NAGASHIMA OHNO & TSUNEMATSU
長島・大野・常松 法律事務所

NO&T Japan Legal Update

February, 2021 No.26

This issue covers the following topic:

■ DATA PROTECTION AND PRIVACY

Update on Recent Amendments to Data Protection Regulations in Japan
- Outline of the Proposed Amendment of the Cabinet Order and the PPC Rules for the Act on the Protection of Personal Information -

■ DATA PROTECTION AND PRIVACY

Update on Recent Amendments to Data Protection Regulations in Japan - Outline of the Proposed Amendment of the Cabinet Order and the PPC Rules for the Act on the Protection of Personal Information -

I. Introduction

On June 12, 2020, the Amendment Act of the Act on the Protection of Personal Information was promulgated (the "Amendment Act")[1] and shall enter into full force by June 2022. Many of the provisions of the Amendment Act have been delegated to relevant subordinate regulation, such as the Cabinet Order[2] and the Rules[3] of the Personal Information Protection Commission of Japan (the "PPC").

This article will provide an outline of the recent Proposal for Amendment to the Cabinet Order (the "Proposed Order") and the PPC Rules (the "Proposed PPC Rules") which were published in December 2020.[4][5] Furthermore, Guidelines and Q&A will be released from June 2021 onward (the "Guideline").

II. Obligations to Report to the PPC and Notify Data Subjects of Data Breaches

(1) Legal Obligation to Report and Notify

Currently, under the Act on the Protection of Personal Information (the "Current Act"), business operators are not legally obliged to report to the PPC or to notify an affected data subject in the event of a data breach, including the leakage of, or unauthorized access to, personal data. Under the Current Act, business operators are encouraged to make efforts to report any data breach to the PPC or other supervising authorities. This pronouncement is, however, not legally binding.

The Amendment Act sets forth new legally binding obligations on business operators to report to the PPC in certain situations where there has been a data breach of personal data handled by the business operator (Article 22-2(1) of the Amendment Act). In addition, when a business operator is obliged to report to the PPC, the business operator

[1] For the details of the Amendment Act of the Act on the Protection of Personal Information, please see the NO&T Japan Legal Update No. 21, March 2020.
[2] The Cabinet Order to Enforce the Act on the Protection of Personal Information (the "Cabinet Order")
[3] One of the rules is the Enforcement Rules for the Act on the Protection of Personal Information. In this article, we refer to this rule as the "PPC Rules".
[4] The date of full enforcement shall be specified by a Cabinet Order. As soon as the date has been determined. the PPC will announce it via the PPC website.
[5] As to the Proposed Order and the Proposed PPC Rules, public comments were being solicited with a deadline of January 25, 2021. The Amendment to the Cabinet Order to Enforce the Act on the Protection of Personal Information and the Amendment to the Enforcement Rules for the Act on the Protection of Personal Information will be promulgated between mid-February and early April 2021.

Author in this Issue

■ Data Protection and Privacy

Oki Mori
Partner
+81-3-6889-7271
oki_mori@noandt.com

Keiji Tonomura
Partner
+81-3-6889-7460
keiji_tonomura@noandt.com

Emi Fujisaki
Associate
+81-3-6889-7447
emi_fujisaki@noandt.com

Naoki Fukumoto
Associate
+81-3-6889-7597
naoki_fukumoto@noandt.com

must also notify affected data subjects of the data breach (Article 22-2(2) of the Amendment Act).

In connection with these reporting and notification requirements, the Proposed PPC Rules contain further detail regarding:

- situations when the reporting and notification obligation will apply;
- mandatory timeframes for reporting and notification;
- the matters to be reported and notified; and
- the method of reporting and notification.

(2) Obligation to Report to the PPC

(a) Situations that Trigger the Reporting Obligation

The Proposed PPC Rules describe four situations which are classified as being highly likely to harm the rights and interests of the data subject:

(i) a data breach of special care-required personal data[6] has occurred or is likely to have occurred (Article 6-2(i) of the Proposed PPC Rules);

(ii) a data breach that may cause financial damage due to unauthorized use has occurred or is likely to have occurred (Article 6-2(ii) of the Proposed PPC Rules);

(iii) a data breach that may have been committed with a wrongful purpose has occurred or is likely to have occurred (Article 6-3(iii) of the Proposed PPC Rules); and

(iv) where more than 1,000 data subjects are or are likely to be affected by a data breach (Article 6-3(iv) of the Proposed PPC Rules).

Business operators, however, shall not be obliged to report a data breach to the PPC in cases where the breached personal data is protected by measures put in place to protect the rights and interests of data subjects, such as advanced encryption (Article 6-2(i) of the Proposed PPC Rules).

According to the PPC, categories (i) and (ii) above each focus on the nature of the breached personal data, whereas categories (iii) and (iv) focus on the manner and scale of a data breach, respectively. With respect to category (ii), it is assumed that credit card numbers, internet banking IDs and passwords are specific examples of personal data that would fall under that category. Matters that fall within category (iii) must be reported because of the high risk of further improper use of the personal data.

(b) Time Restrictions on Reporting

Unlike the GDPR, the Amendment Act itself does not include any time restriction on reporting to the PPC.

The Proposed PPC Rules, however, separates the obligation to report to the PPC into two categories; namely, "prompt reporting" and "confirmatory reporting". A business operator will be obliged to make both a prompt report and a confirmatory report. When a business operator becomes aware of a situation that requires it to make a report to the PPC, the business operator shall promptly report to the PPC (Article 6-3(1) of the Proposed PPC Rules). The Guideline is expected to provide further clarification on the definition of "prompt".

[6] Article 2(3) of the Current Act includes a similar concept to the "*special categories of personal data*" stipulated in the GDPR.

Recent Publications

- ***BENEFICIAL OWNERSHIP DISCLOSURE AND TRANSPARENCY REQUIREMENTS (Philippines)***
  (NO&T Asia Legal Review No.31, January 2021)
  by Patricia O. Ko
- ***LAW ON PUBLIC PRIVATE PARTNERSHIP (Vietnam)***
  (NO&T Asia Legal Review No.31, January 2021)
  by Hoai Tran
- ***DRAFT NEW NEGATIVE LIST: MORE BUSINESSES OPEN FOR FOREIGN INVESTORS (Indonesia)***
  (NO&T Asia Legal Review No.31, January 2021)
  by Ichsan Montang
- ***Recent Movement towards Legalization of Mobile Applications for Taxi or Ride-hailing Services***
  (NO&T Thailand Legal Update No.8, January 2021)
  by Yothin Intaraprasong and Luxsiri Supakijjanusorn
- ***Recent Movement on the Law on Climate Change***
  (NO&T Thailand Legal Update No.8, January 2021)
  by Yothin Intaraprasong and Kwanchanok Jantakram
- ***Personal Data Protection - Duties after your business faces a cyber-attack or hacking***
  (NO&T Thailand Legal Update No.8, January 2021)
  by Yothin Intaraprasong, Yuyu Komine and Poonyisa Sornchangwat
- ***Global Arbitration Review - The Guide to M&A Arbitration - Third Edition Part II (Survey of Substantive Laws) Chapter 14 Japan***
  (Law Business Research Ltd , January 2021)
  by Hiroki Aoki

In relation to a confirmatory report, the Proposed PPC Rules provide that a matter shall, in principle, be reported within 30 days from the date that a business operator first becomes aware of a situation that requires it to report to the PPC. In the event of data breach which may have been committed with a wrongful purpose, business operators will have up to 60 days from the date that a business operator first becomes aware of such data breach to provide a confirmatory report to the PPC (Article 6-3(2) of the Proposed PPC Rules).

(c) Details to Be Reported

The details that must be reported by business operators in prompt and confirmatory reports are as follows:

Matters (Article 6-3(1) and Article 6-4 of the Proposed PPC Rules):	Report to the PPC	Notification to Data Subjects
i. Description of the data breach	✓	✓
ii. Personal data items affected by the data breach	✓	✓
iii. The number of data subjects affected	✓	-
iv. Cause of the data breach	✓	✓
v. Whether there has been or is likely to be further improper use of the personal data and, if so, the details of that further improper use	✓	✓
vi. The status of measures taken in relation to the affected data subjects	✓	-
vii. The status of public announcement made in relation to the data breach	✓	-
viii. Any remedial measures taken since the data breach	✓	✓
ix. Other relevant details	✓	✓

(d) Method of Reporting

In principle, business operators will be able to submit their reports to the PPC online (Article 6-3(3)(i) of the Proposed PPC Rules).

(e) Exemption from the Obligation of a Trustee to Report to the PPC

In the event of a data breach by a trustee to whom a business operator has entrusted the handling of personal data (a concept similar to "processor" under the GDPR), both the trustee and the trustor (a concept similar to "controller" under the GDPR) shall be obliged to report to the PPC in principle. However, the trustee shall not be obliged to report the data breach to the PPC if it notifies the trustor of the data breach (Article 22-2(1) of the Amendment Act).

In such cases, the trustee must promptly notify the trustor of the details to be reported after it first becomes aware of a situation that requires it to report to the PPC (Article 6-4 of the Proposed PPC Rules). It should be noted that the trustee is not exempt from its obligation to continue to investigate the situation and to cooperate with the trustor in reporting to the PPC.

(3) Notification to Data Subjects

(a) When the Obligation to Notify Arises

According to the Amendment Act, when a business operator is obliged to report a data breach to the PPC as mentioned above, the business operator shall also notify all affected data subjects of the data breach (Article 22-2(2) of the Amendment Act). However, unlike the obligation to report to the PPC, in cases where it is difficult to notify the data subject, the business operator may be exempted from doing so provided that sufficient alternative measures are taken to protect the data subject's rights and interests (Article 22-2(2) of the Amendment Act). It is not clear in the Proposed PPC Rules what actions or measures will be sufficient to rely on this exemption.

(b) Time Restriction for Notification

The Proposed PPC Rules stipulate that all affected data subjects shall be notified promptly "according to the circumstances" after the business operator first becomes aware of a situation that requires it to report to the PPC (Article 6-5 of the Proposed PPC Rules). As such, a business operator is not required to notify the affected data subjects at the same time as reporting to the PPC. This is presumed to be based on the recognition that while it is necessary to notify

the affected data subjects promptly, the appropriate timing of such notice will vary from case to case, and prompt notification may even be detrimental to the data subject.

(c) Details to Be Notified

The Proposed PPC Rules state that the affected data subjects should be notified of the data breach "to the extent necessary to protect the rights and interests of the data subjects". The list of details that should be disclosed to the affected data subjects is indicated in the table on page 3 under "Notification".

(d) Method of Notification

The Proposed PPC Rules are silent on how notice should be given to the affected data subjects.

(4) Impact on Business Practices

The range of situations that require reporting under the Proposed PPC Rules is narrower than those situations under the Current Act that obligate a business owner to make efforts to report to the PPC. However, business operators may submit voluntary reports to the PPC even if a situation arises that does not fall under the mandatory reporting categories. In practice, a business operator will need to make that determination on a case-by-case basis. For example, in cases where an external inquiry about why it has not made public announcement of a data breach is expected, a business operator may elect to voluntarily make a report to the PPC and explain to the inquiring party that it is seeking guidance from the PPC and shall respond appropriately.

III. New Matters to Be Disclosed

(1) "Measures Taken for Safety Management"

In the Proposed Order, "*measures taken for safety management of retained personal data*" was included as an additional matter to be disclosed to the public by business operators (Article 8(i) of the Proposed Order).

Similar to Article 20 of the Current Act, although there are no specific provisions in the Proposed Order regarding "*measures taken for safety management*", the PPC provides the examples below of appropriate safety measures for the management of retained personal data. It will be necessary for business operators to make an assessment of their individual situation with reference to the following:

- Establishment of internal controls: establishing and periodically reviewing rules for handling personal data and persons in charge and their duties at each stage, including acquisition, use, disclosure and disposal.
- Establishment of organizational structure: appointment of a responsible person, defining his/her position and duties, and implementing a reporting and liaison system in the event that a data breach occurs.
- Periodic inspections and audits: periodic self-inspections, audits by other departments, and audits by external bodies.
- Education of officers and employees: ensuring that training is regularly conducted and clauses related to confidentiality are included in rules of employment and employees are made aware.
- Prevention of unauthorized access: introduction of measures to protect against unauthorized access.
- Understanding of the external environment: a system to protecting personal information in foreign countries when personal information is handled in such foreign countries.

In addition, there are exceptions to the obligation to disclose the measures implemented for safety management. These include items that may hinder the safety management of such retained personal data if they are disclosed to the data subject. The PPC cites the following examples as exceptions to the disclosure obligation:

- Methods of disposal of equipment containing personal data.
- Theft prevention measures.
- Physical entry and exit control methods for personal data control areas.
- Scope of access control and authentication methods of authorized persons.

- Details of measures to prevent unauthorized access.

(2) Specifying the Purpose of Use of Collected Personal Data in lieu of Disclosing "Measures of Processing Retained Personal Data"

Prior to the publication of the Proposed Order, there was discussion that a business operator's "*measures of processing retained personal data*" would be included as an amendment to the Cabinet Order and would be additional information to be disclosed publicly. Eventually, "*measures of processing retained personal data*" was not included in the Proposed Order and instead business operators are required to clearly specify the purpose of use of the collected personal data. The PPC suggested that specifying the purpose of use of the collected personal data is preferable to implementing an obligation on business operators to disclose their "*measures of processing retained personal data*" because of (i) business concerns about the leakage of trade secrets if business operators were required to disclose their "*measures of processing retained personal data*", and (ii) the importance of making data subjects aware that their personal data is being processed in cases where such processing is not easily assumed from the specified purpose of use. The PPC provides the following examples of how to correctly explain the purpose of use of personal data.

- Cases where advertisements are distributed according to data subjects' preferences by analyzing information such as browsing history and purchase history:

  Good: Information such as browsing history and purchasing history acquired will be analyzed and used for advertisements related to new products and services according to your tastes.

  Bad: We will use it for advertising distribution.

- Cases where not only information acquired from resumes and interviews but also information such as online history (not assumed to be collected by the candidate) are analyzed and used for recruitment:

  Good: In addition to the resume and information obtained in the interview, online history and other information will be analyzed and the results will be used for recruiting activities.

  Bad: The acquired information will be used for recruiting activities.

- Cases where individuals' online history and other information are compiled and scored, and the score is provided to a third party without notifying the relevant data subjects:

  Good: Acquired online history and other information will be analyzed and scored. The score will be provided to a third party.

  Bad: The acquired information will be provided to a third party.

(3) Impact on Business Practices

The addition of the new matters to be disclosed leads directly to a necessity to review a business operator's privacy policy. While checking the contents of the proposed Guidelines in the future, it may be necessary not only to add the contents of measures taken for safety management but also to revise the description of the purpose of use. In particular, it is expected that business operators that conduct profiling, including the use of behavioral targeting advertising, will need to carefully consider how to express the purpose of use of the collected personal data.

IV. Reinforcing Regulations on Cross-Border Transfer

(1) Transfer of Personal Data to Overseas Third Parties with the Prior Consent of Data Subjects

Where a business operator is required to obtain the consent of a data subject prior to any cross-border transfer of personal data to a third party, the business operator is obliged to provide the data subject with information on the protection of personal information in the foreign country where the third party is located. The business operator is also obliged to inform the data subject of the measures implemented to protect personal information taken by the relevant third party and certain other similar information (Article 24(2) of the Amendment Act). With respect to the disclosure of that information to a data subject, the Proposed PPC Rules set out the ways in which that information should be provided as well as the particular details to be included.

(a) Methods of Disclosure of the Information

Business operators may provide the relevant information to a data subject in writing, by electronic means or by any

other appropriate method (Article 11-3(1) of the Proposed PPC Rules).

(b) Information to Be Provided

Article 11-3(2) of the Proposed PPC Rules stipulates that the following information must be provided to the relevant data subject:

(i) the country where the personal data will be transferred;

(ii) information on the system for the protection of personal information in the country where the personal data will be transferred, obtained by appropriate and reasonable methods; and

(iii) information concerning measures that will be taken by the third party recipient of the personal data in relation to the protection of personal information.

While the Proposed PPC Rules only outline the above matters at a high level, further concrete details have been discussed by the PPC in relation to the information to be provided on the protection of personal information in the country where the personal data will be transferred. Specifically, the PPC states that the following information must be provided:

- whether or not there is a system relating to the protection of personal information;
- existence of a certain index for a system relating to the protection of the personal information of the foreign country (e.g., a member of CBPR or reception of adequacy decision based on Article 45 of the GDPR);
- non-existence of obligations of business operators or rights of data subjects in compliance with the eight principles of OECD Privacy Guidelines (e.g., non-existence of restriction due to a utilization purpose or non-existence of restrictions on third-party provision); and
- existence of a system that may have a material impact on the rights and interests of a data subject (e.g., the existence of regulations regarding data localization or the existence of a system regarding government access).

Relatedly, the qualification that such information should only be "obtained by appropriate and reasonable methods" as described in sub-paragraph (ii) above may indicate the PPC's recognition that providing accurate and complete information on foreign data protection systems and keeping such information updated may impose an excessive burden on business operators.

In relation to the measures that will be taken by the recipient third party, according to the PPC, the Guideline will specify the information to be provided so that the data subject is able to recognize essential differences in measures required for protecting personal data between Japan and the foreign country. For example, in cases where the third party (transferee) has not disclosed the purpose of use, the transferring business operator will be obliged to provide that information.

(c) Exception to the Disclosure of the Required Information

(i) Exception 1: when the foreign country cannot be specified

Where the foreign country cannot be specified, the following information must be provided instead:

- the fact that the identity of the country cannot be specified and the reason therefor (Article 11-3(3)(i) of the Proposed PPC Rules); and
- information that could be used as a reference by the data subject when the foreign country cannot be specified, if any (Article 11-3(3)(ii) of the Proposed PPC Rules).

(ii) Exception 2: when the measures taken by the third party recipient are unknown

Where information concerning measures to be taken by the third party recipient for the protection of personal information cannot be provided, the reason for being unable to provide that information must be disclosed (Article 11-3(4) of the Proposed PPC Rules).

(2) Transfer of Personal Data to Overseas Third Parties with an Equivalent Data Protection Regime

As described above, under the Current Act, in principle, a business operator shall obtain the prior consent of a data subject when providing personal data to a third party in a foreign country. However, the business operator may provide personal data to a foreign third party without the prior consent of the data subject where the foreign third party has established a system that conforms to standards equivalent to those that a business operator under the Current Act is required to comply with concerning measures of personal data (the "Equivalent Measures") (Article 24 of the Current Act).

Under the Amendment Act, however, as an additional requirement, when personal data is provided to a foreign third party pursuant to the Equivalent Measures exception, the business operator is obliged to take necessary measures to ensure the continuous implementation of the Equivalent Measures by the third party and to provide the data subject with information on those necessary measures upon request pursuant to the Proposed PPC Rules (Article 24(3) of the Amendment Act).

(a) Necessary Measures to Ensure the Continuous Implementation of the Equivalent Measures by the Third Party

Under the Proposed PPC Rules, the following matters are prescribed as "necessary measures to ensure the continuous implementation of the Equivalent Measures" (Article 11-4(1) of the Proposed PPC Rules):

(i) Verifying, periodically and through appropriate and reasonable means, the implementation status of the Equivalent Measures by the third party and whether or not there is a system in the foreign country that is likely to affect the implementation of Equivalent Measures and, if so, the details of that system.

(ii) Taking necessary and appropriate measures if there is a hindrance to the implementation of the Equivalent Measures by the third party, and suspending the provision of the personal data to the third party when securing the continuous implementation of the Equivalent Measures becomes difficult.

The PPC has indicated that frequency of the business operator's verification (e.g., once a year) will be included in the Guideline.

(b) Information to Be Provided in Response to a Data Subject's Request

With respect to providing data subjects with information related to the applicable Equivalent Measures upon request, the Proposed PPC Rules prescribe the following methods to provide the information, the timeline for providing the information and the contents of the information to be provided.

- Methods to provide information: In writing, by electronic means, or any other appropriate method (Article 11-4(2) of the Proposed PPC Rules).
- Timeline: Upon request and without delay (Article 11-4(3) of the Proposed PPC Rules).
- Information to be provided: In principle, the information listed below (Article 11-4(3) of the Proposed PPC Rules).

(i) The method of establishing a system prescribed in Article 24(1) of the Amendment Act by the third party (e.g., the contracts with transferee, internal regulations or privacy policies commonly applied to transferor and transferee).

(ii) An outline of the Equivalent Measures implemented by the third party.

(iii) The frequency and method of the verification pursuant to Article 11-4(1)(i) of the Proposed PPC Rules.

(iv) The name of the foreign country.

(v) Whether or not there is a system in the foreign country that is likely to affect the implementation of Equivalent Measures by the third party.

(vi) Whether or not there is any hindrance to the implementation of Equivalent Measures by the third party.

(vii) An outline of the measures taken by the business operator pursuant to Article 11-4(1)(ii) of the Proposed PPC Rules relating to the hindrance of item (vi).

If the provision of information may materially hinder the business of the business operator, all or part of above matters may be withheld (Article 11-4(3) of the Proposed PPC Rules).

If a business operator decides not to provide all or part of the information above, it must notify the affected data subjects of that decision without delay and make efforts to explain the reasons for that decision (Article 11-4(4) and (5) of the Proposed PPC Rules).

(3) Impact on Business Practices

Up to now, cross-border data transfers between group companies have often been carried out lawfully under the Equivalent Measures exception. However, as additional requirements outlined above are imposed on business operators, such as the provision of more detailed information, the Equivalent Measures exception will likely become more onerous to use as a justification for cross-border data transfers. Specifically, considering that in some cases a data transfer is implemented only once and there is no continuing relationship between the transferor and transferee, the additional requirements under the Amendment Act could be excessive and too onerous and there is some doubt whether the amendments work practically. In the case of transfer of personal data to a business operator in Japan, the additional requirements will not apply; therefore the burden on the business operator regarding the provision of personal data to a third party will differ vastly depending on the location of the recipient (i.e., Japan or not). It is expected that there will be an increase in the number of cases where a transferor provides a transferee in a foreign country with personal data via a company located in Japan belonging to the transferee's corporate group.

Furthermore, it could be an overly onerous burden for most business operators to investigate systems for protecting personal information in foreign countries and provide that information to data subjects. If the Amendment Act intends to strictly enforce this provision of the regulation without imposing a prohibitive burden on business operators, we are of the opinion that the PPC, rather than each business operator, should conduct an exhaustive analysis of such foreign systems and provide business operators with the necessary information.

V. Development of Provisions for Service (*Sotatsu*) and Public Service (*Koji-sotatsu*)

Pursuant to an amendment to the Current Act in 2014, the major provisions of the Current Act became applicable to foreign business operators outside of Japan. However, foreign business operators remained outside of the scope of the provisions related to reporting and on-site inspections. The Amendment Act ensures that all provisions of the Current Act will be applicable to foreign business operators outside of Japan without limitation (Article 75 of the Amendment Act). According to the PPC, the purpose of this amendment is to remove the previous exceptions for foreign business operators and make clear that non-compliance may lead to penalties.

The Amendment Act establishes provisions concerning service (*sotatsu*) and service by publication (*koji-sotatsu*), either of which is required to be made prior to any administrative actions including requesting a report, requiring submission of materials, or the issuance of a recommendation or an order (Articles 58-2 to 58-5 of the Amendment Act). While the Amendment Act not only relates to foreign business operators, it is understood that the main purpose of the amendment is to avoid practical problems when implementing administrative actions against foreign business operators.

In this regard, Article 27 of the Proposed PPC Rules specifies the documents which require administrative actions to be implemented including requesting a report, requiring submission of materials, or the issuance of a recommendation or an order prescribed in Article 58-2 of the Amended Act. Article 28 of the Proposed PPC Rules prescribes that the methods of service by publication (*koji-sotatsu*) shall be, in principle, publication in an official gazette or a newspaper; and that in the case of service (*sotatsu*) outside of the territory of Japan, such service (*sotatsu*) may be given by a notice of the fact that service by publication (*koji-sotatsu*) has been made in Japan instead of by publication in an official gazette or a newspaper in that foreign country.

VI. Introduction of "Pseudonymized Information"

The Amendment Act introduces the concept of "Pseudonymized Information (*kamei-kako-jouho*)" in order to encourage analysis of data by business operators and to promote innovation by exempting data, which has been processed to remove the ability to identify personal information, from requests for provision or cessation of use by the data subject. The Amendment Act provides that "Pseudonymized Information" means information relating to an individual obtained by processing personal information after taking steps to make it impossible to identify a specific individual unless it is collated with other information (Article 2(9) of the Amendment Act).

The Proposed Order stipulates provisions to supplement the definition of "Pseudonymized Information Database, etc." in the Amendment Act. In addition, the Proposed PPC Rules establish: (i) processing standards for creating Pseudonymized Information; and (ii) safety management measures for preventing leakage of information on the processing methods used to generate the Pseudonymized Information.

VII. Introduction of Individual Related Information

The Amendment Act introduces the new concept of "Individual Related Information (*kojin-kanren-jouho*)". "Individual Related Information" refers to information concerning a living individual that does not fall under any of the defined

categories of personal information, Pseudonymized Information, or Anonymously Processed Information (*tokumei-kako-jouho*), and which is expected to be used as personal data after being transferred to a third party. A typical example of such data is online history not connected to a data subject's name, location information or cookies (Article 26-2(1) of the Amendment Act).

A business operator is obliged to check whether a data subject's consent has been obtained prior to transferring any Individual Related Information to a third party (Article 26-2(1) of the Amendment Act). A number of the provisions of the Amendment Act concerning the provision of personal data to a third party, and the related obligations to prepare and retain records, will also apply or apply *mutatis mutandis* to the provision of Individual Related Information to a third party.

With respect to Individual Related Information, prior to the publication of the Proposed Order and the Proposed PPC Rules, the PPC had already discussed the principle that business operators should, in the process of acquiring consent from the data subject, provide data subjects with sufficient information to ensure that the data subject has substantial opportunity to be fully informed; and business operators should obtain the express consent of the data subject only after the data subject has a full understanding of such information. Business operators will be well served to closely analyze the contents of the proposed revisions to the Guidelines, which are expected to clarify the scope and details of the regulations on Individual Related Information.

VIII. Strengthening the Rights of Data Subjects

(1) Designation of the Disclosure Method

A data subject may make a request to business operators for the disclosure of retained personal data by any of the means prescribed in the PPC Rules (Article 28(1) of the Amendment Act). Specifically, the Proposed PPC Rules will establish the following three methods (Article 18-6 of the Proposed PPC Rules).

(i) by electronic means;

(ii) in writing; or

(iii) by other methods specified by the business operator.

(2) Mandatory Disclosure of Confirmation Records regarding Provision of Personal Data to a Third Party

Under the Current Act, business operators are obliged to confirm certain matters and keep records when providing personal data to a third party or receiving personal data from a third party (Article 25 and 26 of the Current Act). The Amendment Act provides that data subjects are entitled to request the disclosure of such records (Article 28(5) of the Amendment Act). In this regard, Article 9 of the Proposed Order prescribes four exclusions where a business operator may refuse to disclose that information, including cases where disclosure is likely to result in harm to the life, body or property of the data subject or a third party.

IX. Concluding Remarks

The content of the Proposed Order and the Proposed PPC Rules include a large number of matters which could require business operators to reconsider their existing practical treatment of personal data, as well as the scope and contents of their privacy policies. It will be necessary for each company to examine how the Proposed Order and the Proposed PPC Rules may impact their own business and consider whether any additional measures are required. Business operators will likely need to seek guidance from Japanese legal professionals to comply with the new legally binding reporting obligations and ensure that all necessary reports and notices are made when the relevant situation arises.

In addition, foreign companies exchanging personal data with Japanese companies will need to provide Japanese companies with information necessary for Japanese companies to comply with the equivalent laws and regulations, such as the personal information protection system of their own country. Although the PPC already conducts investigations on foreign companies, there is a possibility that number of investigations into foreign companies will increase due to the revisions to the regulations regarding service (*sotatsu*). While there is no system in Japan for high sanctions, such as in the GDPR, or private lawsuits, such as in the CCPA; awareness of individuals' rights regarding personal information is steadily increasing in Japan. For foreign companies conducting business in Japan, a sound understanding of the provisions of the Amendment Act, as well as the Proposed Order and the Proposed PPC Rules, will be essential to ensuring that they and their Japanese business partners comply with Japanese data protection regulations in Japan.

NAGASHIMA OHNO & TSUNEMATSU

www.noandt.com

JP Tower, 2-7-2 Marunouchi, Chiyoda-ku, Tokyo 100-7036, Japan
Tel: +81-3-6889-7000 (general) Fax: +81-3-6889-8000 (general) Email: info@noandt.com

Nagashima Ohno & Tsunematsu is the first integrated full-service law firm in Japan and one of the foremost providers of international and commercial legal services based in Tokyo. The firm's overseas network includes offices in New York, Singapore, Bangkok, Ho Chi Minh City, Hanoi and Shanghai, and collaborative relationships with prominent local law firms throughout Asia and other regions. The over 500 lawyers of the firm, including about 40 experienced foreign attorneys from various jurisdictions, work together in customized teams to provide clients with the expertise and experience specifically required for each client matter.