Status of Triennial Review of the Act on the Protection of Personal Information

Takuya Uehara
takuya.uehara@ohebashi.com

I. Introduction[1]

The Act on the Protection of Personal Information ("**APPI**"),[2] which was enacted in 2003, took full effect in April 2005. It is the core of Japan's data protection legislative framework. It underwent two major amendments in 2015 and 2020-2021, which took full effect in May 2017 and April 2023, respectively.

The 2020-2021 amendment required the government to conduct a triennial review of the status of enforcement of the APPI and take necessary measures as needed. To fulfill this requirement to review the law every three years, the Personal Information Protection Commission ("**PPC**"), which was established as the data protection authority of Japan, has been conducting the first triennial review of the APPI since November 2023.

As of May 2025, the PPC and the experts appointed by it have released several documents which have suggested the direction of the triennial review. First, the PPC published an interim report (the "**Interim Report**") in June 2024 summarizing its views at that time. The PPC then established a study group (the "**Study Group**") in July 2024 comprising of seven experts to mainly discuss the potential introduction of two enforcement systems, namely, the *kachokin seido* (an administrative monetary penalty system) and the *dantai ni yoru sashitome seido oyobi higaikaifuku seido* (the injunctive relief and damage recovery systems through qualified consumer organizations). The Interim Report pointed out that these systems would *"have significant impacts on both businesses and individuals, and require further work to consolidate their opinions."* The Study Group held seven meetings until December 2024 and published a report summarizing its discussions.

Further, based on the results of hearings with experts and other stakeholders, the PPC examined and reassessed the institutional issues that were identified in the Interim Report, including those not discussed in the Study Group. The PPC then began discussing such issues in January 2025, which were associated with these three main topics: (1) how to involve data subjects in the processing of their personal data;[3] (2) how to respond to risks arising out of diversifying ways to process personal data; and (3) how to ensure the effectiveness of compliance by businesses processing personal data. In March 2025, the PPC then published a document summarizing its discussions and views on the institutional issues concerning the APPI (the "**PPC's Views on Institutional Issues**").

---

1. The author thanks his colleagues, Yuki Kuroda and Nanoko Sasaki, for their contribution to this article. For further information about the triennial review, *see* https://www.ohebashi.com/jp/newsletter/01_202504_Kuroda-Uehara-Sasaki.pdf (in Japanese).
2. *Kojin joho no hogo ni kansuru horitsu,* Law No. 57 of May 30, 2003.
3. One unique aspect of the APPI compared to other countries' data protection regulations is that it defines separate concepts for "personal information," "personal data" and "personal data held by a business." Since most of the data processed by businesses falls under the definition of "personal data," this article uses the term "personal data" without making strict distinctions between these terms.

The PPC is still conducting discussions regarding the issues pointed out in the documents mentioned above. No clear timeline for the implementation of the results of such discussions has been made and while specific proposed amendments to the APPI may be published as early as this year, it remains unclear whether all of the issues discussed in these documents will be reflected in such amendments. Nevertheless, some of these discussions, if implemented, would undoubtedly have a significant impact on a wide range of businesses processing personal data in Japan. This article focuses on such key issues and summarizes the current status of the PPC's discussions thereon.

II. Administrative Monetary Penalty System

If businesses processing personal data violate the APPI, they may be subject to sanctions issued by the PPC, such as administrative guidance, advice, recommendations or other orders, publication of their non-compliance,[4] or criminal penalties, including fines of up to 100 million Japanese yen.[5]

Based on the data published by the PPC, while several hundreds of notices of administrative guidance, advice and recommendations have been issued annually, including against major corporations, no orders have been issued to businesses engaged in normal business activities, and no criminal penalties have ever been imposed on companies. These facts have cast doubt on the deterrent effect of the current APPI and given the fact that many other countries have already introduced financial penalty systems, discussions over the potential introduction of an administrative monetary penalty system in Japan have been increasing in recent years.

On the occasion of the current triennial review process, the PPC and the Study Group seem to be seriously considering the introduction of an administrative monetary penalty system for the APPI. However, it has been proposed that the scope of corporate acts that would be subject to monetary penalties should be limited to some extent to avoid excessive regulation that might discourage lawful acts.

The proposal includes the introduction of a penalty that would be imposed on a business only when: (1) it has derived financial benefits by violating the provisions of Article 18 (restriction due to purpose of use), 19 (prohibition of inappropriate use), 20 (proper acquisition) or 27 (restrictions on provision of personal data to third parties) of the APPI; (2) it fails to exercise reasonable care to prevent such violation; (3) individual rights and interests have been or are likely to be infringed by such violation; and (4) the number of the data subjects involved is not less than 1,000.

Another penalty has also been proposed to be imposed on a business when: (1) personal data of not less than 1,000 data subjects have been leaked, lost or damaged; (2) the subject business has grossly neglected to exercise reasonable care to prevent a breach of its obligation to take security control measures; and (3) individual rights and interests have been or are likely to be infringed by such leakage, loss or damage of personal data.

III. Injunctive Relief and Damage Recovery Systems Through Qualified Consumer Organizations

An individual whose rights and interests have been infringed by a violation by a business of the APPI need not only rely on the supervision of the PPC and other administrative agencies, but may also directly seek redress against the business in his/her own capacity. The current APPI grants individuals the right to make a request to cease to use, delete or cease to provide a third party with personal data which has been processed in violation

4. APPI, arts. 147-148.
5. *Id.*, arts. 178-179 and 182-185.

of Articles 18 (restriction due to purpose of use), 19 (prohibition of inappropriate use), 20 (proper acquisition), 27 (restrictions on provision of personal data to third parties) or 28 (restrictions on provision of personal data to third parties in foreign countries) of the APPI.[6] An individual may also file a tort claim against a business that has intentionally or negligently infringed his/her privacy or other rights and interests through the processing of personal data.[7]

However, even if one individual were to file such request or claim, it would not be possible to prevent the same type of damage from occurring to many other individuals. In addition, such request or claim may be abandoned in many cases because of the expenses involved—courts in Japan often only award nominal compensation for mental distress in invasion of privacy cases even without proof of financial damages, e.g., only 1,000-5,000 Japanese yen (or USD 7 to USD 34) per person in cases where less sensitive data is involved, such as names, addresses or email addresses.

In the field of consumer law, there is a consumer organization complaint system in Japan which allows consumer organizations certified by the Prime Minister to file complaints against businesses on behalf of consumers, specifically: (1) complaints to seek the cessation of improper acts by businesses;[8] and (2) complaints to seek collective recovery of financial losses which numerous consumers commonly suffer due to businesses' improper acts.[9] However, the current system cannot completely resolve the problem described above because: (1) consumer organizations may only seek the cessation of the businesses' acts that violate the Consumer Contract Act, not the APPI; and (2) moral damages (i.e., damages for mental distress) may be recovered only when claimed in conjunction with the recovery of financial losses or when caused by businesses' intentional acts.

In light of the issues above, the PPC and the Study Group are considering establishing a new framework similar to the consumer organization complaint system, which would target businesses' acts that violate the APPI or otherwise infringe individual rights and interests, including privacy. Specifically, they are considering establishing: (1) a system where consumer organizations may seek injunctive relief against businesses' acts that are in violation of the APPI, in particular, Articles 18, 19, 20, 27 and 28 thereof, which are already subject to an individual's right to request a business to cease to use, delete or cease to provide a third party with personal data under the current APPI; and (2) a system where consumer organizations may seek collective recovery through the courts for moral damages caused to numerous individuals due to businesses' negligent data breaches.

IV. Other Issues Described in the PPC's Views on Institutional Issues

1. How to Involve Data Subjects with the Processing of Their Personal Data

(a) Adjustment of the Consent Requirement in the AI Age

The current APPI requires businesses to obtain the consent of data subjects when, among others, acquiring sensitive personal data, such as race, medical history or criminal record,[10] or providing personal data to a third party.[11] There have been complicated debates on how strictly the regulations should be applied in situations where training

6. APPI, art. 35.
7. *Minpo* [Civil Code], Law No. 9 of June 21, 1899, art. 709.
8. *Shohisha keiyaku ho* [Consumer Contract Act], Law No. 61 of May 12, 2000, art. 12.
9. *Shohisha no zaisantekihigaitou no shudanteki na kaifuku no tameno minji no saibantetsuzuki no tokurei ni kansuru horitsu* [Act on Special Measures Concerning Civil Court Proceedings for the Collective Redress for Property Damage Incurred by Consumers], Law No. 96 of December 11, 2013, chap. II.
10. APPI, art. 20.
11. *Id.*, art. 27.

data sets containing personal data are used for AI development. This is said to have been causing confusion in practice.

The PPC is of the opinion that parameters making up a learned model of AI do not constitute personal data even if the model was trained with data sets containing personal data, as long as there is no correspondence between such parameters and a specific individual.[12] However, this does not mean that AI developers may use without limitation for AI training purposes the personal data they received from a third party, such as user companies; instead, AI developers may only use such personal data without the data subjects' consent within the scope of work outsourced by the third party. As a result, it is often discussed whether the usage of the subject training data sets falls "within the scope of work outsourced by the third party." Specifically, it is hard to determine whether the usage of training data sets falls "within the scope of work outsourced by the third party" if the AI developer has an intention to provide the learned model to users other than the third party that provided the data sets. There is also a debate as to whether it would be illegal if an AI developer created training data sets containing personal data without data subjects' consent by collecting information that was publicly available on the Internet but unintentionally contained sensitive personal data.

Under these circumstances, the PPC's Views on Institutional Issues demonstrate that it is considering the introduction of a system which would allow for the legitimate provision of personal data to a third party and acquisition of publicly available sensitive personal data without the data subjects' consent as long as it is ensured that such data would be used only for the creation of statistical information including "AI development, etc., which can be categorized as statistical creation, etc." If such system is introduced, the practical confusion surrounding AI development would likely be settled to a certain extent.

(b) Adjustment of Data Breach Notification Requirements

The current APPI requires businesses who have experienced a specific type of personal data breach to report it to the PPC and notify the data subjects involved of such breach.[13] The "personal data" in this context includes information such as user ID, which by itself cannot identify a specific individual but can be easily collated with other information, such as the name and contact information of an individual, to thereby identify a specific individual. Businesses would therefore be required to comply with the reporting and notification obligations even if only such information had been breached, which as a result imposes an excessive burden on businesses.

Under these circumstances, the PPC is considering relaxing the obligation to notify data subjects of a data breach in cases where there is little risk to individual rights and interests, including where only information such as user ID, which has no meaning by itself for those who acquire it, has been breached. This is considered an issue that would have no small impact on practice.

(c) Establishment of New Regulations on Processing Children's Personal Data

The current APPI does not have any special regulations regarding the processing of children's personal data that differ from those of adults, except

12. Q&A on Guidelines Regarding the Act on the Protection of Personal Information, the PPC, last revised on December 2, 2024 ("**APPI Q&A**"), Nos. 1-8.
13. APPI, art. 26.

that it stipulates that a legal representative, including a parent, may make a request for disclosure, etc., on a child's behalf.[14] On the other hand, the PPC makes it clear that, with respect to the processing of personal data of children under the age of 12-15, which requires the consent of data subjects, businesses should obtain the consent of their legal representatives instead of the children themselves.[15]

Under these circumstances, the PPC is considering taking further steps to establish new regulations on the processing of children's personal data, including: (1) a regulation which would obligate businesses to obtain the consent of, or notify, the legal representatives of the data subjects with respect to the processing of personal data of children under the age of 16, which requires businesses to obtain the consent of, or notify, the data subjects; and (2) a regulation which would allow children under the age of 16 or their legal representatives to, without cause, request businesses to cease to use, delete or cease to provide a third party with their personal data.

2. How to Respond to Risks Arising Out of Diversifying Ways to Process Personal Data

(a) Adjustment of Regulations on Information Other Than Personal Data

The APPI only prohibits the inappropriate use or improper acquisition of personal data, i.e., information which can, by itself or with other information which can easily be collated with it, identify a specific individual.[16] In other words, the APPI does not currently regulate the inappropriate use or improper acquisition of information with which no specific individual can be identified. However, the inappropriate use or improper acquisition of such information may also infringe individual rights and interests if the party using or acquiring it can contact the data subjects through such information. For example, a malicious party can send phishing emails to email addresses even if such email addresses do not constitute personal data, i.e., no specific individual can be identified with the email addresses themselves or with other information that can easily be collated with them. In addition, anonymous health information which is not considered personal data can be used for advertising purposes beyond the purposes known to the data subjects.

Under these circumstances, the PPC is considering broadening the coverage of the prohibitions mentioned above by making it prohibited to use inappropriately, or acquire improperly, information with which no specific individual can be identified but the party using or acquiring it can contact the data subjects.

(b) Establishment of New Regulations on the Processing of Biological Data

The APPI does not have any special regulations regarding the processing of biological data that differ from those applicable to other personal data unless it involves sensitive personal data. However, biological data that can be easily obtained without the data subjects' knowledge and that can be used to track their behavior over time due to its uniqueness and immutability, such as facial feature data, is prone to invade the privacy of data subjects even if it is not sensitive personal data.

The PPC is therefore considering establishing new regulations on the processing of such biological data, including: (i) a regulation which would obligate businesses who are processing such biological data to disclose certain items regarding

14. *Id.*, art. 37.
15. APPI Q&A, Nos. 1-62.
16. APPI, arts. 19-20.

the processing, and (ii) a regulation which would allow data subjects to request businesses to, without cause, cease to use, delete or cease to provide a third party with such biological data.

3. How to Ensure the Effectiveness of Compliance by the Businesses Processing Personal Data

In addition to the potential introduction of an administrative monetary penalty system as well as injunctive relief and damage recovery systems through qualified consumer organizations, the PPC is considering introducing measures to ensure the effectiveness of existing penalties, such as expanding the recommendations and orders issued by the PPC as well as criminal penalties.

Specifically, the PPC is considering allowing the issuance of orders, which under the current APPI may be issued only when a business has violated the PPC's recommendations or individual rights and interests have been actually infringed, even when no recommendation has been issued, and individual rights and interests have not yet been infringed but are in imminent danger of being infringed. The PPC is also considering allowing the issuance of recommendations or orders which recommend or require that a business take measures necessary to protect data subjects' rights and interests, including notifying the data subjects of or publishing the fact that the business had violated the APPI.

V. Conclusion

As mentioned earlier, the PPC is still discussing the issues described in the Interim Report, the report of the Study Group, the PPC's Views on Institutional Issues and other documents, and it is uncertain when and how such discussions will conclude and be implemented concretely. Businesses processing personal data in Japan should continue to pay close attention to the developments of this ongoing triennial review process.