Privacy in Japan

Frequently Asked Questions (FAQs)

At Salesforce, trust is our #1 value and the protection of our customers’ data is paramount. We know that many organizations in Japan have questions about their obligations under the Act on the Protection of Personal Information (the “APPI”). To help you develop a better understanding of how the APPI applies to your organization’s potential use of Salesforce’s online services, we have outlined the most common questions asked.

Overview

This document does not provide legal advice and the information we present may not take into account future changes in laws and regulations. We urge you to consult with your own legal counsel to familiarize yourself with the requirements that govern your specific situation.

The Japanese Privacy Act

Japan enacted its first law regulating personal information, the APPI in 2003. The APPI became effective in 2005, and was amended effective May 30, 2017. The amendments were made to meet a higher standard reflecting international trends (in particular, the European GDPR). In 2019, a Supplementary Rule was issued related to EU adequacy, in which Japan and the EU deemed one another's' laws to be adequate to allow transfers of personal data between the jurisdictions. Additional information about the current APPI can be found below.

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 (the "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 (the “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. Purpose of use (Art.15, 16, 18)

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.

5. Penalty for the misuse of personal information (Art.83)

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

6. Transfer of personal data to and from third parties (Art.23, 26)

Business operators generally must obtain consent from a data subject to transfer personal data to third parties, unless an exception applies. 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.

7. Limitation on cross-border transfer of personal data (Art.24)

When transferring personal data to a third party located outside of Japan (excluding the countries in the EEA) 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. However, consent is not required if the recipient agrees to
strong data protection terms like those in the data processing addendum that Salesforce makes available to its customers.

**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 service provider outside of Japan, the business operator will generally be required to obtain data subjects' prior consent for such transfer unless one of the following exemptions applies:

(i) the transfer is to a country that the PPC regards as having data protection laws and regulations equivalent to the APPI (currently limited to European Economic Area member states);

(ii) the transfer is to the recipient that put into place a system compliant with the APPI with regard to handling of personal data; or

(iii) the transfer is to a recipient certified based upon an international framework regarding handling of personal data (currently including only the APEC Privacy Framework).

Salesforce offers customers a contract, including its data processing addendum, that demonstrates it has put in place a robust system for handling data submitted by customers to its services. Salesforce is also certified under the APEC Privacy Framework; more information is available at our JAPAC privacy website.

**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. As used in this document, “Personal Data” refers to personal data that customers submit to the Services as Customer Data. Information about Salesforce’s Sub-processors is available in our public Infrastructure and Sub-processors documentation applicable to each Service, available here.

**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.

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.

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 Master Subscription Agreement which incorporate the Documentation applicable to the specific Services purchased by 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.

What is the APEC Cross Border Privacy Rules system, and does it apply to Salesforce’s customer relationships?

Salesforce has obtained the APEC certification that applies to transfers of data to processors. An
FAQ on Salesforce’s PRP certification is available at our JAPAC privacy website.