NEWSLETTER

Data Incidents Subject to Reporting under the Amended Enforcement Rules for the Act on the Protection of Personal Information

Data Protection Newsletter March 5, 2024

Author:
Yuko Kawai
y.kawai@nishimura.com
Haruka Oshio
h.oshio@nishimura.com

1. Introduction

The Amendment to Part of Enforcement Rules for the Act on the Protection of Personal Information (Rules of the Personal Information Protection Commission No. 5) (the "**Amended Enforcement Rules**") was promulgated along with the Amendment to the Relevant Guidelines (the "**Amended Guidelines**") on December 27, 2023. Both amendments were open for public comment from September 14, 2023 to December 27, 2023 (the "**Public Comments**"). The Amended Enforcement Rules will come into force on April 1, 2024 (the "**Enforcement Date**").

The Amended Enforcement Rules expand the scope of data breach incidents that must be reported to the Personal Information Protection Commission of Japan (the "**PPC**") and notified to the affected data subjects. Also, the Amended Guidelines provide interpretations of the expanded scope along with some specific examples, among other matters.

2. Outline of Data Incidents Subject to Reporting under the APPI (pre-amendment)

Under the Act on the Protection of Personal Information of Japan (the "**APPI**"), when any of the following types of leakage (including access) or loss of, or damage to, "personal data" (excluding personal data for which highly advanced encryption or other necessary measures to protect the data subject's rights and interests has been implemented) (collectively, "**Leakage**") occurs, may occur, or may have occurred (in each case, a "**Data Incident Subject to Reporting**"), in principle, a "business operator" is legally required to report the Data Incident Subject to Reporting to the PPC and notify the data subjects affected thereby (the "**Report and Notification Obligation**"), regardless of whether the business operator caused the Leakage intentionally or negligently.[1]

Leakage of personal data that:

(a) contains special care-required personal information;[2]
(b) is likely to cause proprietary damage as a result of its unauthorized use;
(c) may have been conducted for a wrongful purpose; or
(d) involves the personal data of more than 1,000 data subjects.

In this regard, the APPI defines a "business operator" as a business operator using a personal information

[1] Article 26 (1) and (2) of the APPI and Article 7 of the current Enforcement Rules for the Act on the Protection of Personal Information.

[2] Special care-required personal information is defined under Article 2 (3) of the APPI.

database[3] for its business.[4] As such, the APPI does not exclude foreign entities from the definition of a "business operator", and therefore, they may be subject to the Report and Notification Obligation. Even if foreign entities do not have the same type of obligation under the laws or regulations in the jurisdictions of other countries, this does not mean that they are exempted from the Report and Notification Obligation under the APPI in Japan.

Also, in the APPI, "personal data" is defined separately from "personal information", as "personal information constituting a personal information database".[5] In other words, "personal data" is a narrower concept than "personal information".

3. Changes Made under the Amended Enforcement Rules

The Amended Enforcement Rules have expanded the scope of (c) in 2. above.

More specifically, if a Leakage of not only personal data, but also personal information that a business operator has obtained or is about to obtain and intends to handle as personal data may have occurred, the business operator is subject to the Report and Notification Obligation.[6] This means that a Leakage of information that is not yet actually obtained by a business operator may still be subject to the Report and Notification Obligation. This feature differentiates the Report and Notification Obligation under the Amended Enforcement Rules from the previous rule under which a business operator was only subject to the Report and Notification Obligation with regard to personal data in the business operator's possession. According to the Amended Guidelines, the mere fact that a business operator intends to enter personal information into a personal information database is sufficient to satisfy the requirement that "a business operator intends to handle information as personal data", even if the business operator intends to eventually process such personal information into statistical information (which constitutes neither personal information nor personal data).

However, it should be noted that the Amended Enforcement Rules state that a Leakage in the scope of (c) in 2. above must be caused by an act toward a business operator[7] which may have been conducted for a wrongful purpose. Accordingly, the mere fact that a phishing fraud site exists is unlikely to trigger the Report and Notification Obligation for a business operator, since there is no "act toward a business operator which may have been conducted for a wrongful purpose."

The Amended Guidelines provide some specific examples that may fall under the new scope of (c) in 2. above, including the following case:

---

[3] Which means an assembly of information systematically arranged in such a way that specific personal information can be retrieved by a computer, or an assembly of information designated by a cabinet order as being systematically arranged in such a way that specific personal information can be easily retrieved. Article 16 (1) of the APPI.

[4] Article 16 (2) of the APPI.

[5] Article 16 (3) of the APPI.

[6] Articles 7 (iii) and 8 (1)(ii) of the Amended Enforcement Rules.

[7] For this purpose, the Amended Guidelines explain that a business operator's data processors and other third parties whose services are used by a business operator when handling personal data are included in the scope of "a business operator".

A third party has falsified a link or button on a business operator's website that directs a user to a fake input page, and as a result of the user clicking on the link or button, the user is directed to the fake input page and the personal information entered by the user on the fake input page is transmitted to the third party, where such information was intended to be entered into the business operator's personal information database.

Also, the PPC's following answer to the Public Comments clarifies how to interpret the new scope of (c) in 2. above (in response to a situation where a business operator's employee regularly uses business card management software to manage business cards, and whose bag containing business cards was stolen before personal information on the business cards was registered in the business card management software):

Although analysis is necessary on a case-by-case basis, in general, if the business card management software constitutes a personal information database as defined in the APPI, then the personal information on the business card that is to be registered in the business card management software is likely to constitute "personal information that a business operator intends to handle as personal data", and the theft of the business cards (along with the employee's bag) also is likely to constitute "an act toward a business operator which may have been conducted for a wrongful purpose".

In contrast, the PPC's answer to the Public Comments suggests that an employee of a business operator accidentally losing business cards (for example, by misplacing them) does not constitute "an act toward a business operator which may have been conducted for a wrongful purpose".

4. Outline of the Report and Notification Obligation

(1) Report to the PPC

There is a two-stage deadline for filing initial reports and final reports. After someone at the business operator becomes aware of a Data Incident Subject to Reporting, the business operator must (i) promptly (within approximately within three to five days) report to the PPC the details of the matter that the business operator is aware of at the time of the report ("**Initial Report**"), and (ii) make a final report to the PPC within 30 days (or, in the case of (c) in 2. above, 60 days) ("**Final Report**").[8] Both reports must be made in Japanese using the PPC's online form.

The Final Report must include the following information:[9]

- an outline of the Data Incident Subject to Reporting;
- the types of personal data affected (including personal information that a business operator has obtained or is about to obtain and intends to handle as personal data, in the case of (c) in 2. above);
- the number of affected data subjects;
- the cause(s) of the Data Incident Subject to Reporting;
- whether any secondary damage has occurred or is likely to occur, and if so, the details thereof;

[8] Article 26 (1) of the APPI and Article 8 (2) of the Amended Enforcement Rules.

[9] Article 8 (1) of the Amended Enforcement Rules.

- the status of implementation of communications with the affected data subjects and a public announcement;
- the measures for preventing recurrence; and
- other various matters.

(2) Notification to Data Subjects

After someone at the business operator becomes aware of a Data Incident Subject to Reporting, the business operator also must notify data subjects promptly (the APPI does not stipulate any specific timeline) and provide them with an outline of the Data Incident Subject to Reporting to the extent necessary to protect the data subjects' rights and interests (depending on the circumstances of the Data Incident Subject to Reporting).[10] In certain cases, for example, where the business operator cannot reach data subjects due to the absence of contact information, the business operator may make information about the Data Incident Subject to Reporting publicly available, or establish a contact point and disclose the contact's information, instead of making individual notifications to the relevant data subjects. However, in principle, individual notification must be provided to the affected data subjects, and public announcement (such as a press release) cannot replace such notification.

The notification must include the following information:[11]

- an outline of the Data Incident Subject to Reporting;
- the types of personal data affected (including personal information that a business operator has obtained or is about to obtain and intends to handle as personal data, in the case of (c) in 2. above);
- the cause(s) of the Data Incident Subject to Reporting;
- whether any secondary damage has occurred or is likely to occur, and if so, the details thereof; and
- other various matters.

5. Sanctions

Under the APPI and its relevant guidelines, no administrative fines or criminal penalties are immediately imposed on a business operator due to its failure to submit an Initial Report to the PPC within five days from the occurrence of the Data Incident Subject to Reporting.

However, depending on the details of the Data Incident Subject to Reporting and the time of actual submission of the Initial Report, the PPC may submit inquiries to the business operator, issue guidance (*shido*), advice (*jogen*), or a recommendation (*kankoku*) to the business operator for violations of the APPI, and/or also order them to take certain necessary measures.[12]

6. Leakage subject to the Amended Enforcement Rules

According to the PPC answer to the Public Comments, the Amended Enforcement Rules apply to Leakages

[10] Article 26 (2) of the APPI and Article 10 of the Amended Enforcement Rules.

[11] Article 10 of the Amended Enforcement Rules.

[12] Articles 147 and 148 of the APPI.

that have occurred, or may have occurred on and after the Enforcement Date. In order to correctly and promptly determine whether the Report and Notification Obligation is applicable in the case where a Data Incident Subject to Reporting has occurred or may have occurred, it is necessary to fully understand the Amended Enforcement Rules and Amended Guidelines.

Public Relations Section, Nishimura & Asahi newsletter@nishimura.com