

Enforcement of amended personal information protection regime

August 29 2017 | Contributed by [Nagashima Ohno & Tsunematsu](#)

[Introduction](#)

[Key developments](#)

[Establishment of PPC](#)

[Reporting guidelines](#)

[Enforcement mechanisms](#)

[Comment](#)

Introduction

On May 30 2017 the widely publicised amendments to the Act on the Protection of Personal Information came into force. These amendments mark a significant development in Japan's privacy law regime and are broadly aimed at:

- enhancing the protection of personal information;
- facilitating the use of personal information; and
- bringing Japan's privacy law regime substantially into line with the US and EU models.

In addition to changing how companies must handle personal information, the amendments reflect a significant shift in how such obligations are regulated and enforced, including the manner in which companies must respond to and address potential and confirmed violations of the act. Previously, the task of monitoring compliance with the act was delegated across numerous ministries and regulatory bodies. However, the amendments mark the establishment of the Personal Information Protection Commission (PPC), which will be the regulatory body responsible for managing and ensuring compliance with the amended act. The PPC's establishment reflects an acknowledgement of the importance of privacy-related concerns and the need for a unified and comprehensive enforcement policy across all industries.

This update summarises the amendments and discusses the PPC's role and the regulatory powers and tools prescribed to it by the act to enable it to ensure compliance.

Key developments

The key developments regarding the handling of personal information are as follows.⁽¹⁾

Sensitive information

A new category of personal information, described as 'sensitive information', has been established in order to protect particularly sensitive personal information that could reasonably result in the relevant individual being subject to discrimination, such as information regarding an individual's race, religion, social status or medical and criminal history. Companies must now obtain, at the time such sensitive information is collected, the relevant individual's consent to collect and use the information for specified purposes as communicated by the company to the individual.

Cross-border disclosures

In general, unless certain exemptions apply, companies must obtain the express consent of individuals when transferring data containing personal information outside Japan.⁽²⁾

AUTHORS

[Peter
Armstrong](#)



[Daisuke
Fukamizu](#)



Opting out

Companies that wish to disclose personal information to third parties must now, in addition to obtaining the applicable individual's consent, provide prior notice to the PPC in the required form.

Record-keeping obligations

The amendments introduce new record-keeping obligations for companies regarding their handling of personal information. The information to be recorded includes, for each transfer of personal information:

- the transfer date;
- the transferee's name;
- details of the personal information provided or received; and
- whether consent was obtained (where necessary).

Anonymised processed information

Companies that wish to create or use anonymised data must:

- publicly announce the nature of the information that will be anonymised;
- implement internal rules regarding the anonymising process; and
- when transferring anonymised data, publicly announce such transfer, including the transferee's name and a description of the anonymised data to be transferred.

Establishment of PPC

One of the key features of the amendments is the establishment of the PPC. The PPC will be the central enforcement agency for the Act on the Protection of Personal Information across all business sectors, except the financial sector. **(3)** The PPC has been granted broad powers to enable it to carry out this mandate, including the ability to conduct onsite inspections or dawn raids when deemed appropriate.

Reporting guidelines

Since its establishment, the PPC has published a number of guidelines clarifying and supplementing the requirements of the Act on the Protection of Personal Information, including industry-specific personal information protection guidelines and guidelines on how potential and actual unauthorised disclosures of personal information should be addressed. These publications are useful tools for understanding the PPC's position and how it intends to carry out its regulatory mandate.

While not a legal requirement under the act, the PPC's position is that all potential or actual unauthorised disclosures of personal information, except in minor cases, should be reported to the PPC by way of an incident report. To facilitate the prompt and effective reporting of data privacy issues, the PPC has published a template incident report form on its website; the general expectation is that incident reports should closely follow this template.

According to guidance published by the PPC, incident reports must contain a comprehensive account of the facts and all remedial actions taken, including:

- an overview of the incident, including:
 - the individual or team responsible;
 - the scope of the data breach; and
 - an estimated number of potentially affected individuals;
- an analysis of the cause of the breach;
- an analysis of the potential scope of the impact arising from such a breach;
- a description of the remedial measures to be implemented to mitigate any recurrence;
- the steps taken towards any potentially affected individuals; and
- a discussion as to whether any public statements or press releases will be made.

As noted above, depending on the content of a particular incident report, the PPC may make further inquiries or require supplementary reports to be submitted, either to clarify certain facts or to

report on the remediation of certain identified issues.

Enforcement mechanisms

As noted above, while not a legal requirement *per se*, it is generally understood that entities should voluntarily submit an issue report in accordance with the PPC guidelines and relevant pronouncements on becoming aware of a potential or actual issue. Consistent with general Japanese regulatory practice, the guidelines suggest that the PPC intends to operate in a collaborative manner and encourage market participants to seek input voluntarily from the PPC on potential issues. As such, incident reports represent an important tool for the PPC to address issues as they arise and ensure that, where an issue is found to have arisen, appropriate remedial measures are taken.

Under the Act on the Protection of Personal Information, the PPC is empowered to:

- issue formal reporting orders;
- conduct onsite inspections and dawn raids; and
- publish formal notices and orders regarding any identified problematic conduct.

The PPC is expected to encourage, through the use of its various enforcement powers, open and transparent communication with the various market participants.

Comment

Incident reports represent the initial notification of a particular potential or actual issue. It is therefore expected that the tenor and quality of such reports will influence the PPC's initial response and, potentially, the tone of the entire investigation. For example, if the PPC has cause to believe that key facts have been omitted from, or not appropriately addressed in, an incident report, it may doubt the entity's ability to identify and address the underlying issues raised in the report independently and thus determine it necessary to assume a more active role in the matter. Where a report's content is problematic, inconsistent or otherwise suggests that the entity may be unreliable or unable to conduct an appropriate investigation, the PPC may conduct a dawn raid of the entity's premises or issue a formal reporting order in order to ensure that the matter is properly investigated and that any issues identified are addressed.

Given the PPC's broad discretionary powers, entities are advised to communicate with the PPC in a voluntary, transparent and informed manner. Incident reports should be comprehensive, detailed and based on thorough, substantiated internal research and inquiries. Where applicable, the communications should state that there are outstanding issues or further internal investigations to be conducted, so that the PPC may obtain a complete and accurate understanding of the situation. Comments and other input from the PPC should be carefully considered and, where appropriate, incorporated into any subsequent disclosures or submissions.

The PPC is newly established and has yet to undertake any formal investigations. It therefore remains to be seen how the PPC will approach potential violations of the Act on the Protection of Personal Information in practice. While no case law regarding how the PPC may approach a potential violation of the act exists, the PPC has and continues to publish guidance regarding how it interprets and intends to enforce the act. Entities in Japan are advised to continue to monitor this guidance in order to keep up to date with the PPC and the act.

For further information on this topic please contact [Peter Armstrong](#) or [Daisuke Fukamizu](#) at Nagashima Ohno & Tsunematsu by telephone (+81 3 6889 7000) or email (peter_armstrong@noandt.com or daisuke_fukamizu@noandt.com). The Nagashima Ohno & Tsunematsu website can be accessed at www.noandt.com.

Endnotes

(1) While beyond the scope of this update, the amendments also expand the definitions of 'personal information' and a 'personal information handling business' under the act.

(2) Exemptions primarily apply where:

- the destination jurisdiction is designated by the PPC as having an acceptable personal information protection regime; and
- the third party itself has a personal information protection policy in place which the PPC deems acceptable.

(3) The Financial Services Authority will continue to be the central agency for financial institutions, but is expected to consult and coordinate with the PPC on matters relating to privacy concerns.

The materials contained on this website are for general information purposes only and are subject to the [disclaimer](#).