Miura & Partners

Japanese Law Update Vol.20

Roundtable on the Intersection of AI and Personal Data

February 2, 2026

Aiko KANAYAMA
Takahiro NAKAYAMA
Taro TANAKA
Yasuhiro SHIMIZU
Shota EIMURA

1. Overview

On 10 December 2025, Miura & Partners hosted a roundtable discussion focused on balancing data privacy protection with the effective use of data. The roundtable opened with a keynote address by Ms Denise Wong, Assistant Chief Executive of the Infocomm Media Development Authority of Singapore[1], to facilitate the exchange of best practices between Japan and Singapore. Following the keynote, experts from the government, the private sector, and academia engaged in a wide-ranging exchange of views on the following topics, all of which form part of the three-year review of the Act on the Protection of Personal Information (Act No. 57 of 2003) (the 'APPI').

i. AI development and data subject involvement in the handling of personal data
ii. Handling of children's personal information
iii. Regulation of data relating to physical characteristics
iv. Regulation of personal-related information

2. Keynote Address

In her keynote address, Ms Denise Wong spoke about Singapore's AI governance model. Specifically, she explained that Singapore has adopted a pragmatic approach whereby it does not enact a single, standalone 'AI Act,' but instead aligns its existing data protection law (the

[1] Infocomm Media Development Authority of Singapore ('IMDA') develops and regulates the infocomm and media sectors to create a dynamic, holistic and exciting ecosystem filled with growth opportunities through talent, research, innovation and enterprise. Singapore's Personal Data Protection Commission (PDPC), where Ms. Denise Wong also serves as its Deputy Commissioner, is part of the IMDA.

PDPA) with industry practices. She further highlighted that Singapore's AI governance is underpinned by core principles such as a shared responsibility model in which government, industry, and academia act as partners; a clear risk-based approach; and a strong emphasis on principles over prescription, with a focus on outcomes such as 'fairness', 'transparency', 'accountability', and 'robustness'.

3. Roundtable Discussion

(1) AI development and data subject involvement in the handling of personal data

Under this theme, participants agreed that the requirement to obtain data subject consent in situations such as purpose limitation, acquisition of sensitive personal information, and third-party provision of personal data is increasingly misaligned with data utilisation needs and is seen as a bottleneck in today's digital economy and society.

Provisions to remove the need for data subject consent in certain cases, such as the handling of personal information for AI development, were viewed positively as a means of promoting data access and utilisation. On the other hand, robust data governance remains essential to maintain public trust, including transparency, data security, and measures to mitigate privacy risks.

Participants advocated for flexible legal bases that are co-equal to consent, and a societal commitment to data access and utilisation to recognise the limitations of consent, prevent 'consent fatigue', and ensure Japan remains a global leader in AI innovation.

i. Challenges of Requiring Data Subject Consent in a Digital Economy and Society

With the rapid advancement of digitalisation, vastly larger volumes of data now flow in multiple directions and at great speed compared to when the APPI was originally enacted. To enable AI development, large volumes of data are collected through technologies such as web scraping. In this digital environment, there are many situations in which obtaining data subject consent is difficult or even infeasible, making a consent-based approach less suitable.

ii. Moving Beyond the Consent Principle and Establishing Data Governance

In this digital economy and society, it was considered appropriate to promote data access and utilisation by establishing data governance—including the assurance of trust—without relying solely on data subject consent. Participants welcomed amendments to remove the requirement for consent in cases where personal information is handled for purposes such as AI development.

In building data governance, the government's Data Free Flow with Trust ('DFFT') concept was cited as a useful reference. There was broad agreement on the importance of exploring data governance as a mechanism to ensure the appropriateness of data access and utilisation, while paying close attention to international trends, including DFFT, and rapid economic and societal changes.

As part of this exploration, participants discussed measures to ensure 'trust' under DFFT. While there is no definitive answer, one proposed approach was to enhance transparency through public disclosure and similar measures aimed at ensuring accountability for each company's data utilisation practices. At the same time, it was noted that because data utilisation methods and content may themselves be confidential, disclosures must be balanced to avoid undermining competitiveness or imposing excessive burdens on organisations. In addition to measures to protect data from unauthorised disclosure, trust can also be maintained where

organisations can demonstrate that the benefits of accessing and using data outweigh any residual privacy risks after the application of suitable mitigation measures.

(2) Handling of children's personal information

Under this theme, it was noted that the handling of children's personal information raises issues such as the operational burden and difficulties associated with obtaining consent from legal guardians, as well as consistency with international standards. Participants supported flexible approaches that balance data protection with business burdens, including the use of age management through operating systems (such as iOS and Android) as a better and more effective solution.

i. Practical Challenges of Requiring Legal Guardian Consent

When providing services to children, companies adopt various methods to verify age, such as user declarations or requesting the entry of a date of birth. However, there is no clear guidance or single standard to determine whether legal guardian consent should be obtained, or how to obtain it when required. Accordingly, participants shared the view that if the amended law defines the age at which legal guardian consent is required, due consideration should be given to avoiding excessive burdens and compliance complexities for businesses, such as by allowing organisations to accept a guardian's declaration at face value.

It was also noted that, internationally, many important jurisdictions require legal guardian consent only for children under the age of 13 where consent is the appropriate legal basis. For businesses operating globally, they must consider these international trends and leading standards when complying with domestic regulation. Participants therefore emphasised the importance of flexibility and sufficient grace periods to be provided before implementation. This will also assist Japanese businesses that have, or intend to, internationalise their operations.

ii. Practical Responses that Balance the Protection of Children's Rights and Interests with Business Burdens

While some countries are strengthening regulations, such as by prohibiting children's use of social media, participants shared the understanding that in Japan, regulatory discussions proceed on the premise that children, as members of a digital society, should also benefit from digital services. Accordingly, regulations are being considered to protect children's rights and interests within that framework.

Because such regulations inevitably impose a certain level of burden on businesses, participants emphasised the need to strike an appropriate balance between protecting children's rights and interests and limiting business burdens. Views were shared that flexible operation may be appropriate, such as recognising a legitimate reason for not requiring legal guardian consent in the case of services that are not reasonably expected to be used by children and allowing organisations to provide age-appropriate services and content in accordance with the best interests of the child.

In addition, rather than requiring each service or application to implement separate measures, practical proposals were made to link with parental control mechanisms at the OS level (such as iOS and Android). Participants noted that such a mechanism would be highly effective and efficient from a business perspective, and would also allow parents the convenience of a one-stop approach to oversee and approve their children's digital activities.

(3) Regulation of data relating to physical characteristics

Under this theme, it was noted that data relating to physical characteristics may be acquired or tracked without an individual's awareness. In light of this, proposals were discussed to recognise

the right to request suspension of use of personal data, subject to certain exceptions, while ensuring that socially beneficial uses—such as crime prevention—are not unduly hindered.

As a regulatory approach, it has been proposed that, with certain exceptions, individuals should be entitled to request suspension of use even in the absence of illegality. In response, participants commented that a distinction ought to be drawn between data used for identification (high risk) and data merely related to physical features (low risk). For the former, requirements should not go beyond what is envisaged in the 'Guidelines on the Use of Camera Images', so as to avoid imposing excessive burdens. Consideration should also be given to the socially beneficial aspects of using data relating to physical characteristics—particularly facial data—such as for crime prevention, data retention requirements, protecting individuals' life and physical safety, or providing services that serve individuals' interests and welfare.

(4) Regulation of personal-related information

Finally, with respect to personal-related information such as cookie IDs, there was a discussion that regulations should be extended to prohibit improper use and improper acquisition. Businesses expressed the view that regulatory requirements should be further specified and clarified.

At the same time, it was explained that as long as businesses conduct their operations appropriately, such regulations should not pose issues, and that the proposals are aimed primarily at addressing improper actors, such as unscrupulous data brokers. Participants also shared the expectation that the specific content of what constitutes improper use or improper acquisition should be clearly defined, to recognise existing legal bases for data processing and to protect legitimate business operations carried out in good faith.

4. Conclusion

At this roundtable, multifaceted and practical discussions took place, extending beyond Japan and incorporating perspectives on international initiatives in Singapore.

Looking ahead, ongoing responses will be required as technology advances and society evolves. In a digital economy and society, while data access and utilisation serve as a source of innovation, they must coexist with the protection of individuals' rights and interests in a balanced and practical manner.

From the perspective of future system design, participants agreed that regulatory frameworks should be built on the premise that effective data access and utilisation and the protection of individual rights and interests can coexist. Achieving this balance requires not only defining regulatory requirements and exploring exceptions under existing approaches, but also developing fundamental principles and rules that facilitate responsible data access and utilisation, such as the development of flexible legal bases for data processing that are co-equal to consent, paired with data governance to maintain trust.

To this end, ensuring trust—guided by concepts and principles such as DFFT—is essential, and continued efforts that closely monitor technological progress, societal change, and international trends will be required.