International Law Office

Data protection regulation amendments: data breach reporting and notification obligations

19 March 2021 | Contributed by Nagashima Ohno & Tsunematsu

Introduction
Reporting and notification obligations
PPC reporting obligation
Data subject notification obligation
Effect on business practices

AUTHORS

Oki Mori

Keiji Tonomura

Emi Fujisaki

Naoki Fukumoto

Introduction

On 12 June 2020 the Diet promulgated the Amendment Act of the Act on the Protection of Personal Information, which will come into force by June 2022.(1) Many of the act's provisions have been delegated to subordinate regulations, including:

- the Cabinet Order to Enforce the Act on the Protection of Personal Information; and
- the Personal Information Protection Commission's (PPC's) Enforcement Rule for the Act on the Protection of Personal Information.

In December 2020 further proposed amendments to these regulations were published.(2) This article outlines the effect that these proposed amendments will have on businesses' reporting and notification obligations where data breaches occur. From June 2021 onwards, further guidelines will be published.

Reporting and notification obligations

Under the Act on the Protection of Personal Information, while businesses are encouraged to report data breaches to the PPC or other supervisory authorities, they are not legally obliged to do so. Nor are they obliged to notify affected data subjects, even where personal data is leaked or accessed without authorisation.

Article 22-2(1) of the amendment act establishes new legally binding obligations on businesses to report personal data breaches to the PPC where they have handled such data in certain situations. Article 22-2(2) of the amendment act further states that in these situations, businesses must also notify any affected data subjects of the breach.

The proposed PPC rule amendment contains further details of these new obligations, regarding:

- the situations in which the reporting and notification obligations apply;
- the mandatory reporting and notification time limits;
- the matters that businesses should report to the PPC and which affected data subjects should be notified about; and
- the reporting and notification methods.

PPC reporting obligation

Situations that trigger the reporting obligation

The proposed PPC rule amendment classifies the occurrence or likely occurrence of the following situations as highly likely to harm data subjects' rights and interests:

- a breach of personal data which requires special care(3) (Article 6-2(i) of the proposed PPC rule amendment);
- a data breach that may cause financial damage due to unauthorised use of the breached data (Article 6-2(ii) of the proposed PPC rule amendment);
- a data breach that may have been committed with a malicious purpose (Article 6-3(iii) of the proposed PPC rule amendment); and

- a data breach that affects more than 1,000 data subjects (Article 6-3(iv) of the proposed PPC rule amendment).

However, according to Article 6-2(i) of the proposed PPC rule amendment, businesses are not obliged to report data breaches to the PPC where there are measures in place to protect the data subjects' rights and interests (eg, advanced encryption).

According to the PPC, the first and second situations listed above concern the nature of the breached personal data, while the second and third situations concern the manner and scale of the data breach, respectively.

It is assumed that breaches of credit card numbers, internet banking IDs and passwords apply to the second situation. Cases where the third situation applies must be reported because of the high risk of further improper use of the personal data.

Time restrictions on reporting

Unlike the EU General Data Protection Regulation (GDPR), the amendment act includes no time restrictions for reporting to the PPC.

However, the proposed PPC rule amendment separates the PPC reporting obligation into two categories – namely:

- prompt reporting; and
- confirmatory reporting.

The proposed PPC rule amendment states that businesses must make both a prompt report and a confirmatory report.

According to Article 6-3(1) of the proposed PPC rule amendment, businesses must report to the PPC promptly on learning of an applicable situation. The guidelines are expected to provide further clarification on the definition of 'prompt'.

According to Article 6-3(2) of the proposed PPC rule amendment, businesses must provide a confirmatory report within 30 days of learning of an applicable situation. Where a data breach may have been committed with a malicious purpose, businesses must provide a confirmatory report within 60 days of learning of the breach.

Information to be reported

The information that businesses must report to the PPC and notify affected data subjects about, according to Articles 6-3(1) and 6-4 of the proposed PPC rule amendment, is shown in the following table.

Information	Report to the PPC?	Notify affected data subjects?
A description of the data breach	Yes	Yes
The personal data items that have been affected by the data breach	Yes	Yes
The number of data subjects affected	Yes	Not applicable
The cause of the data breach	Yes	Yes
Whether there has been or is likely to be further improper use of the personal data and, if so, details of that further improper use	Yes	Yes
The status of measures taken in relation to the affected data subjects	Yes	Not applicable
Whether public announcements have been or will be made concerning the data breach	Yes	Not applicable
Any remedial measures that have been taken since the data breach	Yes	Yes
Other relevant details	Yes	Yes

Reporting method

Article 6-3(3)(i) of the proposed PPC rule amendment states that businesses will be able to submit reports to the PPC online.

Exemptions from PPC reporting obligations for trustees

Where a trustee to whom a business has entrusted the handling of personal data (similar to a 'processor' under the GDPR) causes a data breach, both the trustee and the trustor (similar to a 'controller' under the GDPR) must, in principle, report the breach to the PPC. However, according to Article 22-2(1) of the amendment act, the trustee need not report the data breach to the PPC if it notifies the trustor of the data breach.

According to Article 6-4 of the proposed PPC rule amendment, the trustee must promptly notify the trustor of any relevant details on learning of an applicable situation. The trustee must continue investigating the situation and cooperating with the trustor in reporting the breach to the PPC.

Data subject notification obligation

Situations that trigger the notification obligation
According to Article 22-2(2) of the amendment act, where a business must report a data breach to the PPC, it must also notify all affected data subjects. However, unlike the reporting obligation, businesses may be exempt from the notification obligation where it is difficult to notify the data subjects, provided that sufficient alternative measures are taken to protect their rights and interests. The proposed PPC rule amendment is unclear as to the actions or measures that are sufficient for businesses to rely on this exemption.

Time restrictions on notification
Article 6-5 of the proposed PPC rule amendment stipulates that businesses must notify all affected data subjects promptly after learning of a situation that it must report to the PPC, "according to the circumstances". As such, businesses need not notify the affected data subjects when they report the matter to the PPC. This is presumed to be in recognition of the fact that while businesses must notify 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 subjects.

Information about which data subjects must be notified
The proposed PPC rule amendment states that businesses should notify affected data subjects of data breaches "to the extent necessary to protect the rights and interests of the data subjects". (For the information that businesses should disclose to affected data subjects, please see " Information to be reported" above.)

Notification method
The proposed PPC rule amendment gives no information on how businesses should notify affected data subjects.

Effect on business practices

The range of situations that businesses must report under the proposed PPC rule amendment is narrower than that under the Act on the Protection of Personal Information. However, businesses may submit voluntary reports to the PPC in situations that do not fall under the mandatory reporting categories. Businesses must determine whether to report breaches on a case-by-case basis. For example, where a business expects there to be an external enquiry about why it has not a made public data breach announcement, it may elect to report the breach to the PPC voluntarily and explain to the enquiring party that it is seeking guidance and will respond appropriately.

For further information on this topic please contact Oki Mori, Keiji Tonomura, Emi Fujisaki or Naoki Fukumoto at Nagashima Ohno & Tsunematsu by telephone (+81 3 6889 7000) or email (oki_mori@noandt.com, keiji_tonomura@noandt.com, emi_fujisaki@noandt.com or naoki_fukumoto@noandt.com). The Nagashima Ohno & Tsunematsu website can be accessed at www.noandt.com.

Endnotes

(1) For further information please see "Amendment Bill of the Act on the Protection of Personal Information".

(2) The amendments will be promulgated between mid-February and early April 2021. Their enforcement date will be specified by a Cabinet Order and announced on the PPC website.

(3) The concept of personal data that requires special care under Article 2(3) of the Act on the Protection of Personal Information is similar to the special categories of personal data that are stipulated in the GDPR.