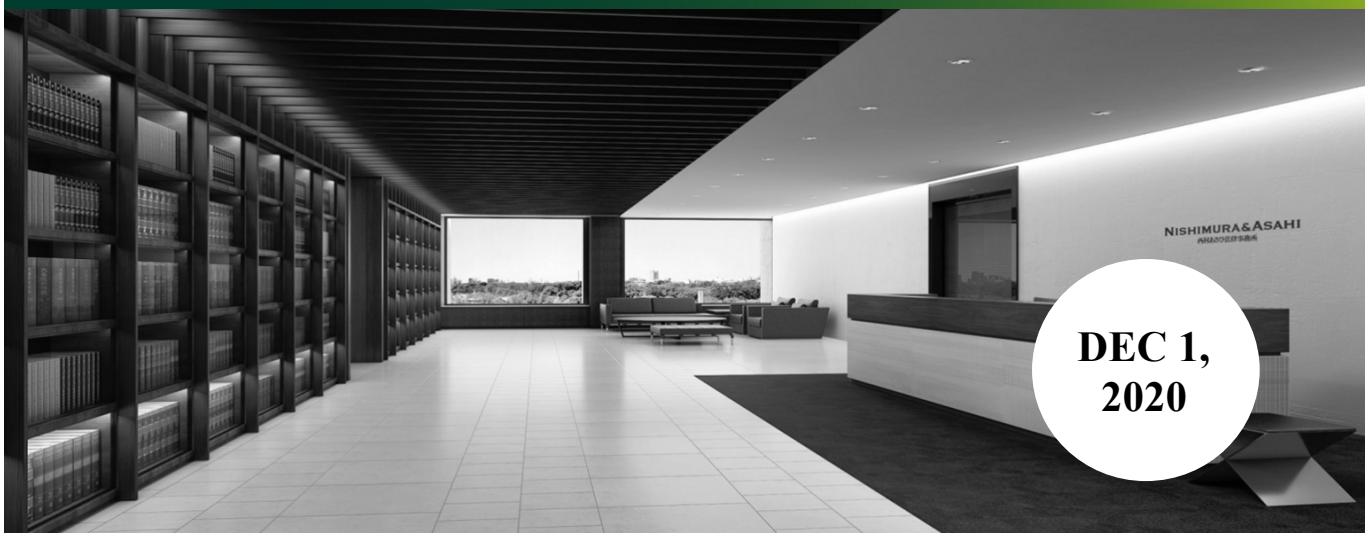
西村あさひ法律事務所

NISHIMURA & ASAHI

Data Protection Newsletter



The 2020 Amendment to the Act on the Protection of Personal Information of Japan

Noriya Ishikawa, Yujin Suga, Mitsuhiro Yoshimura

The 2020 amendment to the Act on the Protection of Personal Information of Japan (the Act itself, "**APPI,**" and this amendment, "**2020 Amendment**") was enacted on 5 June 2020, published on 12 June 2020, and is expected to enter into force within 2 years of the publication date (i.e., by 12 June 2022). The specific date of entry into force has not been determined yet, but will likely be between April and June of 2022.

Japanese legislators have delegated the power to establish the details of the 2020 Amendment, via ministerial ordinances, to the Personal Information Protection Commission ("**PPC**"), the Japanese data protection authority. The PPC is currently preparing its ordinances, which are expected to be published in the months to come. The 2020 Amendment will also affect a series of guidelines and Q&A that the PPC has issued in the past. Although these guidelines and Q&A generally are not legally binding, they have played an important role in Japanese data protection practice, given that the guidelines set out practical, specific rules that are not specified in the text of the APPI. The PPC is also revising its current guidelines and Q&A to reflect the content and enactment of the 2020 Amendment.

Below, we will elaborate on the primary impact of the 2020 Amendment, which may affect the operations of business providers both within and outside of Japan. More practical and specific rules relating to the 2020 Amendment will be available once the PPC ministerial ordinances, and the guidelines and Q&A currently being revised by the PPC, are published.

1. Duty to notify the PPC of data breaches

The current version of the APPI does not establish a legal obligation to notify the PPC of a data breach, in contrast to the data breach notification obligation set out in Article 33 of the GDPR. While the current notification regarding how to respond to a data breach, which was issued by the PPC in 2017 (Notification No. 1 of 2017), encourages a Personal Information Controller (i.e., a business operator that uses a personal information database for its business purposes) to notify the PPC in the event of a data breach, and to communicate the breach to relevant data subjects, prior to the 2020 Amendment, this encouragement was not a legal requirement.

The 2020 Amendment replaced the current framework with legally binding and enforceable notification and communication obligations. Article 22-2 of the amended APPI essentially states that where any leak or loss of, or damage to, Personal Data processed by a Personal Information Controller, or any other incident concerning the security of Personal Data (each, a "**Data Breach Incident**") occurs, the Personal Information Controller is required:

i. to notify the PPC of the Data Breach Incident, in accordance with the relevant PPC ministerial ordinances; and
ii. to communicate the Data Breach Incident to the relevant data subjects, in accordance with the relevant PPC ministerial ordinances.

A Personal Information Controller is exempt from the duty to communicate the Data Breach Incident to data subjects where it is "difficult" for the Personal Information Controller to do so, and where the Personal Information Controller implements "alternative measures," as required to protect the data subjects' rights and interests. Examples of cases where it would be deemed "difficult" to communicate the incident to data subjects include situations where the relevant personal data do not contain the contact details of the relevant data subjects, or where the relevant contact details are not up-to-date, and the Personal Information Controller cannot reach out to the relevant data subjects based on the data the Personal Information Controller retains. The details of the "alternative measures" that must be taken will likely be specified in the PPC guidelines currently being revised.

In addition, when a Personal Information Controller is entrusted by another Personal Information Controller with processing of Personal Data belonging to the entrusting party, the Personal Information Controller may be exempt from the duty to notify the PPC and communicate the Data Breach Incident to data subjects, if the entrusted party notifies the entrusting party of the incident.

Unlike the rules under the GDPR, the 2020 Amendment does not set forth a concrete time limit within which a Personal Information Controller must notify and communicate concerning the Data Breach Incident. The PPC is considering the establishment of a two-stage deadline applicable to the initial report and final report. The relevant PPC ministerial ordinances will stipulate that the initial reports must be made "promptly," without setting a clear time limit, although the guidelines will likely provide some elements about the timing of making these initial reports, for reference purposes. Taking into account the amount of time that it would normally take to ascertain the facts, the PPC is currently considering whether or not a certain time limit (e.g., 30 days) should be set for filing of the final report. In addition, the PPC may stipulate extended deadlines (e.g., 60 days) for some types of data breaches, such as a data leakage caused by fraudulent actions.

Failure to comply with the duties of notification and communication may lead to a recommendation, a cease-and-desist order, and/or publication of the APPI violation.

2. Creation of a concept covering cookie information and location data

The concept of "Personal Data," as defined in the current version of the APPI, usually does not cover cookies and location data. To address this issue, the 2020 Amendment created a new category of information, called "**Individual Related Information**" (*kojin kanren jouhou*). Individual Related Information is defined as "*information relating to a living individual, which qualifies as neither Personal Information, Pseudonymised Information, nor De-identified Information*" (Article 26-2 of the amended APPI, Paragraph 1). According to the review by the Japanese legislators, Individual Related Information generally includes cookies and location data, but excludes statistical information.

Where a business operator that has collected Individual Related Information aims to disclose the Individual Related Information to a third party, and the third party is expected to be able to identify one or more specific individuals by using the Individual Related Information collected by the business operator, the business operator must not disclose the Individual Related Information to the third party unless the business operator confirms with the third party that the following requirements are met (Article 26-2, Paragraph 1 of the amended APPI):

i. the third party has obtained consent from the specific individuals for the third party's receipt of the Individual Related Information from the business operator, and for the use of that information to assemble Personal Data; and
ii. where the third party is located outside of Japan, the third party has provided the specific individuals with (i) a summary of the legal system for protection of personal information in the foreign country where the third party is located, (ii) an outline of specific measures to protect personal information which are or will be taken by the receiving person or entity; and (iii) other information that may be helpful to the relevant data subjects, before obtaining the consent for the third party's receipt of the Individual Related Information from the business operator.

The third party receiving the information must not falsify its answer to the business operator in the verification described above (Article 26-2, Paragraph 3 of the amended APPI). In addition, a business operator is generally required to keep records relating to the verification, including the date and details of the verification (Article 26-2, Paragraph 3 of the amended APPI).

The APPI does not specify any practical steps for the verification process to be conducted by a business operator, or for the consent that must be obtained by a third party recipient. For more details, it will be necessary to review the ministerial ordinances and amended guidelines to be published by the PPC.

3. More stringent cross-border transfer rules

The 2020 Amendment has introduced an enhanced framework to protect Personal Data in the context of a transfer of Personal Data to a person or entity outside of Japan. It has introduced new obligations for Personal Information Controllers to disclose the following matters to the relevant data subjects when the Personal Information Controller intends to obtain consent from those relevant data subjects for a transfer of Personal Data to a person or entity outside Japan (Article 24, Paragraph 2 of the amended APPI):

i. a summary of the legal system for protection of personal information in the foreign country to which Personal Data will be transferred;
ii. an outline of specific measures to protect personal information which are being or will be taken by the receiving person or entity; and
iii. other information that may be helpful to the relevant data subjects.

These rules will be applicable only to consents for cross-border transfer obtained on and after the date the 2020 Amendment enters into force. The PPC guidelines currently being revised will likely specify details regarding what level of summary of the legal system will be required and how detailed the outline of specific measures should be.

4. Prohibition of processing of Personal Information in an illicit manner

The 2020 Amendment has also introduced a new obligation that requires a Personal Information Controller not to process Personal Information in a manner that may facilitate or induce illegal or otherwise unjust activities (Article 16-2 of the Amended APPI).

While the concept of a "manner that may facilitate or induce illegal or otherwise unjust activities" may cover a broad range of processing activities, the preparatory documents and other materials suggest that this concept may typically include: (i) an abusive use of Personal Information that has been made public, and (ii) an abusive use of Personal Information collected by a digital platformer that has a dominant position in the market. In addition, it is important to note, in relation to the GDPR, that practitioners have pointed out this concept may also cover excessive profiling of individuals. While the PPC's ministerial ordinances and guidelines, currently being revised, will likely provide more details, this concept may be used to cover "gray zone" processing that is regulated under the GDPR or other foreign regulations, but was not regulated under the APPI.

5. Practical steps to deal with the 2020 Amendment

As described above, the 2020 Amendment is expected to enter into force between April and June of 2022, and many details regarding the amendment remain to be determined by the PPC's ministerial ordinances, guidelines and Q&A. However, while business operators that are subject to the APPI should pay attention to the upcoming publication of the PPC's ministerial ordinances and amended guidelines and Q&A, and other expected developments, business operators already may start to consider taking practical steps to comply with the 2020 Amendment. These practical steps may include: (i) setting up new or revised internal systems and rules to comply with the duty of notification and communication regarding Data Breach Incidents, (ii) revision of data processing agreements to address the duty of notification and communication regarding Data Breach Incidents, (iii) conducting data mapping to analyze whether any new measures will be needed to comply with the new rules concerning the processing of Individual Related Information, (iv) where a business provider is likely to be subject to the regulations regarding Individual Related Information, revising internal policies to include procedures for verification with potential third party recipients, (v) where a business provider transfers Personal Data to locations outside Japan, revising internal policies and privacy policies to comply with the enhanced cross-border transfer rules, etc.

Noriya Ishikawa
Partner, Frankfurt & Düsseldorf Offices Co-Representative
E-mail: n_ishikawa@jurists.co.jp

Noriya Ishikawa serves as co-representative of our offices in Frankfurt and Düsseldorf, Germany. He advises national and international clients from various industries, in particular with regard to projects involving multi-national data protection law issues, such as drafting policies, data transfer agreements, and outsourcing agreements, as well as IT compliance questions and data breach issues. He won first prize in the "Most Successful Lawyers in 2019 in the Area of Data Protection" sponsored by NIKKEI Inc. (a Japanese media and newspaper publishing organization).

Yujin Suga
Attorney-at-Law
E-mail: y_suga@jurists.co.jp

Yujin Suga is a senior associate at Nishimura & Asahi. With extensive experience in European legal practice, he advises clients in various industries on data protection laws in a range of jurisdictions, including Japan, the EU and the US. He is fluent in English and French, and provides legal advice and assistance to Japanese and international clients.

Mitsuhiro Yoshimura
Attorney-at-Law
E-mail: m_yoshimura@jurists.co.jp

Mitsuhiro Yoshimura is an associate at Nishimura & Asahi. He advises clients in various industries across the world, with experience working at Japanese and international law firms and in multiple fields of law, including intellectual property, data protection, and regulation of pharmaceuticals and medical devices; he speaks English, French, and Japanese.