ANDERSON MŌRI & TOMOTSUNE

DISPUTE RESOLUTION GROUP NEWSLETTER

April 2016

Overview of Important Reform Act

First Substantial Amendment to the Personal Information Protection Act (Core part of the amendment to be enforced by September 8, 2017)

Shinji Kusakabe, Attorney-at-law

Contents

- On September 9, 2015, a reform act constituting the first substantial amendment to the Personal Information Protection Act was promulgated. The core amendments concerning business operators' obligations will come into force by September 8, 2017.
- The various revisions made by the reform act can be largely categorized into: (i) establishment of the Personal Information Protection Commission; (ii) streamlining of the definitions of the types of information to be protected; (iii) expansion of the scope of the regulated business operators; (iv) revision of business operators' obligations; (v) streamlining of cross-border handling; and (vi) creation of the crime of provision of personal information database, etc.
- How the business operators should prepare for the enforcement of the reform act largely depends on the Rules of the Personal Information Protection Commission to be established. However, the responsible divisions of the business operators should fully understand the contents of the reform act and proceed with whatever preparations that can be made before the establishment of the Rules.

Background to Amendment to the Act

Since its promulgation on May 30, 2003 and full enforcement on April 1, 2005, the Act on the Protection of Personal Information (hereinafter, the "Personal Information Protection Act") had experienced no substantial amendment for more than ten years. On the other hand, with the development of information and communication technologies after the enforcement of the Personal Information Protection Act, uses of personal information in business have been diversified. In recent years, personal information has been utilized in manners not contemplated at the time of establishment of the Personal Information Protection Act. An example of this is the delivery of advertisements adapted to an individual's interests and likes analyzed from his/her purchase history, location data and other information related to the individual.

In keeping with the extensive use of personal information in business, consumers are becoming increasingly aware of their rights to privacy. Meanwhile, it has been pointed out that business operators have concerns over the use of personal information due to the ambiguity of the provisions of the Personal Information Protection Act.

As for the global situation, in July 2013, in line

with changing circumstances with respect to handling of personal information, the Organisation for Economic Co-operation and Development (OECD) adopted the proposed revision of the guidelines that would serve as the basis of the personal information protection legislation of the member countries including Japan, and published the amended guidelines in September of the same year. The EU and the United States of America have also improved their frameworks for the protection of personal information. Amid the progress of globalization of corporate activities involving the use of personal information, Japan needs to keep pace with such worldwide trends in protection of personal information.

These factors led to the promulgation on September 9, 2015 of the "Act on the Partial Revision of the Act on the Protection of Personal Information and the Act on the Use of Numbers to Identify a Specific Individual in the Administrative Procedure" (hereinafter, the "Reform Act"), which aims to protect individuals' rights and interests with due consideration to proper and effective use of personal information, and to build systems that are internationally consistent with foreign regulations. The revisions to the Personal Information Protection Act by the Reform Act are wide-ranging, and some are outlined below from the viewpoint of which matters require business operators' special attention (hereinafter, the Personal Information Protection Act before and after the amendment by the Reform Act are referred to as the "Pre-amendment Act" and "Post-amendment Act," respectively, and the specific individual that can be identified by personal information is referred to as the "Person Concerned").

The effective date of the Reform Act varies by clause, and while a certain part of the Reform Act came into force on January 1, 2016, **the parts concerning business operators' obligations will come into force on the day to be specified by an applicable cabinet order, which shall not be later than September 8, 2017**. Business operators need to prepare by then for the enforcement of those parts of the Reform Act (in the sections below, special mention will be made only where the relevant revision has already been enforced as of April 2016).

(1) Establishment of the Personal Information Protection Commission

Under the Pre-amendment Act, Entities Handling Personal Information had been supervised by the competent minister with jurisdiction over the relevant business field (Articles 32-36 of the Pre-amendment Act). As such, guidelines for treatment of the Personal Information Protection Act had been prepared on a business-by-business basis. This compromised uniform and effective law enforcement and impeded law enforcement in the business fields that were not subject to the jurisdiction of any specific competent minister. Furthermore, the absence in Japan of any independent government organization responsible for the protection of personal information could be a ground on which the Japanese personal information protection system was regarded as insufficient from the eyes of EU members or other countries.

As such was the case, the Reform Act established the Personal Information Protection Commission (effective on January 1, 2016) by reorganizing the Specific Personal Information Protection Commission that had been established under the pre-amendment Act on the Use of Numbers to Identify a Specific Individual in the Administrative Procedure (so-called My Number Act).

The Personal Information Protection Commission is a body called independent administrative commission which ranks at the same level of national administrative hierarchy as the Fair Trade Commission and the National Public Safety Commission. The Personal Information Protection Commission is composed of the chairperson and eight commission members and has a secretariat (the number of personnel of the secretariat was just over seventy as of April 2016, which is expected to increase in future years).

The Personal Information Protection Commission is responsible for the enforcement of the Personal Information Protection Act, and **business operators will be particularly affected by the Rules of the Personal Information Protection Commission to be established by the**

Commission. As of the end of April 2016, the said Rules, to which references are made elsewhere herein, have not been established.

(2) Streamlining of the definitions of the types of information to be protected

a. Streamlining of the definition of "Personal Information"

The definition of "Personal Information" to be protected under the Pre-amendment Act was "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 can be easily cross-referenced against other information, thereby enabling the identification of the specific individual)" (Article 2, Paragraph 1 of the Pre-amendment Act). The ambiguity of this definition (in particular, the underlined part within parentheses regarding the ease of cross-reference) had been pointed out as a reason for concern about the handling of personal information by business operators under the Pre-amendment Act.

The Post-amendment Act has changed the above underlined part to a definition for the case in which no "Individual Identification Code" is included in the relevant information (Article 2, Paragraph 1, Item 1 of the Post-amendment Act), and apart from this, **has added** "**information containing Individual Identification Codes" to the definition of "Personal Information"** (Article 2, Paragraph 1, Item 2 of the Post-amendment Act). The Post-amendment Act further defines "Individual Identification Code" as (i) any code into which a distinguishing body part of an individual has been converted so that it may be processed by a computer and which can identify the relevant individual; or (ii) any code allocated to an individual for the purchase or use of goods or services, or that is entered or recorded on cards or other documents issued to an individual, and which can identify the relevant individual, as specified by the applicable cabinet order (Article 2, Paragraph 2 of the Post-amendment Act). While we still need to wait for the publication of the applicable cabinet order for specific details and scope of the "Individual Identification Codes," we may assume that examples of (i) above include fingerprint authentication data and face recognition data, and examples of (ii) above include individual numbers (so-called "My Numbers") and drivers' license numbers.

Such streamlining of the definition of "Personal Information" has clarified that any information containing an "Individual Identification Code" regarding a living individual constitutes "Personal Information." However, it would be difficult to say that the suggested ambiguity of the definition of "Personal Information" will completely disappear, given that the judgment framework used in the above-mentioned underlined part is maintained in the case the relevant information does not contain any "Individual Identification Code."

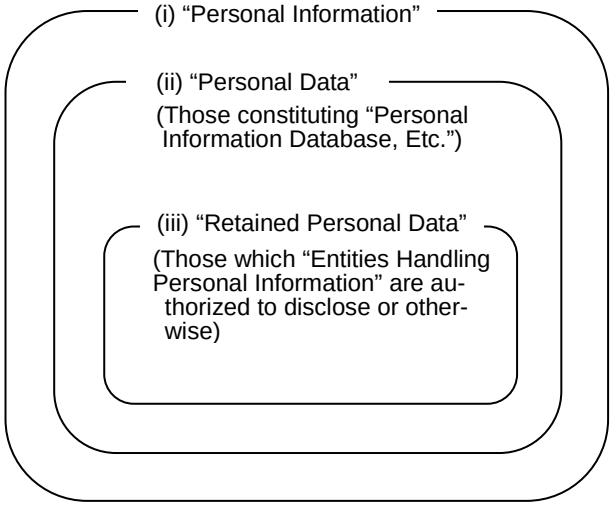
b. Change in definition of "Personal Information Database, Etc."

The Pre-amendment Act defined "Entity Handling Personal Information" as an entity using "Personal Information Database, Etc." for its business (with certain exceptions) (Article 2, Paragraph 3 of the Pre-amendment Act), defined (ii) "Personal Data" as part of (i) "Personal Information" that constitutes a "Personal Information Database, Etc." (Article 2, Paragraph 4 of the Pre-amendment Act), defined (iii) "Retained Personal Data" as part of the "Personal Data" which an Entity Handling Personal Information has the authority to disclose or otherwise (Article 2, Paragraph 5 of the Pre-amendment Act), and set the regulations on Entities Handling Personal Information with respect to each of (i), (ii) and (iii) above. Furthermore, the Pre-amendment Act defined "Personal Information Database, Etc.," which was used for the definition of "Entity Handling Personal Information" and (ii) "Personal Data," as an assembly of information which includes Personal Information and is systematically arranged in such a way that specific Personal Information can be retrieved by a computer or otherwise (Article 2, Paragraph 2 of the Pre-amendment Act).

The above-mentioned structure remains the same under the Post-amendment Act (Article 2,

Paragraphs 4-7 of the Post-amendment Act). However, the Post-amendment Act has revised the definition of "Personal Information Database, Etc.," which is used in the definition of "Entity Handling Personal Information" and "Personal Data," to exclude "any information specified by the applicable cabinet order as being unlikely to harm the rights and interests of any individual considering the manner of use of the relevant information" (Article 2, Paragraph 4 of the Post-amendment Act). While we still need to wait for the publication of the applicable cabinet order for specific details and scope of such information, we may assume that the applicable cabinet order would cite, as examples of this, commercial directories (such as phone books, *Kaisha Shikiho* or other company data books), lists of resident association members and the like (limited to those used for the purpose of information sharing among the members).

Such **narrower definition of "Personal Information Database, Etc." has narrowed down the scope of "Entity Handling Personal Information" and "Personal Data," and to that extent, handling of Personal Information has become less regulated**. That said, it should be noted that the definition of "Entity Handling Personal Information" has become broader in another respect, as detailed in (3) below.



【Information that Entities Handling Personal Information are obligated to protect】

c. Creation of the concept of "Information Requiring Special Consideration"

The Pre-amendment Act did not provide for special treatment of Personal Information that may give rise to unfair discrimination against an individual, such as information on the individual's race and creed. Yet, such information was called by such terms as "sensitive information" in the guidelines concerning handling of Personal Information published by government authorities, and business operators had been required to give special consideration to the handling of the same.

The Post-amendment Act categorizes **such information as "Information Requiring Special Consideration," a new concept, and gives special treatment to it**. "Information Requiring Special Consideration" is defined as "any Personal Information containing the race, creed, social status, medical history or criminal records of the Person Concerned, the fact that the person has suffered damage through a crime, or other descriptions specified by the applicable cabinet order to require special consideration in handling so as to avoid any unjustifiable discrimination, prejudice or other disadvantage to the Person Concerned" (Article 2, Paragraph 3 of the Post-amendment Act). We still need to wait for publication of the applicable cabinet order for specific details and scope of the "Information Requiring Special Consideration."

For details of special treatment of the "Information Requiring Special Consideration," please see (4)-d below.

d. Creation of the concept of "De-identified Information"

Regulation on use of information concerning anonymized individuals must be restrained to promote so-called "big data" businesses.

However, under the Pre-amendment Act, due to the suggested ambiguity of the definition of "Personal Information" as stated in (2)-a above, it was considered to be difficult to interpret that information technically devised to be anonymous would not constitute "Personal Information" that should be protected. Although the Post-amendment Act has clarified the definition of "Personal Information" to some extent by the use

of the concept of "Individual Identification Code" as mentioned in (2)-a above, this alone would not solve the above-mentioned problem.

Therefore, the Post-amendment Act **created the concept of "De-identified Information"** (Article 2, Paragraph 9 of the Post-amendment Act) and **subjected such information only to regulations that are looser** than those imposed on the "Personal Information."

"De-identified Information" means any Personal Information processed by certain means to prevent the identification of a specific individual and to make it impossible to restore the original Personal Information (Article 2, Paragraph 9 of the Post-amendment Act). The method of processing must comply with the standards to be specified by the Rules of the Personal Information Protection Commission (Article 36, Paragraph 1 of the Post-amendment Act).

It is noted that the language of the Post-amendment Act does not expressly provide that "De-identified Information" does not constitute "Personal Information." However, an Entity Handling Personal Information which creates De-identified Information is prohibited, in creating and handling such De-identified Information, from cross-referencing the De-identified Information against other information to identify the Person Concerned (Article 36, Paragraph 5 of the Post-amendment Act). In addition, an entity using a database or other collection of De-identified Information for its business ("Entity Handling De-identified Information" defined in Article 2, Paragraph 10 of the Post-amendment Act) is prohibited, in handling such De-identified Information, from cross-referencing the De-identified Information against other information to identify the Person Concerned (Article 38 of the Post-amendment Act). Thus, with respect to these business operators, no "ease of cross-reference" (please see (2)-a above) mentioned in the definition of "Personal Information" is found, and we may accordingly infer that "De-identified Information" does not constitute "Personal Information."

For details of regulations on "De-identified Information," please see (4)-e below.

(3) Expansion of the scope of the regulated business operators

The Pre-amendment Act defined "Entity Handling Personal Information" as an entity using "Personal Information Database, Etc." for its business, exempting certain entities. Such exempt entities included entities with respect to whom the number of individuals in the "Personal Information Database, Etc." used for their business was 5,000 or less on any single day during the past six months (so-called small enterprises) (Article 2, Paragraph 3, Item 5 of the Pre-amendment Act; Article 2 of the Order for Enforcement of the Act on the Protection of Personal Information).

This **exceptional treatment of small enterprises has been abolished** under the Post-amendment Act (Article 2, Paragraph 5 of the Post-amendment Act). Background factors to this would be the fact that the need of protection of personal information is not lost even when it is handled by small enterprises, and the Japanese government's policy to keep up with global trends.

As a result of this amendment, entities that were not subject to regulations under the Pre-amendment Act for being small enterprises not falling under the category of "Entities Handling Personal Information" will be widely regulated under the Post-amendment Act. Thus, small and medium-sized enterprises in particular will face the question as to whether they are taking adequate measures. In addition, given that the Post-amendment Act is considered to require an Entity Handling Personal Information to verify, in receiving the provision of Personal Data from a third party, the status of the providing party's compliance with law, as stated in (4)-b-(II) below, compliance issues may consequentially arise in large companies that receive the provision of Personal Data from small and medium-sized enterprises.

(4) Revision of business operators' obligations

a. Obligations concerning Personal Information

Relaxation of the scope of change in the purpose of use

Under the Pre-amendment Act, an Entity Handling Personal Information was required to specify as precise as possible the purpose of use of the Personal Information, and upon the acquisition of Personal Information, was required to notify the Person Concerned of such purpose of use or otherwise (Article 15, Paragraph 1, and Article 18 of the Pre-amendment Act). Any change in the purpose of use was limited to the scope reasonably considered to be "duly related" to the purpose of use before the change (Article 15, Paragraph 2 of the Pre-amendment Act).

The Post-amendment Act keeps the above-mentioned framework of regulation, but **the scope of change in the purpose of use was somewhat relaxed to the scope which is reasonably considered to be "related" to the purpose of use before the change** (Article 15, Paragraph 2 of the Post-amendment Act).

It is not clear to what extent this deregulation will facilitate a change in the purpose of use. However, at least, a business operator with a privacy policy that defines the scope of change in the purpose of use to be the "duly related" scope as per the language of the Pre-amendment Act may consider changing that part of the policy to the "related" scope as per the language of the Post-amendment Act.

b. Obligations concerning Personal Data

(I) Tightening of regulation on provision to third parties by the opt-out method

Under the Pre-amendment Act, a business operator was allowed to provide Personal Data to a third party without obtaining the consent of the Person Concerned (by using the opt-out method) on condition of meeting the prescribed requirements, such as making the matters regarding such provision to a third party readily accessible to the Person Concerned (Article 23, Paragraphs 2 and 3 of the Pre-amendment Act).

While the above-mentioned scheme remains unchanged under the Post-amendment Act, it has become necessary for a business operator to **notify the Personal Information Protection Commission of certain matters regarding the provision to a third party** (Article 23, Paragraphs 2 and 3 of the Post-amendment Act). The Personal Information Protection Commission will disclose the matters so notified to the public (Article 23, Paragraph 4 of the Post-amendment Act).

These are measures to enable the Person Concerned to get a complete view of the business operators that provide Personal Data to third parties on the website of or other sources of information provided by the Personal Information Protection Commission and to demand the discontinuance of the provision of his/her Personal Data to third parties, if he/she so wishes. Entities Handling Personal Information that provide Personal Data to third parties must proceed with preparation for the filing of such notification to the Personal Information Protection Commission.

(II) Ensuring of proper provision to third parties and traceability

Unlike the Pre-amendment Act, the Post-amendment Act obligated **a third-party Entity Handling Personal Information that receives Personal Data to confirm, as a rule, the name, address, representative's name and the like of the providing third party as well as the "details of the acquisition of the Personal Data by the providing third party**." While the specific method of confirmation will be specified by the Rules of the Personal Information Protection Commission (Article 26, Paragraph 1 of the Post-amendment Act), **the intent of the phrase "details of the acquisition of the Personal Data by the providing third party" is considered to require the receiving party to confirm the status of the providing party's compliance with law**. When the above-mentioned confirmation is carried out by the receiving Entity Handling Personal Information, the providing party may not make a false statement about the matters for confirmation (Article 26, Paragraph 2 of the Post-amendment Act).

In addition, under the Post-amendment Act, **upon the provision of Personal Data to a third party, both the providing and receiving Entities Handling Personal Information are required, in principle, to create a record regarding the provision and to retain the same for a certain period**. The matters to be recorded, recording method and record retention period will be specified by the Rules of the Personal Information

Protection Commission (Article 25, and Article 26, Paragraphs 3 and 4 of the Post-amendment Act).

The intent of these provisions is: (i) to deter improper divulgation of Personal Data by imposing the obligation of confirmation of certain matters as well as preparation and retention of records at the time of provision of Personal Data to a third party; and (ii) to enable tracing of the leakage route of any leaked Personal Data. The Entities Handling Personal Information that are to be involved in the provision of Personal Data to third parties must develop systems that enable them to appropriately confirm certain matters and to create and retain records.

(III) Creation of obligation of best efforts to erase unnecessary Personal Data

Under the Pre-amendment Act, an Entity Handling Personal Information was obligated to make efforts to keep the content of Personal Data accurate and up to date within the scope necessary for achieving the purpose of use (Article 19 of the Pre-amendment Act).

Under the Post-amendment Act, in addition to the above, the Entity Handling Personal Information **is also obligated to endeavor to erase without delay any Personal Data if the use of which has become unnecessary** (Article 19 of the Post-amendment Act).

The requirements described above are both best-effort obligations, but Entities Handling Personal Information should consider building an erasure process for Personal Data, and business operators with a privacy policy imposing a best-effort obligation as per the Pre-amendment Act would be encouraged to revise the relevant part.

c. Obligations regarding Retained Personal Data

Clarification of right of the Person Concerned to request disclosure

Under the Pre-amendment Act, an Entity Handling Personal Information was obligated to comply with any request of the Person Concerned for disclosure of the Retained Personal Data, or correction, addition or deletion thereof (if any of the Retained Personal Data is untrue), or discontinuance of use, erasure or discontinuance of provision thereof (if the handling, acquistion or provision to third parties of the Retained Personal Data was illegally made) (Articles 25-27 of the Pre-amendment Act). However, owing to the unclear text of these provisions, opinions were divided over whether the Person Concerned was entitled to request disclosure or other actions as a right under private law, and there was a court precedent that denied this (Judgment of the Tokyo District Court of June 27, 2007).

The Post-amendment Act **has clarified that the Person Concerned is entitled to request disclosure or other actions as a right under private law** (Articles 28-30 of the Post-amendment Act). Furthermore, it stipulated that the Person Concerned may file a lawsuit or a petition for provisional disposition order based on his/her rights only after the lapse of two weeks following the out-of-court lodging of a claim against the Entity Handling Personal Information (Article 34 of the Post-amendment Act).

Now that it has become clear that the Person Concerned has a right to request disclosure or other actions concerning the Retained Personal Data and it has also become clear what the procedures to be taken before the filing of a lawsuit or a petition for provisional disposition order are, Entities Handling Personal Information are required to develop systems that allow them to adequately meet within two weeks of any request for disclosure or otherwise from the Person Concerned.

d. Special treatment of the "Information Requiring Special Consideration"

Under the Post-amendment Act, the following special treatment is required for the "Information Requiring Special Consideration" described in (2)-c above, as distinct from other Personal Information, Personal Data and Retained Personal Data:

(I) Phase of acquisition of Personal Information

Prior consent of the Person Concerned is required to acquire any "Information Requiring Special Consideration" except in certain cases (Article 17, Paragraph 2 of the Post-amendment Act).

(II) Phase of provision of Personal Data to

third parties

The provision of any "Information Requiring Special Consideration" to a third party cannot be made without obtaining consent of the Person Concerned by using the opt-out method (Article 23, Paragraphs 1 and 2 of the Post-amendment Act).

(III) Phase of request for discontinuance of use of or other actions regarding Retained Personal Data

If any "Information Requiring Special Consideration" has been acquired or provided to a third party in breach of (I) or (II) above, the Person Concerned may request discontinuance of use, erasure or discontinuance of provision of the Retained Personal Data containing such information (Article 30, Paragraphs 1 and 3 of the Post-amendment Act).

Based on the above, Entities Handling Personal Information will be required to develop a system to treat the "Information Requiring Special Consideration" differently from before, or a system wherein no acquisition of "Information Requiring Special Consideration" occurs in the first place.

e. Regulation on "De-identified Information"

Under the Post-amendment Act, Entities Handling Personal Information and Entities Handling De-identified Information are respectively subject to the following regulations with respect to the "De-identified Information" as explained in (2)-d above. As far as such De-identified Information is concerned, Entities Handling Personal Information and Entities Handling De-identified Information are considered not to be separately subject to the regulation regarding the "Personal Information." Accordingly, **for example, they are not required to obtain consent of the Person Concerned in providing De-identified Information to third parties**.

(I) Regulation on Entities Handling Personal Information

An Entity Handling Personal Information must observe the Rules of the Personal Information Protection Commission **in creating De-identified Information, taking measures to ensure secure management of the original and related information, publishing the information items regarding the individual that are included in such De-identified Information, and publishing certain matters at the time of provision of such De-identified Information to a third party and making an express indication of certain matters to the relevant third party** (Article 36, Paragraphs 1-4 of the Post-amendment Act).

In addition, in preparing and handling De-identified Information, an Entity Handling Personal Information **is prohibited from cross-referencing the De-identified Information against other information to identify the Person Concerned** (Article 36, Paragraph 5 of the Post-amendment Act), and is required to endeavor to take the necessary measures to ensure appropriate handling of the De-identified Information and to publish the details of such measures (Article 36, Paragraph 6 of the Post-amendment Act).

(II) Regulation on Entities Handling De-identified Information

An Entity Handling De-identified Information must observe the Rules of the Personal Information Protection Commission **in publishing certain matters at the time of provision of De-identified Information to a third party and making an express indication of certain matters to the relevant third party** (Article 37 of the Post-amendment Act).

In addition, in handling De-identified Information, an Entity Handling De-identified Information **is prohibited from acquiring the original or related information and from cross-referencing the De-identified Information against other information to identify the Person Concerned** (Article 38 of the Post-amendment Act) and is required to endeavor to take the necessary measures to ensure appropriate handling of the De-identified Information and to publish the details of such measures (Article 39 of the Post-amendment Act).

While regulations on "De-identified Information" are more relaxed than those on "Personal Information," as described above, entities engaged in so-called "big data" businesses need to build systems that are compliant with the Rules of the Personal Information Protection Commission as they will be required to deal with the relevant

issues as per those Rules.

(5) Streamlining of cross-border handling

The Post-amendment Act has revised regulations on cross-border handling of Personal Information, as follows:

a. Extraterritorial application

The Pre-amendment Act was applicable to any act involving Personal Information that was performed in Japan, irrespective of whether the agent of the act was a Japanese individual or corporation or a foreign individual or corporation.

The above applicability remains unchanged and fundamental under the Post-amendment Act. However, the Post-amendment Act has stipulated that the Act is also applicable to certain acts that are performed in a foreign country. More specifically, in the case where **an Entity Handling Personal Information that has, in connection with the provision of goods or services to an individual in Japan, acquired Personal Information of that individual handles in a foreign country the relevant Personal Information or De-identified Information created using the relevant Personal Information, many of the provisions of the Post-amendment Act shall apply to such act** (Article 75 of the Post-amendment Act).

As a result, it has become necessary to verify whether or not the Post-amendment Act applies to any act performed in a foreign country by a company within a corporate group based in or outside Japan.

b. Provision of Personal Data to third parties in a foreign country

As stated in (4)-b-(I) above, even under the Post-amendment Act, Personal Data may be provided to a third party without obtaining consent of the Person Concerned (by the opt-out method) subject to satisfaction of certain requirements. However, **as a special provision, it is stipulated that Personal Data may not be provided to any third party in a foreign country, in principle, without consent of the Person Concerned** (Article 24 of the Post-amendment Act). The cases specified as exceptions to the foregoing are (i) where the receiving third party is in any of the countries prescribed by the Rules of the Personal Information Protection Commission as having personal information protection systems equivalent to those in Japan, or (ii) where the receiving third party has put in place personal information protection systems that satisfy the standards prescribed by the Rules of the Personal Information Protection Commission. Any provision of Personal Data to a third party in a foreign country that falls under either of these exceptions will be subject to the same regulations as those imposed on the provision of Personal Data to third parties in Japan.

Entities Handling Personal Information that had been providing Personal Data to third parties in a foreign country using the opt-out method under the Pre-amendment Act need to determine, based on the Rules of the Personal Information Protection Commission, whether they can continue such handling under the Post-amendment Act as well.

It should be noted that with respect to the provision of Personal Data to third parties in Japan under the Pre-amendment Act, the receiving party was deemed not to constitute a “third party” (a) if the handling of such Personal Data was entrusted to the receiving party within the scope necessary for achieving the purpose of use, (b) if the Personal Data was provided upon succession of the business of the providing party, or (c) if the Personal Data are used jointly with a specific party under certain conditions, and the provision of Personal Data to any such party was deemed not to constitute the provision to a “third party” for which the consent of the Person Concerned was required (Article 23, Paragraph 4 of the Pre-amendment Act).

The above-mentioned scheme remains unchanged under the Post-amendment Act (Article 23, Paragraph 5 of the Post-amendment Act). However, it should be noted that the above-mentioned stipulation that the consent of the Person Concerned is required as a rule for the provision of Personal Data to a third party in a foreign country (Article 24 of the Post-amendment Act) applies equally to the provision of Personal Data in the cases (a), (b) and (c) above as well

(the main sentence of Article 23, Paragraph 5 and the second sentence of Article 24 of the Post-amendment Act).

In addition, even in the case of the provision of Personal Data to a third party in a foreign country, the providing Entity Handling Personal Information is obligated to create a record regarding the provision and retain the same for a certain period (Article 25 of the Post-amendment Act), as stated in (4)-b-(II) above. This obligation is applicable even in the case where the provision occurs in a foreign country if the requirements for extraterritorial application are met (Article 25 of the Post-amendment Act is cited in Article 75 of the same Act). On the other hand, as stated in (4)-b-(II) above, the receiving Entity Handling Personal Information is obligated to confirm the name, address, representative's name and the like of the providing third party as well as the "details of the acquisition of the Personal Data by the providing third party" and to prepare a record regarding the provision and to retain such record for a certain period (Article 26, Paragraphs 1, 3 and 4 of the Post-amendment Act). However, this obligation does not apply to a receiving Entity Handling Personal Information in a foreign country (Article 26 of the Post-amendment Act is not cited in Article 75 of the same Act that provides for extraterritorial application).

c. Receipt of Personal Data from third parties in a foreign country

In the case of receipt of Personal Data from a third party in a foreign country, if the act of receiving occurs in Japan, the receiving Entity Handling Personal Information is obligated to confirm the name, address, representative's name and the like of the providing third party as well as the "details of the acquisition of the Personal Data by the providing third party," and to create a record regarding the provision and retain the same for a certain period (Article 26, Paragraphs 1, 3 and 4 of the Post-amendment Act), as stated in (4)-b-(II) above. As the intent of the phrase "details of the acquisition of the Personal Data by the providing third party" is considered to require the receiving party to confirm the status of the providing party's compliance with law, **if the providing party is in a foreign country, we should assume that the receiving party is required to confirm that the providing party is observing personal information protection laws of the relevant foreign country**. In the near term, practical approaches need to be devised to solve the question of specifically how one should verify the compliance with foreign laws.

Please note that the obligation of the providing Entity Handling Personal Information to create a record regarding the provision and to retain the same for a certain period (Article 25 of the Post-amendment Act) as stated in (4)-b-(II) above is applicable even when the act of providing occurs in a foreign country if the requirements for extraterritorial application are met (Article 25 of the Post-amendment Act is cited in Article 75 of the same Act).

(6) Crime of provision of Personal Information Database, Etc.

The Post-amendment Act **created the crime of provision of Personal Information Database, Etc.** (Article 83 of the Post-amendment Act) as a criminal offense punished by the Personal Information Protection Act. The Act inflicts a penalty on individuals who have engaged in a malicious leakage or misappropriation of personal information in the wake of cases of personal information leakage that have become social problems.

The crime of provision of Personal Information Database, Etc. is constituted if (i) an Entity Handling Personal Information (or in the case of a corporation or any similar entity, an officer, a representative or a manager thereof) or any of its employees or any person who was one of them in the past (ii) provides or misappropriates for the purpose of acquiring a wrongful gain for themselves or for a third party (iii) Personal Information Database, Etc. (including copies or processed versions of all or part of them) that they handled in connection with their duties. An example of cases constituting this crime is where an employee of a company which is an Entity Handling Personal Information sells to any third party outside the company a customer database that has been handled by him/her in the course of his/her

duties.

The statutory penalty for the crime of provision of Personal Information Database, Etc. is imprisonment with labor up to one year or a fine of up to 500,000 yen.
Persons who committed a crime of provision of Personal Information Database, Etc. abroad are also punished (Article 86 of the Post-amendment Act).

In addition, the **joint penalty provision applies to this crime**. As such, if the individual who has committed a violation is the representative, an agent, employee or other worker of a corporation and if such violation was committed in connection with the business of the corporation, the relevant corporation will also be subject to the above-mentioned fine (Article 87 of the Post-amendment Act). Accordingly, each corporation must recognize that this poses a legal risk to itself and should promote its officers' and employees' awareness of this crime through training sessions or other methods.

■ Author:

Shinji Kusakabe, Attorney-at-law
shinji.kusakabe@amt-law.com
Tel: 03-6888-1062
Fax: 03-6888-3062
http://www.amt-law.com/en/professional/profile/SJK