Miura & Partners

Japanese Law Update #19

Roundtable on the Future of Harmonising Personal Information and Privacy Protection with Data Utilisation

2025 年 8 月 7 日

Aiko KANAYAMA
Tomomi HIOKI
Taro TANAKA
Yasuhiro SHIMIZU
Shota EIMURA

■ SUMMARY AND KEY TAKEAWAYS

- On 11 June 2025, Miura & Partners hosted a roundtable focused on harmonising personal information and privacy protection with data utilisation. The discussion centred on two key areas: (1) 'three-year review' of the Act on the Protection of Personal Information ('APPI'), including children's data, biometric data, and advertising regulation; and (2) the newly enacted Act on the Promotion of Research, Development and Utilisation of Artificial Intelligence-Related Technologies (the 'AI Act'). Experts from the private sector, academia, and government agencies participated, sharing diverse perspectives.
- The APPI panel highlighted the importance of balancing children's rights and benefits in digital environments. It advocated for purpose-specific regulations, respect for children's voices, and recognition of practical challenges such as age verification and guardianship in online contexts. Experts concurred that biometric data governance requires nuanced, use-case-based regulation that fosters innovation while ensuring transparency and accountability. This includes addressing risks related to data immutability and potential emotional harm, with an emphasis on policy development grounded in real-world scenarios.
- Regarding AI governance, the AI Act advances innovation and risk management through a PDCA (Plan-Do-Check-Act) cycle. It promotes continuous dialogue between regulators and stakeholders, encourages voluntary company standards, and supports public-private collaboration initiatives like the Hiroshima AI Process.
- The roundtable concluded by emphasising the need for flexible, adaptive regulatory frameworks that balance privacy protection with responsible data and AI use. Static rules are insufficient as risks evolve. Fostering public trust and innovation while avoiding regulatory overreach is essential for Japan's long-term competitiveness. This requires regulatory approaches that incorporate voluntary industry efforts and align with international developments, remaining responsive and proportionate to change.

1. PANEL SESSION I: THE APPI AND ITS THREE-YEARLY REVIEW

A) Protection of Children's Personal Information and Privacy

The panel began by reaffirming the critical need to protect children in digital environments. The discussion moved beyond privacy and data protection, focusing on how to achieve a balanced approach that also considers the benefits children may derive from accessing the internet. Participants exchanged a range of perspectives on how best to align data governance with the broader rights and interests of children.

The panel reaffirmed that any protective approach should be grounded in the best interests of the child and respect for their rights. In this regard, participants noted that children can benefit from using digital services, making it essential to appropriately balance the risks and benefits. As Japan continues to promote digitalisation across society, stakeholders are expected to play a guiding role in helping children safely navigate and thrive in the digital world, ideally starting education at an early age.

When considering specific regulatory frameworks, participants raised several points:

- **Keep issues distinct**: Discussions about protecting children's personal information should be separate from those about the risk of harm in different types of services (e.g., educational services, child-focused services, or general services accessible to children). This distinction helps avoid conflating unrelated issues and enables more targeted approaches.
- **Accommodate diverse service formats**: Traditionally, child-focused services could involve a direct contract with a parent or guardian. However, with more diverse service formats (such as AI-driven services or those offered through schools), seamless compliance is not always feasible.
- **Tailor regulations to purpose**: In some countries, children are restricted or prohibited from using social media. Yet, it is also important to consider the specific needs of children throughout their developmental stage, which evolves with time. Therefore, any regulations should be tailored to the purpose of use and avoid unintended consequences. Rather than applying blanket bans, it is crucial to identify real harms occurring in digital spaces and regulate them appropriately through laws, corporate efforts, and broader societal initiatives.
- **Respect the child's voice**: Children have the right to be heard, but they are often presumed vulnerable. It is therefore essential to ensure that their intentions and voices are accurately reflected. In some cases, a parent or guardian's intentions may not always align with the child's own will, rights, or best interests. Thus, understanding the child's intentions and circumstances – such as when a child sends an SOS via social media – must be done carefully and respectfully.
- **Recognise practical limitations**: Verifying a child's age or a guardian's status online often requires measures beyond what is realistically manageable. Furthermore, service providers could face a heavy and complex burden if expected to identify parents or guardians and fulfil related obligations across both digital and physical environments in every context.

These discussions reaffirmed that a key challenge going forward will be how to strike an appropriate balance between protecting children's rights and personal information, while also responding to the realities of how data is used in society. Participants emphasised the importance of considering both voluntary initiatives by companies and the approaches taken by global firms operating across jurisdictions. It was further suggested that future discussions

should explore not only whether regulation is needed, but also what form it should take – whether through legal frameworks or self-regulatory models.

B) Protection of Biometric Data

Biometric data is widely used for purposes such as security and authentication, and more advanced, beneficial applications are emerging – for example, the use of AI to analyse voice and facial expression data to infer emotional states and detect signs of discouragement and provide responses. At the same time, participants noted that such initiatives often lack transparency: individuals and the wider public frequently have little visibility into how biometric data is collected, processed, or used. This has raised concerns about how to ensure accountability and oversight in practice.

The discussion also focused on how to manage the risks inherent in biometric data in a way that does not unduly inhibit innovation. It was emphasised that regulatory approaches should reflect both the unique characteristics of biometric data – such as its immutability – and the specific contexts in which it is used. Participants stressed that the appropriate form and scope of regulation may vary across different use cases and should not follow a one-size-fits-all model. More specifically, it was noted that regulating all types of biometric data indiscriminately risks stifling innovation. Therefore, a nuanced approach is needed that distinguishes between biometric data used for identification purposes and other identifiable data. This definitional clarity is important to focus on protections appropriately.

There was particular concern about the emotional and psychological harm that could result if biometric data with immutable characteristics – such as facial features – were leaked. This led to a broader reflection on how to reconcile the unpredictability and rapid pace of innovation with the need to ensure appropriate remedies and safeguards in the event of harm.

The discussion also highlighted challenges around consent and training data management. For example, deleting training data used in AI systems can be difficult due to the need to maintain consistency in AI outputs. Additionally, issues such as the nature of the AI model, and the stability of features (e.g., facial features) over time complicate data management. It was also noted that the problem of data deletion should be carefully examined without conflating it with the purpose of data use.

It was also observed that biometric data may be collected in ways that are difficult or impossible for individuals to detect or control, especially in the case of facial data. Moreover, the risks associated with such data do not depend solely on the type of data itself, but also vary depending on how and in what context it is used. In this light, participants agreed that businesses utilising biometric data bear a responsibility to be transparent about potential risks and to actively engage in meaningful communication with users. These practices are essential to maintaining a safe and trustworthy environment.

Finally, the panel shared the view that future discussions should move beyond generalised or abstract notions of risk. Instead, policy debates should be grounded in specific, real-world scenarios. Resources such as the 'Guidelines on the Use of Camera Images' were cited as useful references for developing concrete, use-case-based approaches to regulation.

C) Advertising Regulation

The panel then discussed potential additional regulations for 'personally related information,' including Cookie IDs and data equivalent to pseudonymised or anonymised information. Key points included:

- **Unclear scope of regulation**: Phishing scams and fraudulent ads were identified as targets for regulation. However, in practice, the boundaries of what falls under these rules are unclear to businesses, leading to concerns that innovation could be stifled.
- **Shift in regulatory approach**: Unlike the Telecommunications Business Act (which sets procedural rules for third-party data transmission), the APPI has shifted toward substantive regulation and downstream (output-side) controls.
- **Possible alternatives to regulation**: Some participants suggested that, in certain cases, additional rules may not be necessary if businesses can identify risks in their operations and proactively disclose relevant information to consumers.
- **Avoiding a chilling effect**: Even if new regulations are needed, discussions should proceed carefully to eliminate uncertainty and avoid a chilling effect on legitimate advertising activities. Voluntary initiatives and transparency by companies can be alternatives or complements to heavy-handed regulation.

2. PANEL SESSION II: NEW LEGAL FRAMEWORKS FOR THE AI ERA – JAPAN'S STRATEGY FOR BALANCING INNOVATION AND TRUST

The second panel session centred on how to establish governance that both promotes innovation in AI and manages its associated risks, especially in light of the recent AI Act. This topic generated a lively discussion.

A) Rethinking Traditional Legal Approaches in the Age of AI

Traditionally, when introducing new laws to regulate technology, several conditions have been considered necessary: (i) establishing certain legislative facts, (ii) ensuring the legislative objective is legitimate based on those facts, and (iii) maintaining a reasonable relationship between that objective and the regulatory means. This approach relies on three key assumptions: potential risks can be predicted in advance; the processes or rules to mitigate risks or achieve desired outcomes can be clearly defined; and if something goes wrong, a responsible party can be clearly identified.

However, AI fundamentally challenges these assumptions. AI systems are often unpredictable in their behaviour and risks; their internal processes are complex and hard to fully explain; and it is not always clear who should be held responsible when issues arise. The panel agreed that it is crucial to re-examine these traditional premises as we develop future AI governance, and participants shared helpful suggestions to address the issues. They highlighted the importance of adopting a mindset of experimentation and iteration – trying new technologies first and fixing problems as they arise – rather than rejecting innovation due to imperfections.

B) The AI Act and the PDCA Cycle

The AI Act has a dual aim: to promote national well-being and economic growth (i.e., innovation) while also addressing the risks associated with AI. To achieve this, the Act adopts a governance approach based on the PDCA (Plan-Do-Check-Act) cycle, allowing for flexible

responses to rapidly evolving AI technologies. Notably, the Act does not introduce any new penalties.

Specifically, the AI Act acknowledges that inappropriate use of AI can lead to issues such as personal data breaches or copyright infringements. To ensure AI is developed and used appropriately, the Act requires steps like maintaining transparency in development and usage processes. The Act's supplementary provisions also call for periodic reviews after enactment. The government must examine how the law is working in light of international trends and socio-economic changes, and take follow-up measures as needed. The panel noted that this continuous cycle of review and improvement makes it easier to respond to unforeseen consequences of AI use.

The panel emphasised that for the PDCA-based governance to be effective, active dialogue (engagement) between regulators and stakeholders (including businesses and consumers) is essential. Under the AI Act, if AI research, development, or use harms the public's rights or interests, the government must investigate the cause and then provide guidance, advice, information, and other necessary measures to developers and service providers. This dialogue-focused approach allows flexible and swift responses when issues arise. The session concluded that such an approach helps businesses tackle problems quickly without becoming overly risk-averse in the face of sudden regulatory enforcement.

C) Ensuring Innovation in the Private Sector

The panel stressed the importance of rules that do not stifle innovation. As noted, the AI Act carries no penalties and is designed to be flexible as technology evolves. Participants highlighted that governance must remain effective while avoiding rigid or excessive regulation that could dampen companies' motivation to innovate. Striking this balance is vital to ensure businesses have opportunities to test new technologies and develop new services.

Many Japanese companies have a strong culture of quality control and legal compliance, often closely following government guidelines and industry standards. The government, for its part, respects these voluntary private-sector efforts and aims to foster a virtuous cycle driven by such initiatives. The panel suggested that companies can build public trust and accelerate innovation by proactively self-regulating and being transparent (for example, through open information disclosure).

For global companies, it is essential to comply not only with domestic laws but also with the regulations of every country where they operate. The panel noted that being transparent about compliance across different jurisdictions is a critical corporate responsibility. Participants also highlighted the importance of public–private collaboration in AI governance. For instance, under the Hiroshima AI Process (launched by Japan at the G7 Hiroshima Summit), a voluntary reporting framework was created to allow companies to share information with government authorities. Strengthening this kind of public-private engagement was identified as a key priority.

D) AI & Governance

When it comes to AI governance, the starting point should be a clear understanding of AI's risks and benefits. The panel observed that both the risks and the societal value of AI evolve over time. Therefore, it is important not to be bound by fixed assumptions. Instead, stakeholders should assess risks case by case, considering the technology's maturity and the current social context. For example, as generative AI introduces new privacy and intellectual property challenges, regulators will need to continually assess actual risks and craft appropriate countermeasures.

The panel also noted that effectively implementing the PDCA cycle (as outlined in the AI Act) requires action not only at the policy level but also on the ground. Companies on the front lines should take the initiative to develop their own standards (sometimes called 'intermediate norms') and actively run PDCA cycles in their operations. By doing so, they can build best practices through real-world experience. This hands-on approach is expected to create an environment where businesses can confidently develop and use AI without falling into excessive self-restraint.

3. CONCLUSION AND WAY FORWARD

The roundtable provided an opportunity for in-depth, practice-oriented discussion on the future design of regulatory frameworks that balance the protection of personal information and privacy with the effective use of data and AI. As technology continues to evolve and societal contexts shift, the risks associated with data use are becoming increasingly complex and diverse. Participants shared the view that static, one-size-fits-all rules are insufficient, and that regulatory responses must instead be flexible, adaptive, and subject to ongoing review.

Looking ahead, there was broad agreement that fostering public trust and social acceptance — while avoiding regulatory overreach that could stifle innovation — will be essential to maintaining Japan's long-term competitiveness. Achieving this will require regulatory approaches that take into account both voluntary industry efforts and international developments, and that are capable of responding to change in a balanced and proportionate manner.

Authors

Aiko Kanayama, Partner

Aiko Kanayama graduated from the University of Tokyo, Faculty of Law in 2001 and was admitted to the bar in 2005 (Daini Tokyo Bar Association). Before joining Miura & Partners in January 2019, she held positions at Mori Hamada & Matsumoto, the Ministry of Land, Infrastructure, Transport and Tourism, and Google LLC. Her practice focuses on regulatory compliance, data protection, and corporate governance across a wide range of sectors.

Tomomi Hioki, Partner

Tomomi Hioki passed the Japanese Bar Examination in 2008. After completing legal training, she served as a policy secretary to members of the National Diet, and later as Deputy Director at the Cabinet Secretariat's IT Strategy Office, where she was involved in designing and implementing the 2017 amendment to the Act on the Protection of Personal Information (APPI). She now advises clients on all aspects of data governance, including compliance, reputational risk, CSR, government relations, and crisis response, providing strategic support tailored to each organisation's needs. She also contributes as a member of various expert panels convened by public and private sector bodies.

Taro Tanaka, Partner

Taro Tanaka joined Miura & Partners following experience at a major Japanese law firm and with the United Nations in both Geneva and New York. His practice spans international transactions, AI regulation, business and human rights, ESG/SDGs, D&I, international arbitration, and Southeast Asia-related matters. A Fulbright Scholar, he earned his LL.M. in the U.S. and subsequently worked on human rights issues in conflict zones, including Ukraine and Myanmar. He has represented victims before international tribunals, including the International Criminal Court.

Yasuhiro Shimizu, Associate

Yasuhiro Shimizu graduated from Meiji University (Faculty of Law) in 2014 and Waseda Law School in 2016. He was admitted to the bar in 2017 (Ichiben) and became a certified social insurance and labour consultant in 2020. After practising at Takai & Okazeri Law Office, he joined Miura & Partners in May 2021. From March 2022 to June 2024, he was seconded to the Digital Agency, where he worked on the legislative design and implementation of major regulatory reforms, including the 2023 digital reform bill and the 2024 base registry and digital procedure law. His practice focuses on data protection, digital regulation, and employment law.

Shota Eimura, Associate

Shota Eimura was admitted to the bar in 2022 and joined Miura & Partners in August 2024 after practising at Nishimura & Asahi. He handles a broad range of corporate matters, including crisis management, internal investigations, regulatory enforcement, litigation and dispute resolution. He also advises on consumer protection – particularly the Act against Unjustifiable Premiums and Misleading Representations – and employment law.