TECH, DATA, TELECOMS & MEDIA - JAPAN

Act on the Protection of Personal Information amended

17 April 2020 | Contributed by Nagashima Ohno & Tsunematsu

AUTHORS

Oki Mori

Tomoharu Hagiwara

Naoki Fukumoto

Introduction

On 10 March 2020 a bill to amend part of the Act on the Protection of Personal Information (Amendment Bill) was submitted to the Japanese Diet. The Amendment Bill's main provisions will come into force within two years from the date of their promulgation.

This article examines the parts of the Amendment Bill which are expected to have a significant impact on ongoing business practices.

Reinforcing obligations on business operators

Obligation to report data breaches to PPC and individuals

Obligation to report to PPC

Under the Act on the Protection of Personal Information, business operators are not legally obliged to report data breaches (eg, the leakage of personal data) to the Personal Information Protection Committee of Japan (PPC) or the affected data subject. The PPC's pronouncement specifies that business operators should make efforts to report data breaches to the PPC or other supervising authorities. However, this is not legally binding.

Article 22-2(1) of the Amendment Bill prescribes that business operators will be legally obliged to report to the PPC certain events relating to the breach of security of personal data handled by business operators (eg, the leakage, loss or damage of data) which is likely to harm the rights and interests of data subjects. Unlike the obligations under the EU General Data Protection Regulation (GDPR) to report to supervisory authorities, the Amendment Bill includes no time restriction for reporting to the PPC.

As a side note, 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 a data processor under the GDPR), the trustee will not be obliged to report the data breach to the PPC provided that the trustee notifies the trustor (a concept similar to a data controller under the GDPR) of the data breach (Article 22-2(1) of the Amendment Bill).

Further details of this reporting obligation, including the contents and timing of the report, will be provided under the PPC rules.

Obligation to notify data subjects

Under Article 22-2(1) of the Amendment Bill, when a business operator must report a data breach to the PPC, they must also notify the data subject. However, where it is difficult to notify data subjects, business operators may be exempted from doing so provided that necessary alternative action is taken to protect the data subject's rights and interests (Article 22-2(2) of the Amendment Bill). While further details will be provided under the PPC rules, the PPC explains that such alternative measures may include making a public announcement and inviting enquiries from potentially affected data subjects.

Obligation of proper use

Article 16-2 of the Amendment Bill prescribes that business operators are prohibited from using personal information in a manner that encourages or is likely to encourage illegal or improper conduct. Although the language here is vague, it is expected that the PPC will issue guidance to clarify the interpretation of this article so that it has no detrimental effect on business operators.

Reinforcing opt-out regulations

Addition of matters to be disclosed for opt-out

Under Article 23(1) of the Act on the Protection of Personal Information, a business operator must obtain the consent of data subjects when the business operator provides personal data to a third party under the act. However, there are some exceptions including the opt-out method where a business operator must meet certain requirements (eg, notifying the PPC of certain matters prescribed in the act and the PPC rules (Article 23(2) to (4) of the Act on the Protection of Personal Information)). The Amendment Bill adds the following information to the matters that are required to be disclosed to the PPC and announced to the public (or notified to the data subject) when seeking to use the opt-out method:

- The business operator's name and address and the name of the business operator's representative that provides personal data to a third party (Article 23(2)(i) of the Amendment Bill).
- A method of acquiring personal data to be provided to a third party (Article 23(2)(iv) of the Amendment Bill).
- Other necessary matters prescribed by the PPC rules for protecting the rights and interests of data subjects (Articles 23(2) and 23(8) of the Amendment Bill).

Limitation of personal data subject to opt out

The Amendment Bill limits the categories of personal data that can be provided to third parties when using the opt-out method. Specifically, the following data cannot be provided to a third party (Article 23(2) of the Amendment Bill):

- Special care-required personal information (similar to the generally understood concept of sensitive data under the GDPR).
- Personal data acquired in violation of Article 17(1) (Proper Acquisition) of the Act on the Protection of Personal Information.
- Personal data provided by other business operators through the opt-out method.

Addition of matters to be disclosed by business operators

Addition of matters to be disclosed concerning retained personal data

Under the Act on the Protection of Personal Information, a business operator must disclose to the public certain matters concerning retained personal data. The Amendment Bill adds certain items to the disclosure list, including the address of the business operator and the name of the business operator's representative, as matters to be disclosed (Articles 27(1)(i) and 27(1)(iii) of the Amendment Bill). At the same time, the relevant cabinet order is expected to be revised and the PPC has indicated that, under the amended cabinet order, additional matters will also be added, such as the system for handling personal information, the measures taken concerning personal information and the method of processing retained personal data. As a practical matter, the contents of the cabinet order with regard to the matters required to be disclosed will likely have a greater impact on business operators than the content of the amendment bill itself and many business operators will subsequently need to revise their privacy policies to comply.

Addition of matters to be disclosed concerning joint use

Under the Act on the Protection of Personal Information under the joint use exception, it is possible to provide personal data to a third party without the prior consent of the data subject. When seeking to take advantage of this exception, a business operator must notify the data subjects of the name of the person responsible for controlling the personal data or disclose the name of that person in a readily accessible location, such as posting it on the Internet (Article 23(5)(iii) of the act). The Amendment Bill adds the address of the business operator and the name of their representative as matters to be notified in advance to data subjects or disclosed publicly (Article 23(5)(iii) of the Amendment Bill). Many business operators using the joint use exception will have to revise their privacy policies to comply with these amendments.

Expansion of range of extraterritorial application

Pursuant to an amendment to the Act on the Protection of Personal Information in 2014, the major provisions of the act became applicable to foreign business operators outside Japan. However, foreign business operators remained outside of the scope of the provisions relating to reporting and on-site inspections under the act. The Amendment Bill allows for all provisions of the act to be

applied to foreign business operators outside of Japan without limitation (Article 75 of the Amendment Bill). According to the PPC, the purpose of this amendment is to remove the exception for foreign business operators and make clear that non-compliance may lead to penalties.

In addition, the Amendment Bill establishes provisions concerning service (*sotatsu*) and service by publication (*koji-sotatsu*), either of which must be made prior to any administrative actions under the act, 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 Bill).

While the Amendment Bill 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 measures against foreign business operators.

Reinforcing regulations on cross-border transfers

Under the Act on the Protection of Personal Information, in principle, a business operator must obtain the prior consent of a data subject when providing personal data to a third party in a foreign country. However, in cases where a third party in a foreign country has established a system that conforms to standards equivalent to those that a business operator under the act must comply with concerning the handling of personal data (the equivalent measures), the business operator may provide personal data to such foreign third party without the prior consent of the data subject (Article 24 of the act). The Amendment Bill reinforces this regulation on cross-border transfers.

Where a business operator must obtain a data subject's consent, business operators must, prior to the data transfer, provide the data subject with information on the protection of personal information in the foreign country where the third party is located, as well as the measures implemented to protect personal information taken by the third party and certain other similar information (Article 24(2) of the Amendment Bill).

In addition, where personal data is provided to a third party in a foreign country pursuant to the equivalent measures exception mentioned above, business operators must take necessary measures to ensure the continuous implementation of the equivalent measures by the third party and provide the data subject with information on such necessary measures on request (Article 24(3) of the Amendment Bill). Further details of each amendment will be provided in the PPC rules.

In practice, it is not foreign business operators which receive personal data that will be subject to these new regulations but, rather, Japanese business operators that transfer personal data outside Japan. The strict enforcement of these regulations will likely result in the reduced transfer of personal data by Japanese business operators internationally. If business operators must investigate systems for protecting personal information in foreign countries and then provide such information to data subjects, it could be an onerous burden for most business operators. If the Amendment Bill intends to strictly enforce this provision of the regulation without imposing a prohibitive burden on business operators, the PPC – not each business operator – should conduct an exhaustive survey on such foreign systems and provide business operators with the necessary information.

Introduction of new rules concerning the use of data

Introduction of pseudonymised information

Purpose and definition

The Amendment Bill introduces the concept of pseudonymised information (*kamei-kako-jouho*) in order to encourage the analysis of data by business operators and promote innovation by exempting data that has been processed to reduce the personal identifiability from requests for provision or cessation of use. Under the Amendment Bill 'pseudonymised information' means information relating to an individual obtained by processing personal information (which includes deleting or replacing information such as names and individual identification codes) so that it is impossible to identify a specific individual by such data unless it is collated with other information (Article 2(9) of the Amendment Bill).

Regulations on pseudonymised information

The Amendment Bill does not deal with pseudonymised information, which does not constitute a database and regulates pseudonymised information under:

- pseudonymised information which falls under personal information; and
- pseudonymised information which does not fall under personal information.

While the majority of the regulations pertaining to personal information, personal data and retained

personal data still apply to pseudonymised information that falls under personal information, the Amendment Bill exempts such pseudonymised information from some of these regulations (Articles 35-2(3) to 35-2(9) of the Amendment Bill).

Conversely, the regulations pertaining to personal information, personal data and retained personal data does not apply to pseudonymised information which does not fall under the scope of personal information. Such information is subject to separate regulation under the Amendment Bill that considers the balance between the need to protect such information and its use.

The table below outlines the specific regulations under the Act on the Protection of Personal Information applicable to pseudonymised information as compared with the regulations under the act concerning personal information.

Personal information	**Pseudonymised information which falls under personal information**	**Pseudonymised information which does not fall under personal information**
Restriction due to purpose of use (Article 16).	Restricted to prescribed purpose of use under Article 15(1) except where permitted by law.	N/A
Notification of the purpose of use on acquisition (Articles 18(1), 18(3) and 18(4)).	Notification of the purpose of use on acquisition by publication (Article 35-2(4)).	N/A
Ensuring the accuracy of data content (Article 19).	In the event that it is no longer necessary to use pseudonymised information which falls under personal information, such data must be deleted without delay (Article 35-2(5)).	N/A
Restrictions on provision to third parties (Articles 23(1) and 23(2)) and third parties in a foreign country (Article 24).	Pseudonymised information which falls under personal information must not be provided to a third party (Article 35-2(6)) unless permitted by law (Article 35-2(6)), or in the specific cases set out in Article 23(5) (ie, assignment, business succession and joint use).	Pseudonymised information which does not fall under personal information must not be provided to a third party (Article 35-3(1)) unless permitted by law (Article 35-3(1)) or in specific cases set out in Article 23(5) (ie, assignment, business succession and joint use).
Change in the purpose of use (Article 15(2)). The obligation to notify data subjects of data breaches (Article 22-2 of the Amendment Bill). The publication of matters concerning retained personal data (Article 27). The claim of the data subject (Articles 28 to 34).	N/A (Article 35-2(9))	N/A

Security management measures (Article 20). The supervision of employees (Article 21). The supervision of trustees (Article 22). Handling complaints (Article 35).	Applicable	Applied *mutatis mutandis* (Article 35-3(3))
N/A	Prohibition on collating pseudonymised information with other information for the purpose of identifying a person (Article 35-2(7) of the Amendment Bill). Prohibition on the use of pseudonymised information to contact the data subject by telephone, mail or email (Article 35-2(8) of the Amendment Bill).	Prohibition on collating pseudonymised information with other information for the purpose of identifying a person (Articles 35-3(3) and 35-2(7) of the Amendment Bill). Prohibition on the use of pseudonymised information to contact the data subject by telephone, mail or email (Articles 35-3(3) and 35-2(8) of the Amendment Bill).

Regulations regarding personal data from a transferee perspective

Under the Act on the Protection of Personal Information, the consent of data subjects is not generally required for the transfer of data which does not fall under the category of personal data from the data provider's viewpoint, even if the transferee can identify the data subject by collating such transferred data with other information. A typical example of such a data transfer is through advertising technology using online identifiers such as cookies. In addition, in 2019 the PPC issued recommendations (which is one of the administrative actions that the PPC is entitled to take under the act) to an enterprise which offered a platform for employment applicants and recruiters. The recommendations were issued on the grounds that the enterprise had collated the information acquired via the platform with the information that was provided by the recruiters through cookies which were allocated to the applicants' web browsers. The collated information was then used to calculate the rate of rejection of offers by each applicant, which was subsequently provided to recruiters without obtaining the applicants' consent.(1) Cookies are not generally considered to be personal information under the act and it was not necessarily clear in this case whether the conduct amounted to a breach thereof. Nonetheless, in light of these circumstances, the Amendment Bill has established the following provisions to ensure that the data subject consents to any such data transfer.

The Amendment Bill introduces the concept of 'individual-related information' (*kojin-kanren-jouho*), which refers to information concerning a living individual that does not fall under any of the categories of personal information, pseudonymised information or anonymously processed information (*tokumei-kako-jouho*) (Article 26-2(1) of the Amendment Bill). According to the Amendment Bill, businesses handling individual-related information must generally confirm the items below when they provide such information to a third party and expect that the third party has acquired this information as personal data (Article 26-2 of the Amendment Bill):

- The data subjects have consented to the third party receiving their individual-related information as personal data (Article 26-2(1)(i)).
- In the case of the provision of data to a third party in a foreign country, when acquiring the consent described above, data subjects are provided with the necessary information, including details of the system for the protection of personal information in said country and the measures taken by the third party to ensure the protection of personal information (Articles 26-2(1) and 26-2(2)).

Further, a number of the provisions concerning data transfer to third parties in foreign countries and the related obligations to prepare and retain records when providing data to third parties will also apply or apply *mutatis mutandis* to the provision of individual-related information to third parties.

This new regulation has the potential to have a significant impact on current business practices including targeted advertising.

Enhancement of data subjects' rights

Relaxation of requirements for cessation of use, deletion and cessation of provision of data to third parties

The Amendment Bill makes it easier for data subjects to claim their rights against business operators that retain their personal information. The table below provides further details.

<table>
<tr><th>Requirements</th><th>Claim</th><th>Article</th></tr>
<tr><td>When personal information is handled in violation of the prohibition of improper use.</td><td>Cessation of use and request for deletion.</td><td>Article 30(1)</td></tr>
<tr><td>When a business operator no longer needs to use retained personal data.</td><td rowspan="3">Cessation of use, request for deletion and cessation of provision to third parties.</td><td rowspan="3">Article 30(5) and (6)</td></tr>
<tr><td>In the event of a situation requiring the reporting of a data breach.</td></tr>
<tr><td>Cases where the handling of retained personal data is likely to harm the rights or legitimate interests of the data subject.</td></tr>
</table>

However, provided that both of the following criteria are met, business operators will not be required to respond to claims by data subjects (Articles 30(2) and 30(6)).

- It is difficult to cease the use of, delete or cease the provision to a third party of retained personal data, including where it would be expensive to do so.
- Alternative measures to protect the rights and interests of data subjects are implemented.

Designation of disclosure methods

The Amendment Bill permits data subjects to designate the method of disclosure when making a request to business operators for the disclosure of retained personal data (Article 28-1 of the Amendment Bill). That is, the data subject may request business operators to disclose retained personal data in electronic form. However, when it is difficult to disclose by the method designated by the data subject, including when the method is prohibitively costly, business operators may make such disclosure in physical hard copy (Article 28(2) of the Amendment Bill).

Mandatory disclosure of confirmation records regarding data transfer to third parties

Under the Act on the Protection of Personal Information, business operators must confirm certain matters and keep records when providing personal data to a third party or when personal data is received from a third party (Articles 25 and 26 of the act). The Amendment Bill provides that data subjects can request the disclosure of such records (Article 28(5) of the Amendment Bill).

Expanding scope of disclosure of retained personal data subject

While data to be deleted within six months is not subject to claims by a data subject under the Act on the Protection of Personal Information, the Amendment Bill abolishes such safe harbour provision. As a result, unless exempted by the cabinet order, all personal data, regardless of the time that the relevant data is held, can be subject to the claims of a data subject, including requests for disclosure. This amendment is expected to result in a further partial amendment to the complementary rules for personal data transferred from the European Union to Japan on the basis of the European Union's adequacy certification.

Reinforcement of criminal penalties

In principle, under the Act on the Protection of Personal Information the maximum criminal penalty for a breach of its provisions by business operators is either one years' imprisonment or a fine of Y500,000. The Amendment Bill restates this penalty and, in particular, raises the penalty in situations where business operators violate either the prohibition on the illegal theft of databases (Article 83 of the act) or a PPC order (Article 84 of the act). While the act stipulates that such violation by business operators is subject to a criminal fine up to Y500,000, the violating company will be fined up to Y100 million under Article 87(1)(i) of the Amendment Bill.

Comment

If the Amendment Bill is passed without any revisions, it will be necessary for many companies to revise their privacy policies. In addition, it will also be necessary for some companies to reconsider

whether to use targeted advertising. As such, the Amendment Bill would have a considerable impact on a wide range of business practices. Companies would need to examine how the Amendment Bill could impact their own business and consider necessary measures while paying close attention not only to the content of the Amendment Bill itself but also to the expected revision of the relevant cabinet order and the PPC rules.

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

Endnotes

(1) For further details of this case, please see here.
