Chambers AND PARTNERS

CHAMBERS GLOBAL PRACTICE GUIDES

Data Protection & Privacy 2026

Definitive global law guides offering comparative analysis from top-ranked lawyers

Japan: Trends & Developments

Yuki Kuroda, Takuya Uehara and Nanoko Sasaki
Oh-Ebashi LPC & Partners

JAPAN

Trends and Developments

Contributed by:
Yuki Kuroda, Takuya Uehara and Nanoko Sasaki
Oh-Ebashi LPC & Partners

Oh-Ebashi LPC & Partners is a full-service law firm with over 160 attorneys, and its main offices are in Tokyo and Osaka. It was originally established in Osaka in 1981 but now has an equivalent-sized operation in Tokyo. It was the first Japanese law firm to open an office in China and, together with its Nagoya office, currently has offices in four locations. Its legal practice covers a broad range of fields, including corporate/M&A, risk management and compliance, IP law, life sciences, restructuring/insolvency, competition and antitrust/consumer protection, dispute resolution, finance and insurance, employment law, administration/regulatory law and tax law. It also provides an international practice, a China/Asian practice, a private practice and a pro bono practice.

Authors

Yuki Kuroda is a partner at Oh-Ebashi LPC & Partners and is in charge of data protection and data security issues. He has handled a number of law and technology cases throughout his career. His practice includes Japanese and international data protection cases, and he regularly guides clients on planning new data-intensive businesses and implementing robust data protection/security compliance programmes. He received a PhD degree from Kyoto University Graduate School of Informatics, an LLM degree from the University of California, Berkeley, and a J.D. degree from Osaka University. He is licensed to practise law in Japan and New York.

Takuya Uehara is a partner at Oh-Ebashi LPC & Partners and advises various companies on technology-related matters, including how to operate systems for e-commerce and digital advertisement. He has extensive experience in advising on how to comply with regulations on electronic data usage and protection, and substantial expertise in risk management and compliance, including how to respond to data security incidents. He received an LLM degree from the University of Pennsylvania and a J.D. degree from the University of Tokyo, and is licensed to practise law in Japan and New York.

Nanoko Sasaki is an associate at Oh-Ebashi LPC & Partners, where her practice focuses on data protection and cybersecurity law, commercial litigation and general corporate practice. She has represented a multinational corporation in cyber litigation matters, including a case regarding a sender identification information disclosure order. She has extensive experience in domestic and cross-border M&A, having played significant roles in numerous transactions. She received both a J.D. degree and a B.A. degree from the University of Tokyo, and is licensed to practise law in Japan.

Oh-Ebashi LPC & Partners

Kishimoto Building 2F
2-2-1 Marunouchi, Chiyoda-ku
Tokyo 100-0005
Japan

Tel: +81 3 5224 5566
Fax: +81 3 5224 5565
Email: general_toiawase@ohebashi.com
Web: www.ohebashi.com/en

Introduction

The Act on the Protection of Personal Information (APPI) serves as Japan's fundamental and comprehensive data protection legislation.

When the APPI underwent significant amendments in 2020, it was stipulated that its provisions should be reviewed approximately every three years following the implementation of the amended law. Therefore, the Personal Information Protection Commission (PPC), which was established as the data protection authority under the APPI, initiated its review in November 2023 and published an Interim Report in June 2024.

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, and began discussing such issues in January 2025. The issues were associated with three main topics:

- how to involve data subjects in the processing of their personal data;
- how to respond to risks arising out of diversifying ways to process personal data; and
- how to ensure the effectiveness of compliance by businesses processing personal data.

In March 2025, the PPC published its "Views on Institutional Issues", a document summarising its discussions and its views on the institutional issues concerning the APPI. It then published its "Policy on Institutional Amendments" in January 2026, outlining the following four pillars of the APPI amendment:

- the promotion of proper data utilisation;
- rules to appropriately address risks;
- the prevention of improper use; and
- rules to ensure effective compliance.

The PPC is still conducting discussions regarding the issues highlighted in these document. No clear timeline for the implementation of the results of such discussions has been made; specific proposed amendments to the APPI may be published as early as this spring, but 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 chapter focuses on such key issues and summarises the status of the PPC's discussions thereon as of January 2026.

Note that one unique aspect of the APPI compared to other countries' data protection regulations is that it defines concepts such as "Personal Information", "Personal Data" and "Personal Data the Business Holds". Since most of the data processed by businesses falls under "Personal Data", this chapter will use the term "Personal Data" without making strict distinctions between these terms.

Promotion of Proper Data Utilisation

Adjustment of consent requirements in the AI age

The current APPI requires businesses to obtain the consent of data subjects when acquiring sensitive personal data, such as race, medical history or crimi-

nal record (Article 20), or providing personal data to a third party (Article 27), among other activities. There have been complicated debates on how strictly these regulations should be applied in situations where training 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. However, this does not mean that AI developers may use personal data they received from a third party, such as user companies, without limitation for AI training purposes; 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", which is hard to determine if the AI developer intends 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 for an AI developer to create training data sets containing personal data without the data subjects' consent by collecting information that was publicly available on the internet but unintentionally containing sensitive personal data.

Under these circumstances, the PPC's Views on Institutional Issues and Policy on Institutional Amendments demonstrate that it is considering the introduction of a system that would allow for the legitimate provision of personal data to a third party and the 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 categorised as statistical creation, etc." If such system is introduced, the practical confusion surrounding AI development would likely be settled to a certain extent.

Other directions regarding relaxation of consent requirements

In addition to the points mentioned above, the PPC's Views on Institutional Issues and Policy on Institutional Amendments also suggest that personal data processing that clearly does not contradict the data subject's will and therefore does not harm his/her rights and interests may be allowed without his/her consent. Such processing may include, for example, the provision of customer data from a hotel booking site to the hotel where the customer wishes to stay, or data sharing between banks for overseas remittances.

Consent may also no longer be required for the processing of personal data that is necessary for the protection of life, body or property, or for the improvement of public health or the promotion of the healthy development of children. Under the current APPI, such data processing is allowed without data subjects' consent only if it is difficult to obtain such consent. The PPC is considering easing the requirement by allowing such data processing even when it is not difficult to obtain the data subject's consent but there are reasonable grounds for not obtaining his/her consent – for example, when necessary and appropriate measures have been implemented to prevent privacy violations, such as anonymisation or concluding confidentiality agreements.

The PPC is also considering easing consent requirements when hospitals and other organisations providing medical care acquire sensitive personal data or share personal data with third parties.

Rules to Appropriately Address Risks

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 relating to adults, except that it stipulates that a legal representative, including a parent, may make a request for disclosure, etc, on a child's behalf (Article 37). On the other hand, the PPC makes it clear that, when processing the personal data of children under the age of 12, businesses should obtain the consent from the children's legal representatives rather than from the children themselves.

Under these circumstances, the PPC is considering taking further steps to establish new regulations on the processing of children's personal data, including:

- a regulation that 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 that requires businesses to obtain the consent of, or notify, the data subjects; and
- a regulation that 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.

Establishment of new regulations on the processing of biological data

The current 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 behaviour 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:

- a regulation that would obligate businesses that are processing such biological data to disclose certain items regarding the processing; and
- a regulation that 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.

Adjustment of regulatory framework for businesses entrusted with personal data processing

The APPI currently requires businesses to obtain data subjects' consent when providing personal data to third parties, as discussed above, but there are some exceptions. Specifically, data subjects' consent is not required when personal data is provided to a third party for the purpose of entrusting personal data processing (Article 27, Paragraph 5, Item 1). Instead, businesses must exercise necessary and appropriate supervision over such third-party processors (Article 25).

For instance, cloud service usage may be categorised as entrusted personal data processing. In such cases, cloud service users must supervise service providers, such as through requiring periodic reports on the status of personal data processing. However, such supervision may be impractical when small-scale businesses use large-scale cloud services.

Therefore, the PPC is now considering reviewing regulations for entities entrusted with personal data processing based on practical realities. For example, such entities may no longer be required to implement security measures for the entrusted personal data by themselves as long as they conclude agreements with the entrusting party regarding all aspects of the means of the processing and measures necessary for the entrusting party to monitor the status of the processing.

Adjustment of data breach notification requirements

The current APPI requires businesses that have experienced a specific type of personal data breach to report it to the PPC and notify the data subjects involved of such breach (Article 26).

"Personal data" in this context includes information such as a management ID assigned solely for internal system database integration, 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 the management 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.

Prevention of Improper Use

The current APPI only prohibits the inappropriate use or improper acquisition of personal data – ie, information that can identify a specific individual, either by itself or with other information that can easily be collated with it (Articles 19–20). 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 – ie, 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 that 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 prohibiting the inappropriate use or improper acquisition of information with which no specific individual can be identified but through which the party using or acquiring it can contact the data subjects.

Rules to Ensure Effective Compliance

Introduction of an administrative monetary penalty system

If businesses processing personal data violate the current 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 (Articles 147–148) or criminal penalties, including fines of up to JPY100 million (Articles 178–179 and 182–185).

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 seems 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:

- it has derived financial benefits by violating any of the specific provisions of the APPI, including Articles 19 (prohibition of inappropriate use), 20 (proper acquisition) and 27 (restrictions on provision of personal data to third parties);
- it fails to exercise reasonable care to prevent such violation;
- individual rights and interests have been or are likely to be infringed by such violation; and
- the number of data subjects involved is not less than 1,000.

Ensuring the effectiveness of recommendations, orders, etc

In addition to the potential introduction of an administrative monetary penalty system, the PPC is considering the introduction of measures to ensure the effectiveness of existing penalties, such as recom-

mendations 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 that recommend or require a business to take measures necessary to protect data subjects' rights and interests, including notifying the data subjects or publishing the fact that the business had violated the APPI.

On the other hand, while the Interim Report had suggested that the PPC was considering introducing injunctive relief and damage recovery systems through qualified consumer organisations, which might have been another means to ensure effective compliance of the APPI through new systems where consumer organisations may seek injunctive relief against businesses' acts that violate the APPI or seek collective recovery through the courts for moral damages caused due to businesses' negligent data breaches, the Policy on Institutional Amendments does not refer to such systems. It seems that the PPC does not consider the introduction of such systems to be among its highest priorities.

Conclusion

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

CHAMBERS GLOBAL PRACTICE GUIDES

Chambers Global Practice Guides bring you up-to-date, expert legal commentary on the main practice areas from around the globe. Focusing on the practical legal issues affecting businesses, the guides enable readers to compare legislation and procedure and read trend forecasts from legal experts from across key jurisdictions.

To find out more information about how we select contributors, email Rob.Thomson@chambers.com