JONES DAY

AUGUST 2014

# COMMENTARY

# Framework for Amendment to Japan's Personal Information Protection Act

On June 24, 2014, Japan's Strategic Headquarters for the Promotion of an Advanced Information and Telecommunication Network Society ("IT Strategy Headquarters") within the Cabinet Office announced its "Policy Outline of the Institutional Revision for Utilization of Personal Data"[1] ("Policy Outline").[2]

Following the December 20, 2013 publication of the IT Strategy Headquarters' decision titled "Directions on Institutional Revision for Protection and Utilization of Personal Data,"[3] and further discussions made by the personal data study council established within the IT Strategy Headquarters, the Policy Outline was decided with a view to submit a bill to amend the Personal Information Protection Act (Law No. 57 of 2003) ("the Act") in the January 2015 session of the Diet (Japan's bicameral legislature).

The Policy Outline was open for public comment until July 24, 2014. This is the first amendment to the Act in the more than 10 years since the Act's original enactment in 2003 and its full enforcement beginning in 2005.[4]

While we will have to wait for a bill to be submitted to the Diet early next year for further details of the amendment, this *Commentary* describes the main points set out in the Policy Outline that will significantly affect the business practices and compliance programs of Japanese companies, as well as foreign companies, engaged in the collection and use of personal data in Japan.

## Background[5]

**The remarkable progress in information and communications technology and the rise of "big data" business.** More than 10 years have passed since the enactment of the Act. During this decade, remarkable progress in information and communication technology has been made at an unexpectedly rapid pace, making it possible to store and analyze "big data,"—namely, large amounts of data sent to and collected from personal computers, smartphones, car navigation systems, etc.—at a much lower cost than before. Utilization of such data brings companies valuable information regarding the needs and tastes of consumers for use in the development of new products or services. The Japanese government also considers the use of IT and big data as the key to business success amidst global competition.[6]

Despite such a need and the high value of using big data, it is said that many Japanese companies hesitate

to make use of it, in particular "personal data," because of the ambiguities of the rules under the Act and consumers' growing privacy concerns. The conflict between the usage of big data and privacy is best illustrated by the JR Suica incident. A Suica[7] card is a rechargeable smart card that can be used as a fare card on trains in Japan. The card can also be used for shopping at a number of stores. In late June 2013, East Japan Railway Company ("JR East") decided to sell the processed travel record information and purchase history recorded on customers' Suica cards to a third party. JR East planned to delete each person's name and telephone number before transferring the information so that the third-party recipient could not identify the person. A number of objections and opposing views were raised by consumers, saying that identification could be possible, if combined with other data and information available on the internet and social networking services ("SNS"), and that privacy would be infringed even if there were no violation of the Act. Consequently, JR East abandoned the plan on July 25, 2013.

Under such circumstances, it has been recognized that the Act needs to be amended to set out a new system to facilitate the utilization of personal data while protecting the privacy of individuals.

**Globalization.** As information and communication technology advances, more and more personal data is distributed across national borders, especially through cloud services. To cope with such changes, reviews of privacy rules have been conducted on a global basis, including, inter alia, revisions to the Organization for Economic Cooperation and Development ("OECD") privacy guidelines of July 2013,[8] approval of the draft General Data Protection Regulation by the European Parliament's plenary session in March 2014 in the European Union,[9] and publication of the "Consumer Privacy Bill of Rights" in the United States[10] in February 2012.

Given such a global movement, the Policy Outline recognizes that the Act needs to be reviewed from the perspective of international harmonization.

## Major Matters to Be Revised

**New framework to allow utilization (transfer) of personal data without consent.**[11] Under the Act, with some exceptions, the transfer of Personal Data requires the advance consent of the person (Article 23, Paragraph 1). The Policy Outline states that a new system will be introduced under which Personal Data, that is processed into data with a reduced identifiability of persons, can be transferred without the consent of the person. In other words, if the Personal Data is anonymized, pseudonymized, or otherwise processed so that there is a reduced possibility that the person can be identified, consent of the person will not be required for the transfer of such data.

It is well taken that even with such a reduced possibility of identifying the persons, the persons may be identified and personal rights may be violated if the data is not handled properly. Accordingly, necessary measures will be taken to define the proper handling of the data. Such measures will include, for instance, the prohibition of a data recipient from any attempt to identify persons through analyzing their data in combination with other data.

The question is what measures will suffice to "process the Personal Data into data with a reduced possibility of individuals being identified." The Policy Outline has not provided any clear guidance for judging whether a certain method is sufficient or not. Rather, the Policy Outline states that such processing measures should not be decided uniformly because of the variety of data and usage thereof. Accordingly, under the proposed new framework, such measures will be decided by self-regulatory rules to be established by nongovernmental organizations. A third-party organization equivalent to the privacy commissioner in other nations (which will be established as further explained below) will then certify such nongovernmental organizations and self-regulatory rules.

**Expansion of scope of protection as "personal information."**[12] In the Act, "Personal Information" is defined as "information about a living individual which can identify the specific individual by name, date of birth, or other description contained in such information (including such information as will allow easy reference to other information and will thereby enable the identification of the specific individual) (Article 2, Paragraph 1). As this definition shows, whether the person can

be identified via the information is the key criteria for distinguishing between the personal information to be regulated under the Act and other information. Accordingly, such information as a mobile ID, IP address, location information, etc., does not fall under the definition of "Personal Information" under the Act. However, there is a growing concern that privacy rights may be at risk if such information is not properly handled, as with rapidly developing information technologies such information could be easily linked with other information and the person identified. On the other hand, from the perspective of business, companies are often reluctant to utilize personal data because of such consumer concern over their privacy, and the unclarity in interpreting the Act.

To resolve the above issue and remove the barriers to the utilization of personal data, the Policy Outline proposes to clarify personal data to be protected and lay down regulations as necessary. Information "pertinent to the physical characteristics of individuals, such as fingerprint recognition data and face recognition data" is expressly stated in the Policy Outline as additional information to become protectable. However, it is not clear what other information will be additionally included in the scope of personal information. In light of the discussions made in the personal data study council, it is possible, though yet uncertain, that identification numbers such as passport numbers, driver license numbers, IP addresses, and mobile terminal IDs may become protectable.

As the scope of protectable information may vary with time, due to multiple factors such as the development of information and communication technology and the individual's subjective view, it is suggested that only a general framework will be laid down by law and that specific details will be provided through a Cabinet Order, Ministerial Ordinance, Rules and guidelines.[13]

**Definitions for "sensitive information" or "sensitive data."** The Policy Outline states that the amendment will define information regarding race, creed, social status, criminal record, past record and other information that may cause social discrimination as "sensitive information," and will consider the careful handling of such sensitive information, including a prohibition.

**Multistakeholder process and self-regulation rules**.[14] In order to balance the promotion of the utilization of personal data with the protection of personal information and privacy, the Policy Outline states that a framework for private sector-led self-regulations will be established based upon the concept of a multistakeholder process, which is defined as "a way of laying down regulations and such in an open process in which relevant parties participate, such as the Government, business entities, consumers, and experts."[15] For instance, it is expected that measures to process Personal Data into data with a reduced identifiability of individuals will be laid down by self-regulatory rules taking into account each business practice and characteristics. Further, a third-party organization (as explained below) will certify such self-regulations and nongovernmental organizations.

**Establishment of third-party organization (Privacy Commissioner).**[16] At present, the Act is enforced by the minister of each ministry with the authority to supervise its particular business sector. As a result, each ministry establishes ministerial guidelines for the interpretation and enforcement of the Act, and as of today, 40 ministerial guidelines for 27 business sectors exist. Accordingly, each company needs to analyze and identify which ministerial guidelines apply to its business. It is also possible that more than one guideline applies to a particular company. As a result, the Act has not been uniformly or strongly enforced.

Following centralized enforcement systems adopted in other nations, the Policy Outline sets out that the government will establish an independent third-party authority organization to effectively enforce the laws and regulations, as well as self-regulatory rules. It is planned that the Specific Personal Information Protection Commission, prescribed by the so-called "The Number Use Act,"[17] will be restructured to form the third-party independent organization.

Furthermore, it is expected that the third-party organization will be given stronger powers and more functions than each minister currently has under the Act. Currently, the minister of a relevant ministry may take such measures as (i) advice, (ii) request for report, (iii) recommendation, and (iv) order. In fact, during the eight-year period from 2005 to 2012, there was no case where an order was issued, and only seven where recommendations were issued.[18]

In addition to the above powers and functions, it is planned that the third-party organization will be able to "give instructions, perform onsite inspections, [and] make public announcements." Furthermore, the third-party organization will perform the duties of advance consultation, handling of complaints, cooperation with enforcement authorities of other nations, etc. It is expected that the introduction of "advance consultation" will provide companies with more foreseeability when they start new businesses using the personal data.

**Globalization issues.**[19] Regarding extraterritorial application, the Act is generally interpreted to not apply to foreign entities. However an increasing number of cloud service providers and other foreign entities collect and use the personal information of Japanese residents. Therefore, the mere domestic application of the Act is considered insufficient to protect the privacy rights of people residing in Japan. For this reason, the Policy Outline states that the definition of "Entity Handling Personal Information" to which the Act applies will be revised to adequately enhance the scope of the Act's application to include foreign entities. Further, in order to ensure the proper handling of personal data by such foreign entities, the amendment will provide a legal basis for the third-party organization to provide foreign enforcement authorities with information useful for their enforcement under the pertinent law and regulations.

While the transfer of Personal Data is regulated under the Act, there is no additional requirement or regulation for the extraterritorial transfer of Personal Data. Accordingly, there is no way to regulate or prohibit the transfer of Personal Data to a country where the protection of Personal Data is insufficient. To resolve such an issue and harmonize the level of protection in this regard with many other jurisdictions, the Policy Outline states that if the entities handling personal information transfer Personal Data to a foreign entity, such entity will be required to take necessary action, such as conclusion of a contract requiring the recipient of such Personal Data to take the necessary and appropriate actions for the safe management of the Personal Data. Further, there are various types of transfer of Personal Data, for instance, (i) transfer to a foreign group company, (ii) transfer to a foreign service provider, (iii) joint use with a foreign entity, (iv) transfer to a nonaffiliated third-party entity, (v) transfer associated with business transfer or merger, and (vi) re-transfer to an entity of a third nation. The Policy Outline states that the government will consider both the details of necessary actions and a framework for ensuring their effectiveness depending upon the types of data transfer.

## Conclusion

According to the Policy Outline, it is planned that a bill to amend the Act will be submitted to the Diet in or after January next year as early as possible, and that the third-party organization will be established as soon as possible after enactment of the amendment.

The revisions will significantly impact not only Japanese companies but also foreign companies that collect and use the personal data of Japanese nationals. In particular, given that the amended Act will expressly provide applicability of the Act to foreign entities, it is important to continue watching the development of these revisions in order to analyze and examine its impacts and determine how businesses should comply with the new rules.

## Lawyer Contact

For further information, please contact your principal Firm representative or the lawyer listed below. General email messages may be sent using our "Contact Us" form, which can be found at www.jonesday.com.

**Michiru Takahashi**
Tokyo
+81.3.6800.1821
mtakahashi@jonesday.com

## Endnotes

1 The term "personal data" in the Policy Outline has a broad meaning of data and information related to a person, including personal activities and status, etc. without regard to the identifiability of the person. The term "*Kojin* data," which is the same as "personal data" when translated into English, is used and defined in the Act. The term "personal data" as defined in the Act requires identifiability of the person. To distinguish these two terms in this article, we use the term in lower-case letters when it has a broad meaning as used in the Policy Outline, except when it is used as in a title of official documents. When we refer to the specific term "*Kojin* data" as defined in the Act, we use the term as "Personal Data."

2 An English version is available at http://japan.kantei.go.jp/policy/it/20140715__2.pdf.

3 An English version is available at http://japan.kantei.go.jp/policy/it/2013/1220__fulltext.pdf.

4 Please also see Jones Day Commentary "Personal Information Protection Law in Japan" (November 2005) at http://www.jonesday.com/personal-information-protection-law-in-japan-11-09-2005/.

5 *See* Part 2. I. 1. of the Policy Outline.

6 "Declaration to Be the World's Most Advanced IT Nation," IT Strategy Headquarters, June 14, 2013. An English translation is available at http://japan.kantei.go.jp/policy/it/2013/0614__declaration.pdf.

7 *See* http://www.jreast.co.jp/e/pass/suica.html.

8 OECD, The Recommendations of the OECD Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (2013). *See* http://www.oecd.org/sti/ieconomy/privacy.htm#newguidelines.

9 European Parliament, European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (2014). *See* http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2014-0212&language=EN.

10 White House, Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy (2012). *See* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

11 *See* Part 3. II. of the Policy Outline.

12 *See* Part 3. III. 1. (1) and (2) of the Policy Outline.

13 *See* Part 2. II. 2. of the Policy Outline.

14 *See* Part 3. III. 2. and 3. of the Policy Outline.

15 Footnote 5. of the Policy Outline.

16 *See* Part 3. IV. of the Policy Outline.

17 Act on the Use of Numbers to Identify a Specific Individual in the Administrative Procedure (Act No. 27 of 2013). This law was established to introduce the number system for social security and taxation purposes. A so called "my number," equivalent to a social security number, will be assigned to each person. The Specific Personal Information Protection Commission was established under this law on January 1, 2014 to ensure the proper handling by the national and local governments as well as the business sector of such number and personal information linked to such number.

18 "Outline of Enforcement Situation of Personal Information Protection Act, 2012," issued by Consumer Affairs Agency (September 2013) at http://www.caa.go.jp/planning/kojin/24-sekou__3.pdf (available only in Japanese).

19 *See* Part 3. V. of the Policy Outline.