Data Privacy Protection of Personal Information Versus Usage of Big Data: Introduction of the Recent Amendment to the *Act on the Protection of Personal Information* (Japan)

By: Noriko Higashizawa and Yuri Aihara

Noriko Higashizawa is a partner at City-Yuwa Partners and her practice is focused on employment law and business litigation. She has provided her clients with considerable advice on data security and privacy issues, including development of internal policies and measures in privacy breach matters.

Yuri Aihara is a corporate counsel at Fujifilm Corporation and a former associate at City-Yuwa Partners, and she regularly tackles privacy and data security issues.

MORE and more businesses are waking up to the importance of big data as a strategic resource. By analyzing the purchase history of its customers, a business can easily identify purchase trends and patterns. The increasing availability of cloud processing, analytics, and storage services has enabled businesses of

all sizes across many industries to access big data. However, we must remain concerned both about the collection of personal data and in particular, the promulgation of data privacy laws to both protect personal data and, at the same time, promote the utilization of big data.

In Japan, the Act on the Protection of Personal Information ("PPIA") was recently amended and became effective on May 30, 2017 (the "Amended Act"). The amendments will introduce a number of changes to existing personal data protection system. The term "personal information" as used in the Amended Act, for example, has been clarified to further protect personal data and introduce more necessary regulations. At the same time, the amendments introduce the concept of "Anonymously Processed Information" to promote the use of enormous personal data (i.e., big data) collected through the development of information and communication technology ("ICT"). The Amended Act also introduces new rules in response to the globalization of data flows.

The purpose of this article is to provide practitioners with an understanding of three important changes made by the Amended Act and how these changes are likely to play out in practice. In Part I of this article, we will give a brief explanation on the newly revised definition of personal information under the Amended Act. Part II addresses and clarifies how and when big data should be treated under the new concept of Anonymously Processed Information. Part III discusses the new scheme under the Amended Act on cross-border transfers of personal information.

I. Definition of Personal Information

A. Clarification of definition of personal information

Under PPIA, "personal information" was defined broadly, and the scope of personal information was at times ambiguous. This ambiguity created difficulties among business operators.[1] For instance, information like personal identification numbers would not fall under the definition of personal information under PPIA in the absence of other information that could be easily used to identify a specific individual. With the development of ICT, however, there is a growing concern that privacy

[1] Under PPIA, personal information was 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)".

rights are at risk if information like personal identification numbers are not properly handled, since this type of information can now be easily linked with other information to identify a specific individual.

To clarify the scope of personal information, the Amended Act defined the concept of "Individual Identification Codes." [2] "Individual Identification Codes," include codes, characters, letters, numbers, or symbols as prescribed in the Order for Enforcement of the Amended Act (the "Cabinet Order"). According to the Cabinet Order, Individual Identification Codes consist of two categories of codes:

(1) Codes which a body feature of a specific individual has been converted into data to be provided for use by computers, including DNA sequence data, facial recognition data, iris pattern data, voiceprint data, gait pattern data, palm/finger vein pattern data and fingerprint/palm print data.

(2) Codes which are assigned in regard to the use of services provided to an individual or to the purchase of goods sold to an individual, or which are stated in a document issued to an individual so as to be able to identify a specific user or purchaser, such as a passport number, basic pension number, driver's license number, individual number (so-called "My Number") and national health insurance number.[3]

B. Regulations concerning Special Care-Required Personal Information

The Amended Act introduces the concept of "Special Care-Required Personal Information", which broadly corresponds to concepts of "sensitive personal information" as seen in other jurisdictions, most notably in the EU and an increasing number of jurisdictions in the Asia-Pacific region. "Special Care-Required Personal Information" means personal information comprising the following data which require special care in handling so as not to cause unfair discrimination, prejudice or other disadvantages to the data holder.[4]

The Amended Act directly designates items as "Special Care-Required Personal Information" as follows: race; creed; social status; medical history; criminal record; and history of being a victim of crime.

[2] Amended Act, Art. 2, Paragraph 2.

[3] Cabinet Order, Art. 1.

[4] Amended Act, Art. 2, Paragraph 3.

In addition, the Cabinet Order[5] has designated other items to be "Special Care-Required Personal Information," including:

- Physical/intellectual disabilities, mental disorder;
- Results of a medical check-up, specific health guidance, medical care or prescriptions; and
- Criminal proceedings (including proceedings under the Juvenile Act) brought against a data holder as a suspect or defendant).[6]

A business operator must obtain the consent of the data holder in advance to obtain Special Care-Required Personal Information, [7] and the transfer of such information to a third party based on an opt-out basis is not permitted.[8]

II. Anonymously Processed Information

Under the PPIA, securing the consent of data holders was generally required to utilize their personal information for purposes other than those specified in advance or to provide their personal information to third parties. This system ended up as one of the primary barriers to promoting the use of personal information. To address the obvious administrative problems that this rule created, the Amended Act adopted the concept of "Anonymously Processed Information" to promote the utilization of diverse and vast amounts of personal information for big data use. By so doing, the Amended Act will create new businesses and services and simultaneously to prevent violations of privacy rights. Anonymously Processed Information is not affected by restrictions like the restriction on use beyond the scope of purpose. It also imposes no particular obligations to obtain the consent of the data holder for such uses. Anonymously Processed Information can also be provided to a third party without obtaining consent from the data holder.

A. Definition of Anonymously Processed Information

"Anonymously Processed Information" means information relating to an individual that can be produced from processing personal information so as neither to be able to identify a specific individual by taking prescribed action nor to be able to restore the personal

[5] Cabinet Order, Art. 2.
[6] Cabinet Order, Art. 2.
[7] Amended Act, Art. 17, Paragraph 2.
[8] Article 23, Paragraph 2 of the Amended Act.

information.[9] In other words, we can construe Anonymously Processed Information to mean personal data that is anonymized or otherwise processed so that there is a reduced possibility that the person can be identified.

Please note that statistical information neither falls under personal information nor Anonymously Processed Information. Statistical information is produced by categorizing or classifying information collected from various people aiming to undertake trends/ features of a targeted group.

B. Obligation of Business Operators

Even with a reduced possibility of identifying a specific individual, an individual may nonetheless be identified and personal rights may be violated if the data is not handled properly. Accordingly, the Amended Act attempts to provide guidelines on the necessary measures to be taken to define the proper handling of data. A business operator engaged in generating Anonymously Processed Information must comply with the following six (6) obligations:

(1) to process personal information in accordance with standards prescribed by the Rules of the Personal Information Protection Commission[10] (the "Rules") as those necessary to make it impossible to identify a specific individual and restore the personal information used for the production when producing anonymously processed information.[11]

We will provide an explanation on this process in Section II.C *infra*.

(2) to take action for data security in accordance with standards prescribed by the Rules as those necessary to prevent the leakage of information relating to those descriptions, including deleting individual identification codes from personal information used to produce the Anonymously Processed Information, and information relating to a processing method carried out when having produced

[9] Amended Act, Art. 2, Paragraph 9.

[10] The Amended Act will establish the Personal Information Protection Commission to form a third-party independent organization and to take over the supervisory and enforcement responsibilities of the Consumer Affairs Agency in regards to data protection.

[11] Amended Act, Art. 36, Paragraph 1; Rules, Art. 20.

anonymously processed information.[12]

Pursuant to the Rules, a business operator engaged in generating Anonymously Processed Information needs to (i) define clearly the authority and responsibility of the person handling information relating to those descriptions and individual identification codes which were deleted from personal information used to generate Anonymously Processed Information, including the information relating to the processing method carried out; (ii) establish rules and procedures on the handling of the processing method and related information in accordance with the Rules and procedures, evaluate the handling situation, and based on such evaluation results, take necessary action to seek improvement; and (iii) take necessary and appropriate action to prevent a person with no legitimate authority to handle the processing method.

(3) to disclose to the public the categories of information relating to an individual contained in the Anonymously Processed Information pursuant to the Rules when having produced Anonymously Processed Information.[13]

If a business operator processes personal information which includes a customer's name, sex, date of birth and purchase history and generates Anonymously Processed Information which includes only information on "sex, year of birth and purchase history," the categories in which a business operator needs to disclose to the public are the "sex, year of birth and purchase history." The disclosure can be made by using the internet or other appropriate methods.

(4) to disclose to the public the categories of information concerning an individual contained in Anonymously Processed Information to be provided to a third party and its providing method, and state to the third party explicitly to the effect that the information being provided is Anonymously Processed Information pursuant to the Rules when

[12] Amended Act, Art. 36, Paragraph 2.

[13] Amended Act, Art. 36, Paragraph 3; Rules Art. 21.

having produced Anonymously Processed Information and providing the Anonymously Processed Information to a third party.[14]

(5) not to collate Anonymously Processed Information with other information in order to identify a holder concerned with personal information used to produce the Anonymously Processed Information when having produced Anonymously Processed Information and making itself handle the Anonymously Processed Information.[15]

It should be noted that operators are permitted to generate statistical information by combining Anonymous Processed Information with other information that is not relevant to the data holder or dependent upon the original personal information.

(6) to strive to take necessary and appropriate action to secure Anonymously Processed Information and necessary action to properly handle Anonymously Processed Information, including addressing complaints about the handling, including producing, of Anonymously Processed Information, and strive to disclose to the public the contents of any action taken during production of Anonymously Processed Information.[16]

(4) to (6) of the above-listed obligations are also applied to "an Anonymously Processed Information Handling Business Operator", a business operator who provides a collective body of information comprising Anonymously Processed Information that has been systematically organized so as to be able to search using a computer for commercial purposes.[17]

C. Production of Anonymously Processed Information

The Rules prescribe appropriate methods to process personal information which make it impossible to identify a specific individual and restore the personal information as follows:[18]

(1) deleting a whole or part of those descriptions which

[14] Amended Act, Art. 36, Paragraph 4.
[15] Amended Act, Art. 36, Paragraph 5.
[16] Amended Act, Art. 36, Paragraph 6.
[17] Amended Act, Arts. 37-39.
[18] Rules, Art. 19.

help identify a specific individual contained in personal information.

For instance, if the personal information contains a specific individual's name, address and date of birth (D/M/Y), a business operator can make it Anonymously Processed Information by deleting the name, abstracting the address ("XX city") and replacing date of birth with only month and year of birth.

(2) deleting all individual identification codes contained in personal information.

If personal information contains individual identification codes like a passport number, basic pension number or driver's license number, all of such codes must be deleted.

(3) deleting those codes which link personal information to information obtained by having taken measures against the personal information.

If a business operator tracks a customer's purchase history and also possesses this customer's fundamental personal information (such as name or address) and links them by assigning an identification number to each customer, a business operator can utilize purchase history as Anonymously Processed Information by deleting these identification numbers.

(4) deleting idiosyncratic descriptions.

For instance, if a hospital maintains patient medical histories involving very peculiar cases, the hospital can utilize the medical history by deleting specifics of these cases.

(5) other appropriate action based on the results from considering the attributes of personal information database like the difference between descriptions contained in the personal information and descriptions contained in other personal information constituting the personal information database that encompass such personal information.

When utilizing location information as Anonymously Processed Information, for instance, the information which specifies an address or place of business of a specific

individual must be deleted. To utilize medical checkup data at an elementary school whose database contains data of a student who is exceedingly tall compared to other students, the information of the height of the student should be deleted or abstracted to, for instance, "higher than 150 cm."

III. Globalization of the Protection of Personal Information

The Amended Act establishes new provisions applicable to the provision of personal data[19] to third parties in foreign countries in response to globalization of corporate activities in Japan. These provisions have established personal information protection regime in Japan that will receive an adequacy decision under the EU Data Protection Directive to facilitate the flows of personal data with EU.

A. Regulations for the provision to a third party in foreign countries

1. General Principles

Under the Amended Act, a business operator must obtain prior consent of the data holder before transferring personal data to a third party in a foreign country.[20] In this context, a legal entity located outside of Japan (including a member of the same group of companies) which has a separate corporate identity from the business operator will be considered as "a third party in a foreign country." For example, a subsidiary of a Japanese company which is incorporated in a foreign country will be considered as "a third party in a foreign country." In contrast, a representative office and/or branch office of a Japanese company will not be considered as "a third party in a foreign country" because they are part of the same corporation (i.e., a Japan head office and its branch office both operate as parts of the same corporation). Thus, a Japanese company must obtain prior consent from a data holder of personal information when it provides personal information to its subsidiaries in foreign countries except in the cases explained below.

---

[19] "Personal data" means personal information constituting a personal information database etc. Also, a "personal information database etc." means those set forth in the following which are a collective body of information comprising personal information (excluding those prescribed by Cabinet Order as having little possibility of harming an individual's rights and interests considering their utilization method). Amended Act, Art. 2, Paragraphs 4 and 6.

[20] Amended Act, Art. 24.

2. Exceptions

There are some recognized exceptions to these general principles, including that:

(1) a country determined under the Rules to have a standard personal information protection regime equivalent to Japan is excluded from this restriction.[21]

(2) a person establishing a system conforming to standards prescribed by the Rules to be equivalent to the one that a business operator shall take pursuant to the Amended Act.

(3) other statutory exceptions set forth in Article 23, Paragraph 1 of the Amended Act.[22]

Except in compliance with items (1) and (2) above, it is not possible to use opt-out procedures.[23] Rather, the prior consent from the data holder of personal information is required even for the following cases for transferring personal data to a foreign country:[24]

(i) where personal data is provided accompanied by a business operator entrusting a whole or part of the handling of the personal data within the necessary scope to achieve a utilization purpose;

---

[21] No countries have yet received this designation.

[22] Article 23, Paragraph 1 of the Amended Act provides as follows:

A Business Operator Handling Personal Information handling business operator shall not provide personal data to a third party without obtaining in advance a consent of the holder of the personal data except in those cases set forth below:

(i) cases based on laws and regulations;
(ii) cases in which there is a need to protect a human life, body or fortune, and when it is difficult to obtain a principal's consent;
(iii) cases in which there is a special need to enhance public hygiene or promote fostering healthy children, and when it is difficult to obtain a principal's consent; and
(iv) cases in which there is a need to cooperate with a central government organization, a local government, or a person entrusted by them in the performance of duties prescribed by laws and regulations, and when there is a possibility that obtaining a principal's consent would interfere with the performance of the said duties.

[23] Amended Act, Art. 23, Paragraph 2.

[24] Amended Act, Art. 23, Paragraph 5 provides as follows:

In the following cases, a person receiving the provision of the said personal data shall not fall under a third party in regard to applying the provisions of each preceding paragraph.

(ii) where personal data is provided accompanied with business succession caused by a merger or other reason; and

(iii) where personal data to be jointly utilized with a specified person is provided to that person, and when a data holder has in advance been informed or a state has been in place where a data holder can easily know to that effect as well as of the categories of the jointly utilized personal data, the scope of a jointly utilizing person, the utilization purpose for the utilizing person and the name or appellation of a person responsible for controlling the said personal data (*kyodo riyo*).

Please remember that a recipient of personal data from a business operator shall meet the standards prescribed by the Rules.

3. Standards prescribed by the Rules of the Personal Information Protection Commission

As described above, a business operator is not required to obtain prior consent of the data holder of personal information where the recipient has satisfied the Standards prescribed by the Rules ("Standards") for protective measures in handling personal data. The Standards are as follows:[25]

(1) Between a business operator and the receiver of the personal data, the implementation of the measures pursuant to the purpose of Chapter 4 Sub-chapter 1 of the Amended Act to secure and handle in an appropriate and reasonable manner the personal data received; or

(2) A receiver of the personal date has a certification based on the international regime for the handing of personal information.

4. Items which should be noted to meet the Standards

(1) The measures should be taken in an appropriate and reasonable manner.

[25] Rules, Art. 11.

(2) The measures should be taken pursuant to the purposes of Chapter 4 Sub-chapter 1 of the Amended Act:[26]

- Specifying a purpose for utilization (Article 15 of the Amended Act)
- Restrictions due to the utilization purpose (Article 16 of the Amended Act)
- Proper acquisition (Article 17 of the Amended Act)
- Proper notification of a utilization purpose when acquiring (Article 18 of the Amended Act)
- Proper assurance about the accuracy of data contents (Article 19 of the Amended Act)
- Data control plan (Article 20 of the Amended Act)
- Supervision of employees (Article 21 of the Amended Act)
- Supervision of the trustee (Article 22 of the Amended Act)
- Restriction on third party provision (Article 23 of the Amended Act)
- Restriction on provision to a third party in a foreign country (Article 24 of the Amended Act)
- Public disclosure of matters relating to retained personal data[27] (Article 27 of the Amended Act)
- Disclosure (Article 28 of the Amended Act)
- Correction (Article 29 of the Amended Act)
- Utilization cessation (Article 30 of the Amended Act)
- Explanation of reasons for cessation (Article 31 of the Amended Act)
- Procedure for responding to a demand for disclosure (Article 32 of the Amended Act)
- Fee (Article 33 of the Amended Act)
- Dealing with complaints by business

[26] These measures are prepared in accordance with OECD Privacy Guideline and APEC Privacy Framework.

[27] "Retained personal data" in the Amended Act means personal data which a personal information handling business operator has the authority to disclose, correct, add or delete the contents of, cease the utilization of, erase, and cease the third-party provision of, and which shall be neither those prescribed by Cabinet Order as likely to harm the public or other interests if their presence or absence is made known nor those set to be deleted within a period of no longer than one year that is prescribed by Cabinet Order. Amended Act, Art. 2, Paragraph 7.

operators (Article 35 of the Amended Act)

It is not necessary for a business operator to implement all of the measures referenced above. If some measures are taken in a proper and reasonable manner from the perspective of the purpose of Chapter 4 Sub-chapter 1 of the Amended Act, this would satisfy the Standards. Case studies are attached in an Appendix to this article for ease of understanding how this might work.

(3) If a third party in a foreign country receives certification under the CBPR system of APEC, the provision of the personal data to such third party will not require the consent of the data holder because it can be said that a receiver of the personal date has the certification which is based on the international regime for handing of the personal information.

B. Extraterritorial application of the Amended Act

The provisions which obligate Japanese business operators under the Amended Act also apply to business operators who handle personal information or Anonymously Processed Information in foreign countries for businesses providing goods or services to the customers in Japan. If an internet shopping operator located in foreign country acquires personal information from Japanese consumers to sell and deliver the goods to them, or if a mail service provider located in a foreign country acquires personal information from Japanese users, these business operators must comply with the provisions of the Amended Act. The Personal Information Protection Commission provide advice, guidance or recommendations in the event foreign business operators breach the provisions of the Amended Act.

Appendix - Case Studies

Case 1: A company in Japan ("Japan Business Operator") entrusts a service provider located in a foreign country ("Foreign Service Provider") to handle personal data

Measures to be taken to meet the Standards:

- An agreement, a written confirmation or a memorandum of understanding (the "Service Agreement") between Japan Business Operator and Foreign Service Provider should be signed or executed.
- Foreign Service Provider should specify purpose of use in the Service Agreement.
- Foreign Service Provider should acquire the personal data in accordance with and its scope of use should be restricted in the Service Agreement.
- Japan Business Operator should notify its customers of purpose of use.
- The Service Agreement should contain a provision confirming the accuracy of the received personal data or otherwise obligating Japan Business Operator to ensure the accuracy of it.
- The Service Agreement should contain a provision in which Foreign Service Provider is obligated to implement security measures to protect the personal data.
- The Service Agreement should contain a provision in which Foreign Service Provider takes appropriate measures to supervise its employees handling or use of personal data.
- The Service Agreement should contain a provision in which Foreign Service Provider takes appropriate measures to supervising a trustee's / subcontractor's handling or use of personal data.
- The Service Agreement should prohibit Foreign Service Provider from disclosing the personal data to any third party.
- The Service Agreement should also contain provisions about the personal data and its public disclosure, cessation of use, storing and managing, fees and procedures to handle complaint from Japan Business Operator in the event that the personal data to be transferred to Foreign Service Provider falls under the definition of retained personal data.

Case 2: A Japanese subsidiary ("Japanese Subsidiary") transfers personal data to its parent company ("Foreign Parent Company")

Measures to be taken to meet the Standards:

- Internal rules and/or privacy policy commonly applicable to both Japanese Subsidiary and Foreign Parent Company ("Global Internal Rules") should be established.
- Purpose of use should be specified in the employment regulations/work rules.
- Use of Employees' information should be within the scope of use consistent with employment regulations/the work rules. (Consent should be obtained whenever employees' information is used beyond the said scope. In such a case, Japanese Subsidiary may obtain the consent from its employees.)
- Foreign Parent Company should obtain the personal data in accordance with the Global Internal Rules.
- Japanese Subsidiary should notify its employees of the purpose of use.
- Japanese Subsidiary should ensure the accuracy of the employees' personal information.
- Global Internal Rules should require that Foreign Parent Company to implement security measures to protect personal data.
- The Global Internal Rules should require the Foreign Parent Company to take appropriate measures to supervise its employees' handling or use of the personal data.
- The Global Internal Rules should prohibit Foreign Parent Company from disclosing the personal data to any third party.
- The Global Internal Rules should also contain provisions about the personal data, including its public disclosure, cessation of use, storing and managing, procedures for responding to a demand, fees and procedures for handling complaint from Japanese Subsidiary in the event that the personal data to be transferred to Foreign Parent Company falls under the definition of retained personal data.