

DATA SECURITY NEWSLETTER

July 26, 2024

Japan's Data Protection Authority Releases Interim Summary of Proposed Amendments to the Act on the Protection of Personal Information

Atsushi Okada
Partner

atsushi.okada@mhm-global.com

Hiroyuki Tanaka
Partner

hiroyuki.tanaka@mhm-global.com

Noboru Kitayama
Partner

noboru.kitayama@mhm-global.com

Naoto Shimamura
Senior Associate

naoto.shimamura@mhm-global.com

Kohei Wachi
Senior Associate

kohei.wachi@mhm-global.com

1. Overview of the "Interim Summary"
2. Strengthening the protection of individual rights and interests – possible regulations aimed at protecting children and enabling qualified consumer organizations to file injunctions
3. Enhancing effective monitoring and supervision – potential introduction of an administrative fine system
4. Supporting the utilization of data – data utilization without the need for individual consent
5. Other
6. What's Next?

1. Overview of the "Interim Summary"

The Personal Information Protection Commission ("**PPC**"), Japan's data protection authority, released an "[Interim Summary](#)" on June 27, 2024, which outlines the current direction of upcoming amendments to the Act on the Protection of Personal Information ("**APPI**"). As stipulated by a supplementary provision in the APPI, a review of the APPI is required to be made every three years following its implementation. This triennial review is currently underway, and the Interim Summary has been issued as part of this process. The public has been invited to comment on the Interim Summary until July 29, 2024, after which the PPC will finalize proposed amendments based on the feedback received. The Interim Summary highlights three major policy directions under

DATA SECURITY NEWSLETTER

consideration for amendments to the APPI: (1) strengthening the protection of individual rights and interests, (2) enhancing effective monitoring and supervision, and (3) supporting the utilization of data. These discussions reflect the current perspective of the PPC. On July 24, 2024, the PPC announced the establishment of a "[Review Committee on the Triennial Review of the Act on the Protection of Personal Information](#)." The committee is expected to further explore the issues that significantly affect businesses or individuals, such as the introduction of administrative fines, and the potential establishment of a new system for consumer organizations to seek injunctive relief and indemnification of damages. The outcomes of this review are expected to be compiled within 2024.

2. Strengthening the protection of individual rights and interests — possible regulations aimed at protecting children and enabling qualified consumer organizations to file injunctions

The PPC is focusing on the following five areas for more substantial protection of individual rights and interests.

(1) New regulations on biometric data

The PPC is considering additional rules for handling biometric data. Under the current APPI, biometric data is regarded as personal information, but no special rules apply to biometric data. Biometric data is treated in the same manner as general personal information.

The Interim Summary explores amendments that would require businesses to specify the purposes for which biometric data is used in a more detailed way, such as explaining any project or service that will use the biometric data. Additionally, revisions are under consideration that would allow individuals more autonomy to stop the use of their biometric data, as compared to other types of personal data.

(2) Regulations on improper use and unauthorized acquisition

The current APPI prohibits the acquisition of personal information through "illegal or unfair acts" and "deception or other wrongful means." Specific examples of inappropriate use and wrongful acquisition are detailed in guidelines; however, to enhance the predictability of their application, the Interim Summary has pointed out the need to further delineate the scope of

DATA SECURITY NEWSLETTER

these provisions.

The current APPI assumes that individuals are able to decide whether or not to provide their personal data at their own free will. However, there are situations where it is not reasonable to expect individuals to make such determination. Given these circumstances, there is also consideration of additional regulations on the acquisition and use of personal information in situations where it is not expected that individuals are able to make voluntary decisions. For example, when substitute services are difficult to obtain but the provision of personal information is a mandatory condition for obtaining such services. The Interim Summary mentions digital platform services, credit services, and employment as examples.

(3) Enhancing opt-out system for provision of personal data to third parties

Under the current APPI, the provision of an individual's personal data to third parties generally requires the consent of the individual. However, a business is not required to obtain individual consent for third-party transfers if it files a notification with the PPC to rely on an "opt-out" system, which requires the business to notify individuals in advance, or otherwise make it easy for the individuals to find out, that they can "opt out" of the provision of their personal data to third parties. This opt-out system was established with businesses in mind that sell databases containing personal data or provide personal data through residential maps, among other things.

The Interim Summary has highlighted concerns that businesses registered under the opt-out system might unintentionally provide personal data to criminal groups, and that businesses may purchase personal data that was obtained without proper authorization. Consequently, rules are being considered that would impose obligations on opt-out registered businesses to verify (i) a third-party transferee's identity and intended use of the personal information and (ii) the circumstances and identity of the source from which personal information is obtained.

Furthermore, it has been noted that it can be challenging for individuals to learn the status of their personal information that is being provided to third parties and the process for stopping the transfer. In order to address this issue, the PPC is considering measures to ensure that individuals are aware of such status and process.

DATA SECURITY NEWSLETTER

(4) Regulations regarding children's personal information

The current APPI does not have special rules to protect the personal information of children, and there is no definition in the APPI of the age range of who is deemed to be a "child." The Q&A issued by the PPC indicates that the specific age at which someone is considered a child can vary depending on the type of personal information involved and the nature of the business, but that, generally speaking, individuals aged 12 to 15 and under are considered children for which consent of a legal guardian is required.

The Interim Summary indicates that it is currently being considered whether to clarify the legal requirements for obtaining consent from legal guardians and for providing guardians with relevant information regarding protection of information. There is also consideration of whether to make it easier to stop the use of children's personal data and to set the age criterion for children at the under-16 level.

(5) Establishing a new system for consumer organizations to seek injunctive relief and indemnification of damages

Under the current APPI, individuals have the right to request businesses to stop the use of their personal data and to prohibit its provision to third parties in certain cases, such as where the APPI is violated or there is a risk of infringement of their rights. However, these measures can be considered to be a rather limited means of legal redress.

The Interim Summary is considering the introduction of a new system for consumer organizations to seek injunctive relief and, on behalf of consumers, indemnification of damages, from the perspective of enhancing deterrence against illegal handling of personal information and improving the effectiveness of victim recovery.

A system facilitating injunctive relief would be anticipated to target unlawful acts that violate the law. The introduction of such a system faces many challenges, such as ensuring appropriate expertise, sharing initial information, considerations in terms of presentation of evidence, streamlining reporting and supervision channels, and providing financial support to the consumer groups. Such a system applied to the protection of personal information could have a considerably large impact.

The introduction of any such system will likely continue to be examined from multiple perspectives, including a balancing of the burden on businesses against the necessity for protection of individual rights and interests.

DATA SECURITY NEWSLETTER

3. Enhancing effective monitoring and supervision – potential introduction of an administrative fine system

Currently, enforcement of the APPI primarily relies on administrative guidance and recommendations from the PPC, with formal orders being extremely rare. As a general rule, criminal penalties are only applied in cases where the PPC first issues an order and the order is violated. Therefore, the commission is considering strengthening enforcement in three ways.

(1) Implementation of an administrative fine system

In Japan, although there are criminal penalties for violating orders from the PPC, there is no system of administrative fines in place as an administrative punishment.

The Interim Summary discusses the possible introduction of an administrative monetary penalty system as a more effective means of monitoring and supervision. This consideration stems from the need to deter egregious cases where illegal use of personal information results in substantial profits, and to recover undue gains. The Interim Report suggests that introducing an administrative fine system requires a detailed examination and categorization of the types of illegal acts targeted, methods for calculating the penalties, and setting minimum penalty amounts.

(2) Reviewing the Implementation of Recommendations and Orders

The current APPI requires the PPC to make recommendations first before the PPC issues orders. However, it has been pointed out that it may be necessary for the PPC to issue orders immediately in cases where an individual's rights and interests are imminently threatened. The possibility of taking administrative actions against third parties involved in illegal acts is also under consideration.

(3) Expanding the scope of criminal penalties

Under the current APPI, violations that directly trigger criminal penalties are quite limited. Given the variety of recent serious cases involving the improper handling of personal information, the Interim Summary is examining whether to broaden the scope of direct criminal penalties. Additionally, the PPC will

DATA SECURITY NEWSLETTER

examine the appropriateness of the statutory penalties.

(4) Reform to the data breach reporting system

Under the current APPI, any of the following types of personal data breaches, or the likelihood thereof, must be reported to both the PPC and the affected individuals: (1) breaches involving Special Care-required Personal Information as defined under the APPI, such as race, religion, or medical data; (2) breaches that may lead to financial damage due to unauthorized use, such as stolen credit card numbers; (3) breaches that may have been carried out with malicious intent, such as a cyber attack or data exfiltration by an employee; and (4) breaches that involve more than 1,000 individuals. It has been noted that the requirement to report even a single incident is a significant burden for businesses.

The Interim Summary is now considering allowing exemptions from immediate reporting when the risk of infringement of individuals' rights and interests is relatively low, permitting the submission of a consolidated final report instead. Additionally, the PPC is looking into clarifying the necessary criteria for determining when obligations arise concerning the "likelihood" of data breaches. The PPC is also considering adding the illegal provision of personal data as a reporting trigger.

4. Supporting the utilization of data – data utilization without the need for individual consent

While the amendments primarily indicate a direction towards strengthening regulations, the Interim Summary also presents measures to support initiatives aimed at facilitating the use of data.

(1) Utilization of data without individual consent

The APPI generally requires the consent of the individual in the following cases:

- Handling personal information beyond the scope necessary to achieve a notified purpose
- Acquiring Special Care-required Personal Information
- Providing personal data to third parties

However, with the rapid advancement of digital technology, especially in

DATA SECURITY NEWSLETTER

fields related to health, medical care, and emerging technologies such as generative AI, there is an increasing need to utilize personal information. In response, the Interim Summary is considering the possibility of establishing exceptions to the requirement for obtaining individual consent for technologies and services that form the social infrastructure. The balance between public interest evaluation and the protection of individual rights is being emphasized. Additionally, the application of exceptions related to public health in the use of personal information in the field of medical research is also being considered for clarification in guidelines.

(2) Promotion of Voluntary Initiatives in the Private Sector

The Interim Summary is examining the implementation of Privacy Impact Assessments and the appointment of personal data handling officers. While these are not currently mandated under the current APPI, they are being considered as key elements in establishing data governance structures, with measures being explored to encourage voluntary initiatives.

5. Other

In addition to the items mentioned above, discussions are also progressing on the regulatory approach to current issues including profiling, privacy-enhancing technologies, and genomic data.

6. What's Next?

As mentioned above, the PPC has published the Interim Summary for public comment from June 27 to July 29, 2024. Based on the feedback received, the commission plans to finalize the direction of the amendments. While the official timeline has not yet been announced, it is anticipated that a draft of the amendment will be published in 2025 and, if approved in the Diet, come into effect in 2027.

Mori Hamada & Matsumoto is keeping a close watch on these developments. Although the exact details of the amendment remain unclear, it is advisable for businesses to proactively monitor any existing or proposed changes and assess how these amendments could potentially affect their operations.