can look to and rely on both the Certification and the Continuous Implementation System exemptions from the APPI consent requirement for the cross-border transfer of personal data. See also "How does Salesforce comply with applicable requirements regarding cross-border transfer of Personal Information under the APPI?" and "How does Salesforce help customers pursue compliance with the APPI's cross-border transfer limitations in their use of Salesforce's Services?" below.

f. What disclosure obligations does the APPI create for cross-border transfers of personal data?

If a customer is relying on the Continuous Implementation System exemption described above, the customer must, upon request, provide a data subject with a description of the actions the company has taken to implement a Continuous Implementation System in connection with personal data transferred offshore. The rules issued by the PPC sets out a number of items which must be disclosed to data subjects, without undue delay, in connection with such a request. These items include a description of how the Continuous Implementation System was established, details about the measures implemented and information regarding the offshore jurisdictions. Similar disclosure obligations are also required where a customer is relying on the

Certification exemption.

To respond promptly to any such disclosure requests, customers should consider preparing documentation which sets out the required items as it applies to these offshore transfers of personal data. In order to assist customers in preparing such documentation, as it applies to the use of Salesforce Services, customers can look to Salesforce's Trust and Compliance Documentation. In addition, Salesforce has other template resources available to help customers' meet these disclosure obligations. Our account executives can make those resources available to customers upon request.

2. General

a. Does Salesforce transfer Customer Data outside of Japan?

Salesforce may entrust Salesforce affiliates or third-party service providers to process personal data on behalf of customers (each a "Sub-processor") in connection with the provision of the services. This may entail storage and/or processing of customer data outside of Japan. Such storage and/or processing could be considered as cross-border transfer of personal data.

b. How does Salesforce comply with applicable requirements regarding cross-border transfer of Personal Information under the APPI?

Salesforce has implemented procedures designed to ensure that personal data is processed only as instructed by the customer, throughout the entire chain of processing activities by Salesforce and its Sub-processors. In particular, Salesforce and its affiliates have entered into agreements with their Sub-processors containing privacy, data protection and data security obligations that provide a level of protection appropriate to their processing activities.

c. How does Salesforce help customers pursue compliance with the APPI's cross-border transfer limitations in their use of Salesforce's services?

Salesforce has designed its services and contractual terms to enable customers to exercise an appropriate level of supervision over Salesforce and its Sub-processors. These agreements include the terms of Salesforce's Main Services Agreement (formerly known as the Master Subscription Agreement) which incorporate the documentation applicable to the specific services purchased by the customer. In addition, should a customer desire additional terms, Salesforce makes available to its customers a Data Processing Addendum that is tailored to enable its customer to meet applicable requirements of privacy laws, including the APPI.

d. Where can I find additional legal documentation and information about Salesforce's services?

- Salesforce's global Data Processing Addendum can be found here.

- Salesforce's global Main Services Agreement can be found here.
- The Security Privacy and Architecture Documentation (**"**SPARC") detailing Salesforce's security measures, and the Infrastructure and Sub-processor Documentation listing Salesforce's sub-processors, are available on the Trust and Compliance website here.
- Salesforce's Privacy website can be found here, and provides further information on Salesforce's Privacy programme as well as helpful references including white papers on key topics and documents providing information to assist customers with the completion of data protection impact assessments ("DPIAs").
- The Salesforce Compliance website detailing our compliance certifications and attestations can be found here.

Salesforce also has a dedicated Security page which details best practices, training and security advisories.