NEWSLETTER

Japan: Policy Direction for Amendment of the APPI – Enhance AI Development and Introduce Administrative Fines, etc.-

Data Protection Newsletter January 20, 2026

Authors:
Noriya Ishikawa
n.ishikawa@nishimura.com
Yuko Kawai
y.kawai@nishimura.com
Kei Hattori
k.hattori@nishimura.com

On January 9, 2026, the Policy Direction for Amendment of the Act on the Protection of Personal Information[1] (Act No. 57 of 2003) ("APPI") was published by the Personal Information Protection Commission of Japan ("PPC"). This Policy Direction for Amendment of the APPI ("Policy Direction") was created with the goal of prompt submission of the draft amendment to the APPI to the Diet, which was also indicated in the Basic Policy on Ideal Data Utilization Systems.[2] This newsletter provides a detailed overview of this Policy Direction. In addition to relaxing regulatory requirements to enhance AI development and utilization, like the simplification proposal in the EU Digital Omnibus,[3][4] this Policy Direction also introduces administrative fines for violations of certain data processing regulations.

1. Promotion of Appropriate Data Utilization

In alignment with the Basic Policy on Ideal Data Utilization Systems, this Policy Direction proposes that the framework for data subjects' consent should be reviewed from the perspective of whether the processing of their personal data affects their rights and interests, and that through such a review, proper data utilization can be achieved while preserving the trust of data subjects.

(1) Data provision and acquisition for the creation of statistical data

Under the current version of the APPI, as a general rule, businesses must obtain the prior consent of data subjects to provide personal data to third parties or to acquire sensitive personal information (Art. 27(1) and Art. 20(2)). In this regard, the Policy Direction proposes that **data subjects' consent to these events should not be required; provided that such data is to be used exclusively for the creation of statistical information, etc. (including development of AI that can be categorized as the creation of statistical information), and subject to other conditions which will be set forth in the amended supplementary provisions**. This

1 https://www.ppc.go.jp/files/pdf/01-1_seidokaiseihousin.pdf.

2 Regarding the Basic Policy on Ideal Data Utilization Systems, please see N&A Newsletter of July 3, 2025.

3 Proposal for a Regulation of the European Parliament and of the Council Amending Regulations (EU) 2024/1689 and (EU) 2018/1139 as Regards the Simplification of the Implementation of Harmonised Rules on Artificial Intelligence (Digital Omnibus on AI), COM (2025) 836 final (Nov. 19, 2025).

4 Proposal for a Regulation of the European Parliament and of the Council Amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as Regards the Simplification of the Digital Legislative framework, and Repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus), COM (2025) 837 final (Nov. 19, 2025).

proposal is primarily intended to enhance **AI development and utilization** in Japan.[5]

(2) Other rules for (i) purposes of use limitation, (ii) third-party provision of personal data, and (iii) acquisition of sensitive personal information

As a general rule, the current version of the APPI requires businesses to obtain the prior consent of data subjects in order to process their personal information beyond the scope necessary for achieving the specified purpose of use (Art. 18(1)), acquire sensitive personal information (Art. 20(2)), or provide their personal data to third parties (Art. 27(1)) (collectively, "Consent Required Processing"). In this regard, the Policy Direction proposes that **prior consent of data subjects should not be required where it is clear, in light of the circumstances of the acquisition of their personal information, that the Consent Required Processing does not conflict with the data subject's intent and therefore does not harm their rights or interests**.
In addition, the Policy Direction is intended to relax and clarify the requirements for the exemption from prior consent of data subjects. First, the current version of the APPI exempts businesses from obtaining prior consent from data subjects in cases where Consent Required Processing is carried out for the protection of life, etc., or for the improvement of public health, etc., in situations where it is difficult to obtain consent of data subjects (Art. 18(3)(ii)(iii), Art. 20(2)(ii)(iii), and Art. 27(1)(ii)(iii)). The Policy Direction proposes that the **current requirement of "difficulty to obtain consent of data subjects" be relaxed**.
Second, the current version of the APPI exempts businesses from obtaining prior consent of data subjects in cases (a) where businesses are "academic research institutions, etc." and need to use/provide personal data or sensitive personal information for academic research purposes, or (b) where (i) personal data is provided to "academic research institutions, etc." which need to process such personal data for academic research purposes or (ii) sensitive personal information is collected from "academic research institutions, etc." for academic research purposes (Art. 18(3)(v)(vi), Art. 20(2)(v)(vi), Art. 27(1)(vi)(vii)). The Policy Direction proposes that it be expressly stipulated that **"academic research institutions, etc."** above **include institutions or organizations operating for the purposes of providing medical care**.

2. New Rules to Properly Address Risks

The Policy Direction proposes some new rules in light of the recent changes to risks to individual rights and interests due to recent changes to aspects of data processing.

(1) Personal data of children

The current version of the APPI does not provide specific rules on the personal data of children, although some measures are recommended to be taken pursuant to various guidelines. The Policy Direction proposes that **for data subjects under 16 years of age**, (i) it be stipulated in the amended APPI that the **requirements of consent, notification, and the like under the APPI be applicable to the data subjects' legal representatives**, (ii) the requirements for requesting suspension of use and erasure of personal data (Art. 35) be relaxed, and (iii) a duty clause that the best interests of children are taken into primary consideration be established.

---

[5] AI development and utilization in Japan is being strongly pursued as a national strategy in the AI Basic Plan published on December 23, 2025, pursuant to Article 18 of the Act on the Promotion of Research and Development, and Utilization of AI-related Technology.

(2) Biometric data

The current version of the APPI does not provide specific rules for the protection of biometric data. The Policy Direction proposes that, with respect to **facial feature data**, etc., (i) **certain matters be legally required to be publicly available**, (ii) the requirements for data subjects' requests for suspension of use or erasure (Art. 35) be relaxed, and (iii) third-party provision of biometric data based on the opt-out mechanism (Art. 27(2)(3)(4)) be prohibited.

(3) Obligations of contractors

When businesses outsource the processing of personal data to contractors, the current version of the APPI requires businesses to supervise contractors to ensure the security of the personal data (Art. 25). In practice, businesses are required to select appropriate contractors, execute a data processing agreement, and monitor the contractors' processing of personal data, pursuant to the relevant guidelines. However, many businesses depend on contractors in relation to the processing and safeguarding of personal data, and it is not always possible to supervise contractors to the extent necessary. Accordingly, the Policy Direction proposes that the obligations of contractors processing personal data be reviewed. Specifically, it states that **explicit statutory obligations should be imposed on contractors not to process personal data beyond the scope necessary for the performance of the outsourced services unless certain exceptional circumstances exist**. On the other hand, in cases where contractors do not determine means of processing personal data (i.e., businesses designate them), if businesses agree with contractors on (i) all means of contractors' processing personal data and (ii) certain measures necessary for said businesses to monitor the circumstances of contractors' processing personal data, those contractors should, in principle, be exempted from obligations of businesses processing personal data required under the APPI (although some obligations, such as security control measures required by the APPI, will still apply to these contractors).

(4) Relaxing personal data breach notification obligations (notice to data subjects)

Under the current version of the APPI, businesses subject to a personal data breach which meets the threshold for filing a report to the PPC must also notify the affected data subjects of the personal data breach and take alternative measures (publication of the notification, in most cases) if it is difficult to notify the affected data subjects of the personal data breach (Art. 26(2)). In this regard, the Policy Direction proposes that **obligations regarding notifying data subjects affected by a data breach be relaxed if not issuing such a notification is unlikely to harm their rights and/or interests**.

3. Prevention of Inappropriate Use and Improper Acquisition

The current version of the APPI prohibits businesses from utilizing personal information in a way likely to foment or induce unlawful or unjust acts (Art. 19) or from acquiring personal information by deception or other wrongful means (Art. 20(1)). In light of the increasing risk of personal data etc. being exploited in an improper manner like crimes, the Policy Direction proposes that (i) the inappropriate use and improper acquisition of information

related to personal information[6], etc. that enables targeted approaches to the relevant data subjects be prohibited, and (ii) when personal data is provided to third parties based on the opt-out mechanism (Art. 27(2)(3)(4)), confirmation of the recipients' identity and intended purposes of use be required.

4. Strengthening Enforcement (incl. Administrative Fines)

(1) Introduction of administrative fines

In order to deter malicious violations involving the processing of large volumes of personal data which can be misused for monetary or other economic benefits, the Policy Direction proposes that an administrative fines be imposed for severe infringements of data subjects' rights and interests under the APPI. Specifically, fines would be imposed in **cases where monetary or other economic benefits are obtained through any of the following acts**:
(a) providing personal information to a third party under circumstances where it can be anticipated that illegal acts or unjust discriminatory treatment will be carried out through the use of such personal information;
(b) utilizing personal information requested by a third party under circumstances where it can be anticipated that the third party may engage in illegal acts or unjust discriminatory treatment through the use of the relevant personal information;
(c) acquiring personal information by deception or other wrongful means;
(d) **providing personal data to third parties without the prior consent** of data subjects in violation of Art. 27(1);[7] or
(e) processing **personal information** that was **acquired under the special exception framework for statistical compilation, etc.,** for **purposes beyond the scope necessary for achieving the specified purpose of use**, or **providing** such information **to third parties** (or the like) in violation of the obligations under such special exception framework (see 1(1)).

The Policy Direction clarifies that, in addition to the acts above, the following requirements should be met for imposition of administrative fines:
(i) businesses are regarded as having failed to exercise the due care reasonably required to prevent the relevant conduct (**due care**);
(ii) the number of data subjects whose personal data was processed through the relevant acts exceeds 1,000 (**large-scale processing**); and
(iii) the degree of harm to data subjects' rights and interests is significant (**infringement of data subjects' rights and interests**).

According to the Policy Direction, **the amount of an administrative fine will be equivalent to the amount of monetary or other economic benefits obtained in connection with the acts above**. Unlike the GDPR, the turnover of the relevant business will not be taken into account when calculating the amount of administrative

[6] Under the APPI, "information related to personal information" means information relating to a living individual which does not constitute (a) personal information, (b) pseudonymized personal information, or (c) anonymized personal information (Art. 2(7)). Information related to personal information typically refers to cookies and other online identifiers, location information, and information indicating interests and preferences.

[7] Data provision under certain exceptions already stipulated in the current version of the APPI (such as outsourcing data processing and joint-use) are not expected to fall within item (d).

fine.

(2) Requests, recommendations, and orders

The Policy Direction proposes that the requirements for the PPC's issuance of orders be reviewed so that corrective actions for violations can be demanded promptly, and that the PPC be allowed to issue recommendations or orders requiring businesses to take measures necessary to protect data subjects' rights and interests, such as notifying the affected data subjects of the facts of a violation or making such facts publicly available. In addition, the Policy Direction proposes that additional provisions be established to allow the PPC to request that third parties assisting with or facilitating violations cease such violations.

(3) Strengthening penalties

The Policy Direction proposes that unauthorized provision of personal information databases, etc., carried out for malicious purposes should also be subject to criminal penalties, and that the maximum limit of these penalties be increased. In addition, other penalties will be introduced for the unlawful acquisition of personal information through fraudulent or similar acts.

5. Outstanding Issues

In addition to the four points explained above, the Policy Direction also notes that the following issues will be reviewed on an ongoing basis.

(1) Streamlining personal data breach reporting framework

The streamlining of the personal data breach reporting framework is currently being reviewed (e.g., via business entities receiving confirmation by third parties (such as accredited personal data protection organizations) regarding organizational structures and procedures).

Many of the data breaches subject to reporting obligations such as large-scale leaks of personal data or leaks resulting from acts suspected to have been carried out for fraudulent purposes (Art. 26(1)) are attributable to cyberattacks. The legislative discussion on mandating incident reporting to the competent authorities under the Act on the Prevention of Damage Caused by Unauthorized Acts Against Critical Computer Systems (Act No. 42 of 2025; hereinafter referred to as the "Cyber Response Capability Enhancement Act") will coordinate with this review under the APPI for consolidating reporting formats and reporting contact points for these reporting requirements.

Furthermore, the threshold for personal data breach reporting (specifically the requirement of "risk" of occurrence of data breaches) will be revised to take into account the degree of risk to data subject' rights and interests, while ensuring consistency with the threshold for reporting requirements to the competent authorities under the Cyber Response Capability Enhancement Act.

(2) Coordination among stakeholders

The Policy Direction does not introduce a new remedy system to allow certain organizations (such as existing qualified consumer organizations) to seek collective injunctive relief or damage recovery, although such a new

collective remedy structure has been discussed in the PPC. However, this Policy Direction states that it is necessary to foster an environment in which organizations, including qualified consumer organizations, can serve as recipients of data subjects' concerns. To this end, the Policy Direction proposes that the Personal Information Protection Act Consultation Hotline be used to obtain a better understanding of the actual practices of businesses' processing personal data and promote coordination among any relevant stakeholders.

Public Relations Section, Nishimura & Asahi newsletter@nishimura.com