June 2017

Practice Group:

Privacy, Data Protection and Information Management

Data Security in Japan: New Cross-Border Data Transfer Rule

By Yuki Sako and Nobu Kawanaka

Does your business outside of Japan receive any personal information from Japan, perhaps from your affiliates, business partners, or customers based in Japan? Does your business in Japan transfer any personal information outside of Japan, perhaps to your overseas affiliates or business partners? If yes, here is what you need to know about the new cross-border personal data transfer rule that became effective on May 30, 2017.

Amendment to the Personal Information Protection Act

Legislative and Regulatory History

The Personal Information Protection Act (the "PIPA"), enacted originally in 2003, is the main law concerning personal data protection in Japan. In 2015, the Diet passed its first major amendment to the PIPA since its full enforcement in 2005 (the "Amended PIPA"). The Personal Information Protection Committee (the "PPC"), a new government agency created in 2016 under the Amended PIPA, proposed and, through a series of required public consultation, promulgated various regulations and guidelines under the Amended PIPA.[1]

Key Highlights of the Amended PIPA

Key points under the Amended PIPA include the following:

Expansion of the scope of application — removal of the 5,000-individuals threshold

Before the Amended PIPA, businesses (regardless of whether they are corporate entities or individuals) that collected, used, or retained certain personal information relating to 5,000 or fewer individuals were exempt from various obligations under the PIPA. The Amended PIPA eliminates the 5,000-individuals threshold, resulting in a greater scope of application.

New rule on Personal Data transfer with an opt-out option[2]

Under the Amended PIPA, Personal Data (defined below) can be transferred to a third party in Japan for and within the purposes notified to the relevant individuals or publicly disclosed, with an opt-out procedure and prior notification to the PPC. New recordkeeping obligations would also apply to a transferor. Those who receive Personal Data would be required to

[1] Other governmental bodies have also promulgated guidance applicable to respective industries under their jurisdiction. For example, from February through March 2017, the PPC and the Financial Services Agency (the "FSA") have jointly issued the guideline, practice guidance, and Q&A applicable to financial services sector.

[2] This does not include so-called "shared use," which allows sharing Personal Data with parties identified in a prior notice or public disclosure, typically using a privacy policy. It is important to note that if the transferee, regardless of whether under a third-party transfer or shared use, is located outside of Japan, additional consent requirement (prior affirmative consent) may apply.

check due transfer process of the Personal Data they receive and be responsible for certain recordkeeping.

Special rules for "De-identifiable Personal Information" and "Sensitive Personal Information"

"De-identifiable Personal Information," Personal Information (defined below) that is de-identified pursuant to the PPC regulations (essentially, making the Personal Information anonymous so that it does not identify a relevant Principal), is subject to less stringent rules, e.g., no consent is required for providing to a third party; however, certain public disclosures are required.

"Sensitive Personal Information," which includes information about race, religion, social status, medical records, criminal records, or the fact that the individual had been victimized, is subject to stricter rules, essentially requiring prior affirmative consent to collect or share with a third party unless an exception applies.

Expansion of extraterritorial reach

The Amended PIPA applies to certain businesses that are located and doing business outside of Japan, as discussed in Section 2 below.

Additional requirement for cross-border Personal Data transfer

Cross-border Personal Data transfer would be, unless one of the exemptions or exceptions apply, subject to additional requirements that may include obtaining prior affirmative consent Please see Section 3 for further information.

What Is Included in "Personal Information"?

Under the Amended PIPA, "Personal Information" essentially means information about a living individual that (i) can identify a specific individual by name, date of birth, or other description containing such information recorded in documentation, pictures, or electronic records, or represented by sound or bodily movements (including such information that will allow easy reference to other information, thereby enabling identification of a specific individual); or (ii) includes individual identifying codes.

Further, when Personal Information is assembled in a searchable manner, it collectively is referred to as a "Personal Information Database," and each piece of the Personal Information comprising such Personal Information Database is referred to as "Personal Data."

The Amended PIPA at a Glance

The below table provides a high-level summary of key duties and responsibilities that apply to businesses when obtaining and/or using Personal Information or Personal Data under the Amended PIPA.[3] Certain provisions of the Amended PIPA do not apply to businesses that merely collect and use Personal Information but do not make a Personal Information

[3] This table was prepared based on a table included in the Q&A issued jointly by the PPC and the FSA and only highlights some of the key obligations applicable to businesses and does not cover all of the provisions under the Amended PIPA. For example, the table does not cover provisions that provide various rights of individuals who provide their Personal Information, such as rights to request disclosure or correction, obligations of businesses in relation to such rights, or special rules for De-identifiable Personal Information, among others.

Database using the Personal Information collected. The Amended PIPA provides a number of exemptions and exceptions, which are not necessarily mentioned in the below table.

Article of Amended PIPA	Personal Information	Personal Data	Summary
§ 15: Specifying Purposes	Applicable	Applicable	Businesses should specify purposes of use in handling Personal Information; generally, purposes can be changed to the extent new and old purposes are reasonably related.
§ 16: Limitation of Use	Applicable	Applicable	Businesses shall not use Personal Information other than what is necessary for specified purposes without obtaining prior affirmative consent or by relying on an exception or exemption.
§ 17: Proper Collection	Applicable	Applicable	No deceptive or other improper means should be used to obtain Personal Information; Sensitive Personal Information can only be obtained with prior affirmative consent or by relying on an exception.
§ 18: Notification of Purposes	Applicable	Applicable	Unless purposes of use are publicly disclosed prior to collection of Personal Information, notice or public disclosure of purposes must be given immediately upon obtaining the Personal Information; exemptions and exceptions may apply. When making changes to the purposes of use, notice of updated purposes must be given or publicly disclosed.
§ 19: Keeping Accuracy of Personal Data	N/A	Applicable	Businesses should maintain accuracy of and update Personal Data as necessary to achieve purposes of use; businesses should remove Personal Data when it becomes unnecessary to use it.
§ 20: Security Control Action	N/A	Applicable	Businesses must establish and implement protective measures for retained Personal Data, pursuant to the Amended PIPA ("Security Control Action"). Under the PPC General Guideline, Security Control Action includes: a data protection policy, organizational measures, human

Article of Amended PIPA	Personal Information	Personal Data	Summary
			resource-related measures, physical safeguard measures, and technical measures.
§ 21: Supervision of Employees	N/A	Applicable	Businesses must provide necessary and appropriate supervision over their employees.
§ 22: Supervision of Third Parties	N/A	Applicable	When retaining contractors to handle Personal Data, businesses must provide necessary and appropriate supervision over them.
§ 23: Restriction on Third-Party Provision	N/A	Applicable	Unless an exemption or exception applies, businesses must obtain prior affirmative consent from relevant individuals to provide Personal Data to a third party; businesses may provide Personal Data to a third party when relevant individuals are notified of the provision or the provision is publicly disclosed and notification is filed with the PPC prior to the provision; businesses may provide Personal Information when engaging and delegating all or a part of business operation in handling Personal Data to a third party to achieve purposes of use; businesses may share Personal Data to specified parties if the relevant individuals are notified of such shared use or the sharing is publicly disclosed prior to sharing.
§ 24: Restriction on Cross-Border Third-Party Provision	N/A	Applicable	When a business provides Personal Data to a third party located outside of Japan, it must obtain prior affirmative consent from the relevant individuals for such cross-border provision; in addition to satisfying requirements under § 23, unless a transferee is located in one of the countries designated by the PPC,[4] the transferee is certified under the Asia-Pacific Economic Cooperation ("APEC") cross-border privacy rules ("CBPR")

[4] As of the date of this publication, the PPC had not designated any country.

Article of Amended PIPA	Personal Information	Personal Data	Summary
			framework or certain appropriate and reasonable measures are placed to ensure that the transferee complies with obligations equivalent to those under the Amended PIPA. Please see Section 3 below.
§ 25: Recordkeeping of Third-Party Provisions (as provider)	N/A	Applicable	When providing Personal Data by way of third-party provision, businesses must record such provisions and retain such records for an applicable retention period of up to three years.
§ 26: Recordkeeping of Third-Party Provisions (as recipient)	N/A	Applicable	When receiving Personal Data by way of third-party provision, businesses that receive Personal Data must check the due transfer process and keep records of transfers for an applicable retention period of up to three years.

Administrative Sanctions and International Cooperation

Businesses in compliance with the obligations under the Amended PIPA may be subject to various administrative sanctions, such as inspection, instruction, advice, warning, or orders. Furthermore, the Amended PIPA enables the PPC to cooperate and share information with non-Japanese governments to enhance international enforcement efforts.

Expanded Extraterritorial Reach

In principle, a Japanese law generally does not apply to conducts outside of the jurisdiction of Japan. However, Article 75 of the Amended PIPA provides that some provisions of the Amended PIPA may apply to conduct that takes place outside of Japan. Under Article 75 of the Amended PIPA, some articles of the Amended PIPA apply to businesses that are located outside of Japan but handle Personal Information acquired during the course of providing goods or services to residents in Japan, even if those goods or services are provided from overseas.

In this regard, the PPC takes the position that in cases where a business located outside of Japan obtains Personal Information through an electronically transmitted inquiry from a potential customer in Japan via its website (e.g., through an online question form), acquisition of Personal Information may be deemed to take place inside Japan thereby becoming subject to the relevant provisions of the Amended PIPA. On the other hand, a business located outside of Japan that provides services through a website accessible from Japan but has adequate preventive measures in place to prevent it from providing its goods or services to residents in Japan is not likely to be subject to the Amended PIPA under Article 75 by virtue of having such a website. Further, Article 75 would be applied to a non-Japanese business that directly collects Personal Information from relevant individuals but

not businesses that obtain Personal Information from a Japanese business, e.g., a Japanese affiliate, in which case that Japanese affiliate is subject to the Amended PIPA.

Cross-Border Transfer of Personal Data

One of the most significant changes the Amended PIPA brought is introducing new rules on cross-border provision of Personal Data. Under Article 24 of the Amended PIPA, except for cases that satisfy one of the limited statutory exceptions or exemptions, a business is likely to be required to obtain prior affirmative consent from relevant individuals (as opposed to an opt-out option) to provide Personal Data to a party outside of Japan.

Consent Requirement and Exceptions and Exemptions

Article 23 of the Amended PIPA provides general rules that apply to Personal Data provisions and provides multiple arrangements where Personal Data can be provided or shared. Article 24 of the Amended PIPA provides special rules that apply to Personal Data provisions to "a third party in overseas."

Under Article 24 of the Amended PIPA, to provide Personal Data to "a third party in overseas," a business must:

1. (i) obtain prior affirmative consent for *cross-border provision* from relevant individuals (ii) upon identifying either the countries to which the Personal Data will be provided or situations where the Personal Data will be provided to overseas with sufficient specificities, unless:
   a. it satisfies one of the statutory exceptions, examples of which are:
      i. the provision is based on Japanese laws[5]; or
      ii. the provision is necessary to protect the life, body, or property and it is difficult to obtain consent from the relevant individuals;

or

   b. the recipient is excepted from "a third party in overseas" if it satisfies one of the following:
      i. the recipient is located in a country designated by the PPC as having personal data protection system equivalent to the standards of Japan;[6]
      ii. the provider and recipient ensure, with respect to the subject Personal Data, implementation of appropriate and reasonable measures in line with certain provisions under the Amended PIPA, which include all of the provisions set forth in the table above; or
      iii. the recipient is certified to satisfy international standards regarding Personal Information protection. In this regard, currently, the PPC only recognizes the APEC CBPR system as the international standard.

[5] For example, one may disclose Personal Date to a third party pursuant to a disclosure order issued by a Japanese court.
[6] As of the date of this publication, the PPC has designated no country.

As we mentioned above, Article 23 provides general rules for Personal Data provisions. The specific type of arrangement under Article 23 would determine what options (exceptions or exemptions) are available under Article 24.

Below, we set forth certain types of arrangements that many businesses may come across:

2. The provision satisfies one of the statutory exceptions, examples of which are:

    c. the provision is based on Japanese laws; or

    d. the provision is necessary to protect the life, body, or property and it is difficult to obtain consent from the relevant individuals.

In this case, requirement under Article 24 would also be excepted; no affirmative consent is required.

3. The provision satisfies general third-party provision requirements with an opt-out option by providing:

    a. prior notification or public disclosure regarding intended third-party transfers;

    b. prior notification to the PPC; and

    c. an opt-out option.

In this case, the transferee must be excepted from "a third party in overseas" by satisfying item (b) of Section a. above.

4. The provision satisfies one of the following exemptions for the provider from becoming "a third party" under Article 23:

    d. the provider engages and delegates all or part of business operations in handling Personal Data to a party to the extent it is necessary for achieving purposes of use;[7]

    e. Personal Data is provided due to a merger or other succession of businesses; or

    f. Personal Data is shared among identified parties (so-called "Shared Use") pursuant to prior notification or public disclosure regarding intended Shared Use.

In this case, the provider must obtain prior affirmative consent from relevant individuals or the recipient must be excepted from "a third party in overseas" by satisfying item (b) of Section a. above.

    g. The provider provides Personal Data based on prior affirmative consent for provision from relevant individuals.

In this case, the consent must be obtained in the manner that is required under Article 24, i.e., there must be consent for cross-border provision and certain items must be specified pursuant to Article 24.

This new cross-border Personal Data transfer rule would apply to all the Japanese businesses that share, e.g., client data or employee data, with non-Japanese affiliates or business partners that are located outside of Japan. On the other hand, if a branch in Japan shares Personal Data with the head office located outside of Japan, such provision is unlikely to trigger the cross-border transfer rule, as it takes place within the same corporate

[7] Please note that purposes of use must be notified or publicly disclosed when obtaining Personal Information pursuant to the Amended PIPA.

entity; however, the overall entity itself is likely to be the business that is directly subject to the Amended PIPA and may be required to comply with other parts of the law.

Recordkeeping for Third-Party Transfers of Personal Data

It is also important to note that the Amended PIPA introduced new recordkeeping obligations for businesses to keep track of all the third-party provisions, including cross-border provisions. Provisions that satisfy an exception or exemption are generally excepted from the recordkeeping obligation.

The Amended PIPA Went Live on May 30, 2017

All of the provisions of the Amended PIPA that had yet to become effective became effective on May 30, 2017. In applying the new regulatory framework to the current state of global businesses in a practical manner, there are questions yet to be answered, and we expect to see more questions arising as businesses put greater efforts together in fully complying with the Amended PIPA. While it appears that the PPC intends to provide additional guidance as it sees necessary and appropriate, how this newly born agency with little track record would provide supervision over businesses in practice and bring enforcement is still yet to be seen.

As cybersecurity and data protection continue to be key policies in regulatory agendas across the globe, all businesses should continue to pay close attention to developments of the Amended PIPA and the PPC in Japan, as well as data protection regimes in other jurisdictions.

Please contact the authors for any questions regarding the Amended PIPA or other personal data protection-related compliance.

Authors:

Yuki Sako
yuki.sako@klgates.com
+81.3.6205.3622

Nobu Kawanaka
nobu.kawanaka@klgates.com
+81.3.6205.3618