
CHAMBERS GLOBAL PRACTICE GUIDES

Artificial Intelligence 2025

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

Japan: Law & Practice

Keiji Tonomura, Yukiko Konno,
Minh Thi Cao Koike
and Yoshiteru Matsuzaki
Nagashima Ohno & Tsunematsu



JAPAN

Law and Practice

Contributed by:

Keiji Tonomura, Yukiko Konno, Minh Thi Cao Koike and Yoshiteru Matsuzaki
Nagashima Ohno & Tsunematsu



Contents

1. General Legal Framework p.6

1.1 General Legal Background p.6

2. Commercial Use of AI p.7

2.1 Industry Use p.7

2.2 Involvement of Governments in AI Innovation p.7

3. AI-Specific Legislation and Directives p.8

3.1 General Approach to AI-Specific Legislation p.8

3.2 Jurisdictional Law p.8

3.3 Jurisdictional Directives p.8

3.4 EU Law p.8

3.5 US State Law p.8

3.6 Data, Information or Content Laws p.9

3.7 Proposed AI-Specific Legislation and Regulations p.10

4. Judicial Decisions p.10

4.1 Judicial Decisions p.10

5. AI Regulatory Oversight p.11

5.1 Regulatory Agencies p.11

5.2 Regulatory Directives p.12

5.3 Enforcement Actions p.13

6. Standard-Setting Bodies p.13

6.1 National Standard-Setting Bodies p.13

6.2 International Standard-Setting Bodies p.14

7. Government Use of AI p.15

7.1 Government Use of AI p.15

7.2 Judicial Decisions p.15

7.3 National Security p.15

8. Generative AI p.16

8.1 Specific Issues in Generative AI p.16

8.2 Data Protection and Generative AI p.17

9. Legal Tech p.17

9.1 AI in the Legal Profession and Ethical Considerations p.17

10. Liability for AI p.18

10.1 Theories of Liability p.18

10.2 Regulatory p.19

11. Specific Legal Issues With Predictive and Generative AI p.19

11.1 Algorithmic Bias p.19

11.2 Facial Recognition and Biometrics p.19

11.3 Automated Decision-Making p.20

11.4 Transparency p.20

12. AI Procurement p.21

12.1 Procurement of AI Technology p.21

13. AI in Employment p.21

13.1 Hiring and Termination Practices p.21

13.2 Employee Evaluation and Monitoring p.23

14. AI in Industry Sectors p.24

14.1 Digital Platform Companies p.24

14.2 Financial Services p.24

14.3 Healthcare p.24

14.4 Autonomous Vehicles p.26

14.5 Manufacturing p.26

14.6 Professional Services p.26

15. Intellectual Property p.27

15.1 IP and Generative AI p.27

15.2 Applicability of Patent and Copyright Law p.28

15.3 Applicability of Trade Secrecy and Similar Protection p.28

15.4 AI-Generated Works of Art and Works of Authorship p.29

15.5 OpenAI p.30

16. Antitrust p.30

16.1 Emerging Antitrust Issues in AI p.30

17. Cybersecurity p.31

17.1 Applicability of Cybersecurity Legislation to AI p.31

18. ESG p.32

18.1 ESG Dimensions of AI p.32

19. AI Governance and Compliance p.32

19.1 AI Governance and Best Practice Compliance Strategies p.32

Contributed by: Keiji Tonomura, Yukiko Konno, Minh Thi Cao Koike and Yoshiteru Matsuzaki,
Nagashima Ohno & Tsunematsu

Nagashima Ohno & Tsunematsu is the first integrated full-service law firm in Japan and one of the foremost providers of international and commercial legal services based in Tokyo. The firm's overseas network includes offices in New York, Singapore, Bangkok, Ho Chi Minh City, Hanoi and Shanghai, as well as collaborative relationships with prominent local law firms throughout Asia and other regions. The TMT practice group comprises about 50 lawyers and legal professionals and represents major Japa-

nese telecommunications carriers, key TV networks, and many domestic and international internet, social media and gaming companies not only in transactions but also in disputes, regulatory matters and general corporate matters. Another strength of the TMT practice group is that – in view of the firm's robust client base – it is well positioned to consistently meet requests from clients to provide advice in many different areas, from business strategies to daily compliance and corporate matters.

Authors



Keiji Tonomura is a partner at Nagashima Ohno & Tsunematsu. His practice focuses on M&A, IP/IT-related transactions, and data security/privacy matters, with a particular focus on the

TMT sectors, including new business fields such as fintech, AI and blockchain. Keiji has served as a member of the working group within the Japanese Ministry of Economy, Trade and Industry (METI)'s Study Group on AI and Data Contract Guidelines since January 2018 and has been a member of the Liberal Democratic Party's Project Team on the Evolution and Implementation of AIs since 2023. He has also been a member of Tokyo Dai-ichi Bar Association since 2007.



Yukiko Konno is a counsel at Nagashima Ohno & Tsunematsu. Leveraging her experience of participating in policy discussions on international data flow frameworks and AI

governance at Japan's Ministry of Economy, Trade and Industry (METI), Yukiko focuses on delivering comprehensive legal advice in various technology-related fields. Her expertise particularly emphasises AI governance, data privacy and protection (both domestic and international), and cybersecurity. Yukiko is a member of Tokyo Dai-ichi Bar Association (since 2009).

Contributed by: Keiji Tonomura, Yukiko Konno, Minh Thi Cao Koike and Yoshiteru Matsuzaki,
Nagashima Ohno & Tsunematsu



Minh Thi Cao Koike is a counsel at Nagashima Ohno & Tsunematsu. He advises domestic and foreign tech companies, internet service companies and

telecommunications companies on technology-related law and privacy regulations, and also has extensive experience in domestic and international M&A transactions involving tech companies. Minh was admitted to the Bar in Japan (Tokyo Dai-ichi Bar Association) in 2010 and in New York in 2017. He co-authored a book on legal tech in 2020 and a book on web3 and metaverse in 2024.



Yoshiteru Matsuzaki is a senior associate at Nagashima Ohno & Tsunematsu, where his practice focuses on technology and complex commercial transactions. Yoshiteru has more

than ten years' experience both as an in-house counsel at a global tech giant and as a private practice lawyer. He received an LLB from Tokyo University of the Arts and an LLM (Law and Technology Certificate) from University of California, Berkeley.

Nagashima Ohno & Tsunematsu

JP Tower
2-7-2 Marunouchi
Chiyoda-ku
Tokyo 100-7036
Japan

Tel: +81 3 6889 7000
Fax: +81 3 6889 8000
Web: www.noandt.com/en/

NAGASHIMA
OHNO &
TSUNEMATSU

Contributed by: Keiji Tonomura, Yukiko Konno, Minh Thi Cao Koike and Yoshiteru Matsuzaki,
Nagashima Ohno & Tsunematsu

1. General Legal Framework

1.1 General Legal Background

Despite the absence of comprehensive AI-specific legislation in Japan, several general legal frameworks apply to AI technologies, as follows.

Tort Law (Civil Code)

Under Article 709 of Japan's Civil Code, liability may arise from intentional or negligent actions that infringe on rights or legally protected interests, including harm caused by AI. Tort law provisions encompass potential liabilities for AI users, developers or providers based on their foresight and preventive measures.

Privacy and Data Protection Law

The Act on the Protection of Personal Information (APPI) regulates the processing of personal data in developing, training and utilising AI. For details, see **8.2 Data Protection and Generative AI**.

IP Law

Copyright and patent laws are both applicable to AI – although their application remains debated. The Copyright Act includes provisions such as Article 30-4 that permit the use of copyrighted works for information analysis without the consent of the copyright holder and such provisions can apply to AI training under certain conditions. For detailed analysis, see **15. Intellectual Property**.

Criminal Law

The Japanese Penal Code encompasses various crimes that may apply when AI is misused, including fraud (Article 246), defamation (Article 230), and obstruction of business (Article 233). The risks particularly emerge with generative AI, which can create deepfakes or synthesised content that may be used in fraud schemes,

impersonation, or business interference. Additionally, the Unauthorised Computer Access Law addresses AI-related misconduct, including unauthorised computer access (Article 11) and the unlawful acquisition of identifiers such as passwords (Article 12).

Antitrust Law

The Act on Prohibition of Private Monopolisation and Maintenance of Fair Trade (the “*Anti-Monopoly Act*”) addresses the potential risks of monopolistic practices or anti-competitive behaviours involving AI and algorithms, as detailed in **16.1 Emerging Antitrust Issues in AI**. Particular risks include inadvertent price coordination when competitors use similar AI systems and potential market dominance through data accumulation.

Labour Law

The Employment Security Act governs collection of applicant information using AI in hiring processes – although current labour laws lack specific provisions on autonomous decision-making systems. Key concerns include potential discrimination in AI-based hiring and evaluation systems. For more details on AI in employment contexts, see **13. AI in Employment**.

Product Liability Law

Under Japan's Product Liability Act, manufacturers are liable for damages caused by defective products that harm life, body or property, irrespective of the manufacturer's negligence. Although standalone AI software may not qualify as “*product*”, if integrated into a device, the entire assembly is considered a product. Determining what constitutes adequate safety for AI and proving defects remain challenging, particularly for systems whose decisions may not be fully explainable.

Contributed by: Keiji Tonomura, Yukiko Konno, Minh Thi Cao Koike and Yoshiteru Matsuzaki,
Nagashima Ohno & Tsunematsu

Consumer Protection Law

AI applications provided to consumers are subject to consumer protection laws in Japan. The Act Against Unjustifiable Premiums and Misleading Representations could apply when generative AI is used in advertising that creates misleading or deceptive impressions about the quality and/or terms and conditions of products or services. Additionally, the Consumer Contract Act protects consumers from unfair solicitation practices, which could include those conducted by AI-driven systems such as robo-advisers. These existing consumer protection frameworks apply to AI applications.

2. Commercial Use of AI

2.1 Industry Use

AI and machine learning are transforming various industries in Japan, with predictive and generative AI technologies both driving innovation and efficiency across sectors, as follows.

- Financial services – predictive AI detects fraud and forecasts market trends for risk management and investment strategies. Major Japanese banks have integrated generative AI for automated reporting, personalised financial advice, and enhanced customer support systems.
- Healthcare – AI-based diagnostic support systems assist medical professionals in interpreting imaging data and identifying potential health issues. Generative AI is accelerating drug discovery through molecular structure design and streamlining medical documentation through automated summarisation.
- Manufacturing – companies implement predictive maintenance systems that reduce equipment downtime and optimise production processes. Generative AI is enhancing

manufacturing by enabling natural language-controlled robotics and automating complex design tasks, particularly in the automotive and electronics sectors.

- Retail – predictive analytics optimise inventory management and supply chain operations. Generative AI is creating personalised shopping experiences, virtual shopping assistants, and automatically generating product descriptions and marketing materials.
- Design and advertising – creative industries utilise generative AI for innovative package design and creating virtual brand personalities for commercials. One beverage company has notably launched a campaign featuring AI-generated characters and packaging designs.
- IT – generative AI supports software development by automating code generation, testing, and system operations, thereby accelerating development cycles.

2.2 Involvement of Governments in AI Innovation

The Japanese government continues to strengthen its AI development strategy in 2025 through targeted investments and strategic policy frameworks. For fiscal year 2025, Japan allocated approximately JPY196.9 billion for AI-related activities.

In November 2024, the government announced the “*AI and Semiconductor Industry Strengthening Framework*”, which plans for JPY10 trillion in public support by 2030. Although a significant portion of this framework focuses on next-generation semiconductor development, it also encompasses AI technologies. The 2025 fiscal year marks the first year of this framework’s implementation, with the budget including fundamental research for innovative AI semicon-

ductors (JPY40 billion) as one component of the broader initiative.

The government has established sector-specific strategies for AI implementation across priority industries. In healthcare, the Cabinet Office is leading a JPY22 billion investment in generative AI development for medical diagnostic support. In the transportation sector, the government is providing financial support for Level 4 autonomous driving initiatives in 50 regions nationwide.

3. AI-Specific Legislation and Directives

3.1 General Approach to AI-Specific Legislation

Currently, there is no comprehensive cross-sectoral legislation regarding AI. As stated in “*AI Governance in Japan Version 1.1*”, the reason for this lies not only in the belief that comprehensive regulations are currently unnecessary from the perspective of fostering innovation but also in the idea that it may be preferable to respect rule-making at the individual sector level in certain specific fields, such as the automotive and medical sectors.

In individual legal domains, such as the APPI and the Copyright Act, rules and amendments to existing laws are being made to promote the utilisation of AI. One such introduction occurred in 2023, with the Next-Generation Medical Infrastructure Act, which is a special law under the APPI. Specifically, to facilitate the use of AI in research and development in the medical field, the Next-Generation Medical Infrastructure Act introduced the concept of pseudonymised medical data through an amendment in May 2023. This is expected to promote research and devel-

opment of AI diagnostic tools utilising big data in the medical field.

Furthermore, the government has provided guidance on the interpretation of existing laws and regulations in relation to the use of AI (see 3.3 **Jurisdictional Directives**). Although these are not binding interpretations, they serve as useful references for businesses.

3.2 Jurisdictional Law

In Japan, there are currently no specific laws or regulations that apply exclusively to AI; instead, there are only regulations within individual areas of law. For details on the proposed AI-specific legislation currently under consideration, please refer to 3.7 **Proposed AI-Specific Legislation and Regulations**.

3.3 Jurisdictional Directives

On 19 April 2024, the Ministry of Economy, Trade and Industry (METI) and the Ministry of Internal Affairs and Communications (MIC) released the “*AI Guidelines for Businesses*” (an updated Version 1.1 was subsequently released on 28 March 2025). These guidelines propose a framework aiming to balance the promotion of innovation and the mitigation of risks by providing unified guidelines for AI governance in Japan.

3.4 EU Law

3.4.1 Jurisdictional Commonalities

There is no applicable information in this jurisdiction.

3.4.2 Jurisdictional Conflicts

There is no applicable information in this jurisdiction.

3.5 US State Law

There is no applicable information in this jurisdiction.

Contributed by: Keiji Tonomura, Yukiko Konno, Minh Thi Cao Koike and Yoshiteru Matsuzaki,
Nagashima Ohno & Tsunematsu

3.6 Data, Information or Content Laws

What follows is a discussion of how data protection laws and information and content laws in Japan have evolved or been introduced to foster AI technology, as well as the role of public body recommendations or directives in this context.

Data Protection Laws

In Japan, the APPI covers data protection. Its recently introduced rules and guidance concerning AI are as follows.

AI development and use of personal information

According to the default rules of the APPI, when collecting and using personal information, such information can only be used for the purposes specified at the time of collection. Changing those purposes requires the consent of the individual. However, with the introduction of “*pseudonymised personal information*” (ie, information processed in a way that renders it impossible to identify a specific individual unless collated with other information) in the amended APPI enacted in 2022, it is now permitted to change the purposes of the use of collected personal information without the consent of the individual – making it easier to use collected personal data in AI machine learning.

In March 2023, the Personal Information Protection Commission (PPC) announced “*The Use of Camera Systems With Facial Recognition Function for Crime Prevention and Safety Assurance*”. While not introducing new rules or interpretations under the APPI, this serves as a reference guide for private businesses utilising facial recognition technology for purposes such as crime prevention.

Handling of generative AI and personal information

The PPC’s “*Cautionary Notes on the Use of Generative AI Services*” (June 2023) outlines the following points of caution for businesses.

When businesses input prompts containing personal information into generative AI services, it is crucial to ensure that the scope of the data used is strictly necessary to achieve the specified purposes. If businesses input prompts containing personal information into generative AI services without obtaining prior consent from the individuals, and if the personal information is used for purposes other than responding to the prompt, such businesses may violate the provisions of the APPI. Therefore, when inputting such prompts, it is essential to confirm that the service provider does not use the personal information for machine learning or similar purposes.

On 3 February 2025, the PPC issued an alert concerning DeepSeek. According to the alert, data obtained by DeepSeek, including personal information collected through the use of its services, is:

- stored on servers located in China; and
- subject to Chinese legislation, including the Cybersecurity Law of China.

On 5 March 2025, the PPC released its views on future amendments to the APPI in a document titled “*Considerations on Institutional Issues of the APPI*”. The document proposes that, under certain conditions, the handling of personal data solely for the purpose of obtaining and utilising generalised and versatile analytical results – where relationships with identifiable individuals are excluded, such as in the creation of statistical data – may be conducted without obtaining the data subject’s consent. It is also noted that

Contributed by: Keiji Tonomura, Yukiko Konno, Minh Thi Cao Koike and Yoshiteru Matsuzaki,
Nagashima Ohno & Tsunematsu

such statistical data creation could encompass certain AI development activities. As of now, no specific amendments to the law have been enacted.

Copyright Laws

AI development and the use of existing works

Under the Copyright Act, using works without the consent of the copyright owner can lead to copyright infringement. However, Japan has a specific provision that does not consider it an infringement to use works for information analysis purpose (Article 30-4 of the Copyright Act). This makes it relatively easy to use third-party works for AI machine learning in Japan. However, there are restrictions when the purpose of such use of works includes enjoying the thoughts or sentiments expressed in a work, or when it unfairly harms the interests of the copyright owner.

Generative AI and copyright infringement

On 29 February 2024, the Agency for Cultural Affairs released a report detailing its interpretation of copyright laws concerning AI and copyright. This report outlines the criteria for recognising AI-generated works as copyrighted works, as well as the basic principles regarding copyright infringement when AI-generated works that are similar to the original works are used.

On 31 July 2024, the Agency for Cultural Affairs released the *“Checklist and Guidance on AI and Copyright”*, providing guidance for AI developers, providers, users and the general public on how to avoid copyright infringement. Although the guidance itself does not carry legal binding force, it serves as an explanatory resource supplementing documents such as *“Concepts Regarding AI and Copyright”*. The guidance introduces practices that are considered desirable both for AI developers and others seeking

to mitigate risks arising from the intersection of copyright and generative AI, as well as for business or individuals aiming to preserve and exercise their rights. It is therefore expected to serve as a valuable reference for AI developers, users, and other stakeholders.

3.7 Proposed AI-Specific Legislation and Regulations

On 28 February 2025, the Japanese government approved and submitted to the National Diet the *“Bill on the Promotion of Research, Development and Utilisation of Artificial Intelligence-Related Technologies”* (the *“AI Bill”*). The AI Bill aims to promote the research, development and utilisation of AI by providing for the formulation of a basic government plan and the establishment of the Artificial Intelligence Strategy Headquarters. As for obligations imposed on businesses, the AI Bill merely stipulates a duty for AI-utilising businesses to co-operate with national policies and initiatives, without prescribing any penalties for non-compliance. Accordingly, unlike the EU’s AI Act (which imposes stringent regulatory obligations on businesses), the AI Bill is positioned as *“framework law”* that primarily establishes fundamental principles to promote the development and utilisation of AI, without introducing heavy compliance burdens.

4. Judicial Decisions

4.1 Judicial Decisions

First, in June 2022, the Tokyo District Court ruled that the operator of Tabelog (a well-known Japanese restaurant ratings site) was found liable for damages under the Anti-Monopoly Act for *“abuse of a superior bargaining position”* by changing its algorithm to the disadvantage of some users and continuing to use the changed algorithm. Thus far, the Japan Fair Trade Com-

mission (JFTC) has indicated that a restaurant ratings site may have a superior position and that acts such as unilaterally changing the algorithm and forcing restaurants to conclude contracts favourable to the site may constitute an abuse of a superior position.

On the other hand, in January 2024, the Tokyo High Court (court of appeal) ruled that the ratings site operators may have a superior bargaining position but they were not liable for *“an abuse of a superior bargaining position”* given that the purpose of the change and the manner in which the algorithm was changed in this case were reasonable. The case is currently on final appeal.

The above-mentioned judgments are still considered to be highly influential decisions because:

- an abuse of a superior bargaining position was found based solely on the fact that the algorithm was changed to the disadvantage of the parties; and
- the reason for changing the algorithm largely determines whether the act was carried out unjustly in light of normal business practices, which is one of the requirements for *“an abuse of a superior bargaining position”*.

Regarding the second point, this lawsuit is notable from the perspective of information asymmetry, which is an aspect of AI services.

In addition, the fact that the ratings site operators initially refused to disclose the algorithm itself – which was an issue in the process of this lawsuit – as highly confidential information but eventually agreed to disclose it became noteworthy. In this regard, this lawsuit is also notable from the perspective of the principle of transparency, which is an aspect of AI governance.

Further, on 16 May 2024, the Tokyo District Court ruled that an *“inventor”* as defined in the Patent Act is limited to natural persons and does not include AI (see **15.2 Applicability of Patent and Copyright Law**).

5. AI Regulatory Oversight

5.1 Regulatory Agencies

Although the Cabinet Office has formulated a national strategy for AI and the pending AI Bill (see **5.2 Regulatory Directives**) would establish an Artificial Intelligence Strategy Headquarters within the Cabinet to lead and co-ordinate national AI policy, there are currently no cross-sectional and binding laws and regulations for AI in Japan (see **1.1 General Legal Background**). Therefore, there is no regulatory authority that plays a leading role in regulating AI. Instead, the following ministries and agencies are primarily responsible for the enforcement of AI-related laws by sector and application within the scope of the laws and regulations under their jurisdiction.

In relation to AI, the Ministry of Health, Labour and Welfare (MHLW) has jurisdiction over labour laws (ie, the Labour Standards Act, the Labour Contract Act, and Employment Security Act, among others) and the Pharmaceutical and Medical Devices Act (PMDA). In connection with labour laws, the MHLW addresses AI-related employment issues, such as the use of AI in recruitment, personnel evaluation and the monitoring of employee (see **13. AI in Employment**). In connection with the medical devices field, there is a move to accommodate AI-enabled medical devices under the PMDA (see **14.3 Healthcare**).

Contributed by: Keiji Tonomura, Yukiko Konno, Minh Thi Cao Koike and Yoshiteru Matsuzaki,
Nagashima Ohno & Tsunematsu

The Ministry of Land, Infrastructure, Transport and Tourism (MLIT) has jurisdiction over the Road Traffic Act, which establishes rules for automated driving.

The METI has jurisdiction over various AI-related laws and regulations (such as the Unfair Competition Prevention Act, which protects big data as “*limited provision data*”) and is actively formulating guidelines and other relevant materials for businesses involved in the development and utilisation of AI, such as the “*Contract Guidelines on Utilisation of AI and Data Version 1.1*” and the “*AI Guidelines for Businesses*” (see **3.3 Jurisdictional Directives**). In addition, the Japan Patent Office (JPO) (an external bureau of METI) has jurisdiction over the Patent Act (see **15.2 Applicability of Patent and Copyright Law** regarding the protection of AI-enabled technologies and datasets under the Patent Act).

The PPC has jurisdiction over the APPI. The PPC addresses APPI-related issues where personal data is involved in the development and use of AI.

The JFTC has jurisdiction over the Anti-Monopoly Act and the Subcontract Act. The JFTC addresses issues that the use of AI, including AI and algorithmic price adjustment behaviour and dynamic pricing, may have on a fair competitive environment.

The Financial Services Agency (FSA) has jurisdiction over the Banking Act and the Financial Instruments and Exchange Act, among others. The FSA addresses risks and other issues related to investment decisions by AI for financial instrument business operators (see **14.2 Financial Services**).

The Agency for Cultural Affairs has jurisdiction over the Copyright Act. For further details regarding the protection of AI-enabled technologies and datasets under the Copyright Act, please refer to **15.2 Applicability of Patent and Copyright Law**.

The MIC addresses the policy related to information and communication technologies (including the policy related to advancement of network systems with AI as a component). As noted earlier in this section, the MIC jointly issued the “*AI Guidelines for Businesses*” with the METI.

5.2 Regulatory Directives

Japan’s AI-governance regulatory framework is primarily anchored by Version 1.1 of the “*AI Guidelines for Businesses*” issued jointly by the METI and the MIC on 28 March 2025. In addition, the Cabinet-approved AI Bill – once enacted – will become the other main pillar of the regime.

The “*AI Guidelines for Businesses*” create a non-binding “*soft law*” framework that helps organisations develop, provide and use AI safely and responsibly across the entire life cycle. Grounded in the human-centric principles of dignity, diversity, inclusion and sustainability first articulated in “*Social Principles of Human-Centric AI*” (2019), the document adopts a risk-based, goal-oriented, agile-governance approach. It sets out:

- overarching ideals and ten core cross-cutting guidelines – human-centricity, safety, fairness, privacy, security, transparency, accountability, literacy, fair competition and innovation – plus additional duties for advanced AI systems aligned with the G7 Hiroshima AI Process;
- detailed, role-specific expectations for AI developers, providers and business users covering data governance, bias mitigation, safety testing, red-teaming, documentation,

Contributed by: Keiji Tonomura, Yukiko Konno, Minh Thi Cao Koike and Yoshiteru Matsuzaki,
Nagashima Ohno & Tsunematsu

- stakeholder disclosure and incident response; and
- a living-document mechanism so that multi-stakeholder dialogue, international standards work, and emerging regulation can be reflected in the “*AI Guidelines for Businesses*” promptly.

The “*AI Guidelines for Businesses*” therefore aims to balance promotion of innovation with mitigation of evolving social, legal and technical risks, enabling trustworthy AI deployment that supports Japan’s broader Society 5.0 vision while remaining interoperable with OECD, EU and other global frameworks.

The AI Bill, approved by the Cabinet on 28 February 2025 and now before the Diet, would become the country’s first AI-specific statute, setting out a soft-law, innovation-oriented framework rather than imposing EU-style hard obligations on private actors. The 28-article bill is largely a basic law, as it:

- enshrines broad principles;
- instructs the government to draw up a comprehensive AI Basic Plan;
- creates a Cabinet-level AI Strategy Headquarters that will collect data on AI R&D and use, analyse risk incidents and issue guidance and other measures; and
- promotes shared infrastructure, HR development, and international co-operation.

Only one provision addresses private business entities (ie, developers, providers and business users of AI systems), requiring them to strive for active AI adoption and to co-operate with national or local government’s measures. There are no penalties for non-compliance except that failure to co-operate with the government would be subject to government guidance or advice.

5.3 Enforcement Actions

Although the development and use of AI itself was not a target of enforcement, there was a case where the handling of personal data in a service using AI became an issue. In this case, back in 2019, a service provider used AI technology to calculate the expected job offer rejection rate for individuals during job hunting and provided it to client companies without the consent of the subject individuals. The PPC issued a warning and guidance to the service provider, whereas the MHLW issued administrative guidance.

6. Standard-Setting Bodies

6.1 National Standard-Setting Bodies

Government agencies, national research institutions, and industry groups each contribute significantly to developing and establishing AI-related standards and guidelines.

Japanese Industrial Standards

Established by the METI on 21 August 2023, the Japanese Industrial Standards (JIS) introduced JIS X 22989, “*Information technology – Artificial intelligence – Artificial intelligence concepts and terminology*”. This standard, identical to the International Organization for Standardization (ISO)’s ISO/IEC 22989, defines the concepts and terminology related to AI. Additionally, JIS Q 3850 “*Information technology – Governance of IT – Governance implications of the use of artificial intelligence by organisations*” is being developed to align with the ISO/International Electrotechnical Commission (IEC)’s ISO/IEC 38507:2022 and is intended to provide practical governance guidelines for AI use in organisations.

Contributed by: Keiji Tonomura, Yukiko Konno, Minh Thi Cao Koike and Yoshiteru Matsuzaki,
Nagashima Ohno & Tsunematsu

AI Safety Institute

The AI Safety Institute, established on 14 February 2024 by the Cabinet Office and the Information-technology Promotion Agency (IPA), focuses on enhancing AI safety standards domestically and internationally. The AI Safety Institute collaborates with international standardisation bodies such as ISO/IEC SC42 to standardise safety measures and partners with similar organisations in other countries, including the US AI Safety Institute, to develop frameworks for reliable safety evaluation methods and testing procedures for AI systems. The institute has published several key documents, including the *“Guide to Red-Teaming Methodology on AI Safety”* (Version 1.10, updated from September 2024), the *“Guide to Evaluation Perspectives on AI Safety”* (Version 1.10, updated from September 2024), and the *“Data Quality Management Guidebook”* (Version 1.0, March 2025).

The Consortium of Quality Assurance for Artificial-Intelligence-Based Products and Services

The Consortium of Quality Assurance for Artificial-Intelligence-Based Products and Services (the *“QA4AI Consortium”*)- a collaborative effort of leading IT companies, academic institutions, and the National Research and Development Agency – has published the *“Guidelines for Quality Assurance of AI-Based Products and Services”*. These guidelines address key areas such as data integrity, model robustness, system quality, process agility, and customer expectations, providing detailed checklists that aid in developing reliable AI products.

Research and Guidance by AIST

The National Institute of Advanced Industrial Science and Technology (AIST) continues to lead in AI research and standards development. The *“Machine Learning Quality Management Guide-*

line (Revision 3.2.1)” published by AIST classifies the quality of machine learning systems into three categories: quality at the time of use, external quality, and internal quality. It further details methods for applying quality control tailored to these quality categories, which are essential for ensuring the effectiveness and reliability of AI systems in various applications.

6.2 International Standard-Setting Bodies

In Japan, aligning business practices with international AI standards is becoming increasingly important for companies involved in AI development and deployment.

The *“AI Guidelines for Businesses”* emphasises the importance of adhering to international standards that ensure responsible development, deployment and management of AI systems. The guidelines advocate a proactive approach to integrating international standards into Japanese business practices. They include direct references to comprehensive standards such as ISO/IEC 23894:2023, which addresses various environmental considerations for AI systems. Moreover, the guidelines cover standards relevant to various aspects of AI implementation, from information security (ISO/IEC 27001) and data quality (ISO/IEC 25012) to privacy protection (ISO/IEC 27701, ISO/IEC 29100, and ISO/IEC 27018).

Although current Japanese regulations do not mandate compliance with these international standards, the proactive involvement of Japanese experts in their development illustrates Japan’s commitment to aligning domestic practices with global benchmarks. This participation bolsters Japan’s position on the international stage and helps ensure that local practices are

in sync with international standards, reducing potential discrepancies and conflicts.

7. Government Use of AI

7.1 Government Use of AI

Regarding the introduction of AI technology in government, the *“Agreement on the Use of Generative AI such as ChatGPT in Government Operations (Second Edition)”*, adopted by the Japanese government on 15 September 2023, provides that ministries and agencies must not handle sensitive information through so-called *“terms-of-service-based cloud services”* ie, services that become available merely by agreeing to standard terms and conditions – when using generative AI tools in government operations. It also sets forth various operational precautions for the use of generative AI.

Separately, on 6 February 2025, the Japanese government issued its *“Cautionary notice to all ministries and agencies regarding the use of the DeepSeek”*. The notice referred to information previously provided by the PPC to private businesses, indicating that data entered into DeepSeek is stored on servers located in China and is subject to Chinese laws. Ministries and agencies were urged to fully recognise these risks and exercise careful judgment before utilising such services.

On 28 March 2025, the Digital Agency published a draft titled *“Guidelines on the Procurement and Utilisation of Generative AI for the Evolution and Innovation of Government Administration”* and submitted it for public consultation. These guidelines aim to promote the use of generative AI while simultaneously managing associated risks, and set forth the framework for the government’s approach to AI promotion, governance,

procurement and utilisation. The guidelines target systems that incorporate text-generating AI components (excluding systems handling sensitive information such as specially designated secrets and matters related to national security). They also stipulate the establishment of a chief AI officer (CAIO) within each ministry and agency, and require that any occurrence of a risk case be reported to the respective CAIO.

7.2 Judicial Decisions

There are no particular judicial decisions regarding issues related to the use of AI technologies by government agencies in Japan.

7.3 National Security

In the AI Strategy 2022 formulated by the Cabinet Office in April 2022, it is stated that *“[i]n light of the increasing complexity of the international geopolitical situation and changes in the socio-economic structure, various initiatives are being considered for key technologies, including AI from the perspective of economic security, and it is necessary to co-ordinate related measures so that the government as a whole can effectively focus on these issues”*. This was the first time AI-related announcements referred to economic security.

In May 2022, the Economic Security Act was enacted, which also stipulates the provision of information and financial support for the specified critical technologies (including AI-related technologies). In addition, following the enactment of the Economic Security Act, in April 2024, the METI designated the *“Cloud Program”* (including generative AI) as critical material under the Economic Security Act and announced its plan to establish relevant computing resources domestically. This plan aims to make resources for the Cloud Program – with a particular focus on generative AI – accessible to a broad range

Contributed by: Keiji Tonomura, Yukiko Konno, Minh Thi Cao Koike and Yoshiteru Matsuzaki,
Nagashima Ohno & Tsunematsu

of developers, in order to secure a stable supply of such services.

In the “*Interim Report*” published by the AI Strategy Council and the AI Systems Study Group in February 2025, it is stated in the section regarding government utilisation and related matters that – for areas such as medical devices, autonomous vehicles, and foundational services (particularly those involving significant impacts on public life, social activities, and issues related to the safety of life and health or systemic risks) “*it remains appropriate for the competent agencies to continue addressing these areas under existing laws, regulations, and guidelines; however, if new risks emerge in the future that cannot be addressed within the existing frameworks, the government should clarify the interpretation of the relevant frameworks and consider revising existing systems or establishing new systems as necessary.*”

8. Generative AI

8.1 Specific Issues in Generative AI

Discussions around generative AI technologies (such as GPT) and their ethical, legal and social implications in Japan continue to grow more prevalent and increase in intensity. These issues can be categorised into several critical areas, as follows.

IP Violations

Generative AI creates copyright challenges in Japan both at the development phases and the usage phase. While Japan’s Copyright Act permits using copyrighted works for AI training under the “*non-enjoyment purpose*” exception, this does not apply when training specifically targets reproducing creative expressions. Infringement occurs when AI-generated materials show

both similarity and dependency to existing works, with copyright holders able to establish dependency through evidence of access or high similarity. AI users and developers both bear liability risks – ie, users when creating infringing content, and businesses when their systems frequently produce infringing materials without implementing proper safeguards.

Invasion of Publicity Rights

The unauthorised use of celebrity images in AI-generated content raises concerns about publicity rights violations. These concerns include the creation of accurate deepfakes and blending features from multiple celebrities to form new virtual characters for both commercial and non-commercial uses, leading to new legal and ethical challenges. In 2024, there has been a surge in AI-generated investment advertisements impersonating corporate executives, with numerous cases of unauthorised use of real individuals’ likenesses – demonstrating how generative AI amplifies publicity rights violation risks.

Misuse of Personal Data and Invasion of Privacy

The use of personal data by generative AI without prior consent can lead to inappropriate handling or use for unintended purposes. This includes the risk of AI learning from this data and incorporating it into its output, sometimes inaccurately, which can lead to privacy violations. Advanced generative AI models in 2025 have demonstrated concerning abilities to identify specific locations from photographs using only visual cues, creating privacy risks when individuals share images that could inadvertently reveal personal locations.

Leakage of Confidential Information

Generative AI may inadvertently disclose sensitive or proprietary information. If AI systems are

Contributed by: Keiji Tonomura, Yukiko Konno, Minh Thi Cao Koike and Yoshiteru Matsuzaki,
Nagashima Ohno & Tsunematsu

trained on confidential data, there is a risk that this information could be exposed to other users or misused by entities for competitive advantages, breaching confidentiality obligations.

Misinformation

Generative AI can produce inaccurate or entirely fabricated information, spreading misinformation and impacting decision-making processes.

Bias and Discrimination

Improperly designed and monitored AI systems can perpetuate or amplify existing biases, resulting in unfair or discriminatory treatment.

Illegal and Unethical Use

Generative AI has been implicated in various illegal and unethical activities across three main areas: deepfakes and impersonation, obscene or illegal content generation, and cybercrime facilitation. In April 2024, individuals were arrested on suspicion of distributing obscene materials after selling posters featuring AI-generated sexual imagery. In February 2025, three teenagers were arrested for using generative AI to create automated programs that fraudulently contracted more than 1,000 mobile lines through unauthorised access. Additionally, in April 2025, the Tokyo District Court delivered a guilty verdict with a three-year prison sentence (suspended for four years) to a 25-year-old unemployed man who created ransomware using generative AI despite having no specialised IT knowledge. This marked the first conviction in a criminal case involving the misuse of generative AI.

8.2 Data Protection and Generative AI

Under Articles 17 and 18 of the APPI, which advocate for purpose limitation and data minimisation, personal information handling operators – acting as controllers – must ensure that the usage of personal information in generative

AI services aligns with the purposes for which the data was collected. As mentioned in 3.6 **Data, Information or Content Laws**, the advisory issued by the PPC emphasises the critical importance of the appropriate handling of personal data within AI applications. The PPC cautions that using personal data in generative AI without prior consent and for purposes other than those disclosed could violate the APPI. The PPC has highlighted the need for data subjects' explicit consent before using their sensitive personal information in AI models, aligning with the APPI's consent requirements under Article 20.

Additionally, individuals have specific rights under the APPI, such as the right to rectify or delete incorrect personal data under Article 34 and the right to request suspension or deletion of unlawfully processed data under Article 35. However, it is important to note that personal information used in generative AI may not always fall under the definition of “*retained personal data*”, which refers to data systematically organised for retrieval. Consequently, the rights to request disclosure, correction, or cessation of use may not be applicable in all scenarios where AI generates output.

9. Legal Tech

9.1 AI in the Legal Profession and Ethical Considerations

Whether AI chatbot legal advice and AI automated drafting services violate the Attorneys Act that prohibits non-lawyers from providing legal services is a major issue. This was highlighted when the Ministry of Justice responded to enquiries from legal tech service providers about the legality of such services in 2022, suggesting that their contemplated services may constitute the unauthorised practice of law. However,

Contributed by: Keiji Tonomura, Yukiko Konno, Minh Thi Cao Koike and Yoshiteru Matsuzaki,
Nagashima Ohno & Tsunematsu

In August 2023, the Ministry of Justice issued guidelines clarifying that the following types of contract drafting, review and management services do not constitute the unauthorised practice of law:

- services that assist in the drafting of contracts and review of legal issues in the ordinary course of business regarding corporate legal matters that do not involve litigation or disputes;
- services where the language or clauses of the contracts being reviewed are the same as or similar to those pre-registered in the system, such as contract templates or checklists, and are presented without individual modification (as opposed to services that involve the legal analysis of the content of the contract based on specific factual background or instructions regarding the content and the preparation of detailed, case-specific drafting or modification of the contract); and
- services used by lawyers who individually review the AI-generated material and make necessary changes themselves.

The guidelines have made it clear that the scope of legality for AI contract review services is quite broad.

The Japan Federation of Bar Associations (JFBA) has also been active in this space. In June 2023 it established an AI Strategy Working Group that is gathering information and analysing a wide spectrum of issues, including the impact of AI tools on legal practice, their compatibility with the Attorneys Act, potential effects on the judiciary, and possible implications for fundamental human rights and other legal interests. The AI Strategy Working Group is further considering the development of practical guidelines for lawyers on the responsible use of generative AI.

10. Liability for AI

10.1 Theories of Liability

In Japan, AI is not recognised as a legal entity, and there is no specific legislation regarding liability arising from the acts or use of AI. Therefore, general civil and criminal liability will apply to them.

Civil liability is as described in **1.1 General Legal Background** but, in some cases, depending on the relationship between the injured party and the manufacturer, manufacturer's liability may be based on a contract. In addition, regarding automated driving, the “operator” (the owner of the vehicle) may be liable for damages; specifically, the operator is liable unless it can be proven that it was not negligent.

In terms of criminal liability, professional or ordinary negligence resulting in injury or death (Article 211 of the Criminal Code or Article 210 of the Criminal Code) are typically considered to be applicable to the developers and users of AI, but other crimes may also be applicable depending on the circumstances. In addition, in cases where the actions of a third party intervene and the use of AI causes damage to others, the issues of joint tort liability with regard to civil liability and conspiracy with regard to criminal liability may arise.

In relation to the above-mentioned civil liability, if a product has a defect, product liability will be imposed regardless of whether the manufacturer was negligent; this may have a chilling effect on AI developers. In this regard, this risk can be hedged by insurance, which can encourage development.

Regarding the sharing of responsibility in the supply chain, the “*Contract Guidelines on Utili-*

sation of AI and Data Version 1.1” (see 5.1 Regulatory Agencies) note that there are difficulties in determining the attribution of liability (percentage of negligence) based on tortious acts because of the difficulty of verifying causal relationships after an accident and the fact that the results of AI use depend on learning datasets – the content of which is difficult to identify – and the input data at the time of use, which is unspecified. In addition, claims for damages may be made based on contractual liability between the user and the AI developer, and between the AI developer and the data provider for the generation of trained models. It is desirable to clearly specify the division of responsibility in the contract according to the circumstances.

In addition, the model version described in “Contract Guidelines on Utilisation of AI and Data Version 1.1” is a good reference for common industry practice.

10.2 Regulatory

In Japan, there is no cross-sectional legislation or guidelines regarding criminal and civil legal liability with regard to AI.

11. Specific Legal Issues With Predictive and Generative AI

11.1 Algorithmic Bias

Algorithmic bias refers to situations in which a bias occurs in the output of an algorithm, resulting in unfair or discriminatory decisions. In Japan, there has not been a case in which a company has been found legally liable for illegality arising from algorithmic bias. However, if a company were to make a biased decision based on the use of AI, it could be found liable for damages based on tort or other grounds. In addition, companies may face reputational risk if unfair or

discriminatory decisions are made in relation to gender or other matters that significantly affect a person’s life, such as the hiring process.

There are no laws or regulations that directly address algorithmic bias. Companies are expected to take initiatives themselves to prevent the occurrence of algorithmic bias. By way of example, the “AI Guidelines for Businesses” recommend the following: “AI developers must ensure that AI models are trained on representative datasets and are inspected for any unfair biases in the AI system. AI providers are to regularly assess the inputs and outputs of the AI models and their decision-making bases, and monitor for the occurrence of any bias. AI business users must ensure fairness in the data inputs and responsibly make business decisions based on the AI’s outputs, being mindful of any bias included in the prompts.”

Given that all processes involved in data generation and selection, annotation, pre-processing, and model/algorithm generation are subject to potential bias, documentation regarding the specifics of these processes should be obtained and maintained. However, when using complex algorithms such as deep learning, it may not be possible for humans to understand the above-mentioned process – even if collecting the material in relation to such process – in the first place. Therefore, it is advisable to select algorithms that can be used by taking into account aspects of “explainable AI” (“XAI”).

11.2 Facial Recognition and Biometrics Personal Data

Facial or biometric authentication requires the capture of biometric data such as facial images and fingerprint data. Such data is considered personal information under the APPI, but is not regarded as personal information requiring spe-

cial care (Article 2, paragraph 3 of the APPI). Therefore, when acquiring such information, as long as its purpose of use is notified or disclosed, the individual's consent is not required. However, depending on how the data is acquired and used, it may constitute an improper acquisition (Article 20, paragraph 1 of the APPI) or improper use (Article 19 of the APPI). It is therefore advisable to consider this issue carefully.

Privacy and Portrait Rights

In addition, depending on how facial images and biometric information are obtained and used, there may also be infringement of privacy rights and portrait rights (ie, infringement of personality rights). Although the debate over the circumstances in which an infringement of privacy and portrait rights occurs has intensified with a growing number of court precedents, it is difficult to definitively specify what type of acquisition and use would be permissible, as the debate surrounding facial and biometric authentication has not yet crystallised. With regard to the use of video images, in practice, it is advisable to refer to the *"Guidebook for Utilisation of Camera Images Version 3.0"* (March 2022).

11.3 Automated Decision-Making

Profiling will be used as an example of automated decision-making. While some foreign countries have introduced regulations on the use of AI in profiling, such as Article 22 of the EU's General Data Protection Regulation (GDPR), there are no laws or regulations that directly regulate profiling in Japan. Notwithstanding this, however, the provisions of the APPI must be complied with. By way of example, when personal data is acquired for profiling purposes to analyse behaviour, interests and other information from data obtained from individuals, the purpose of the use of such data must be explicitly notified or disclosed to the public in accordance with

the APPI. However, it should be noted that individuals' consent is not required under the APPI, unless acquiring personal information requiring special care. In addition, precautions should be taken to avoid inappropriate use (Article 19 of the APPI).

Further, if automated decision-making leads to unfair or discriminatory decisions, liability for damages and reputational risk could be an issue, similar to those issues discussed in **11.1 Algorithmic Bias**.

11.4 Transparency

In Japan, there are no laws or regulations that provide specific rules for AI transparency and accountability. However, in the Version 1.0 of the *"AI Guidelines for Businesses"* published by the METI and the MIC on 19 April 2024, transparency and accountability are established as common principles for businesses involved in the AI field. This means that, when utilising AI, it is necessary to ensure that AI systems and services can be verified and are within technically feasible limits – with appropriate information on the AI systems being provided to stakeholders. This includes information about the use of AI, its application scope, methods of data collection, the capabilities and limitations of the system, and the methods of the AI system's use.

However, there is no clear guidance on when and what information should be disclosed when AI such as chatbots replaces services typically provided by people. The foregoing can also be problematic from the standpoint of the APPI. By way of example, if AI is actually being used but the company does not disclose this – leading the user to mistakenly believe that a human is making decisions and providing personal data – there may be a breach of the duty to properly

acquire the data or the duty to notify the purpose of its utilisation.

12. AI Procurement

12.1 Procurement of AI Technology

Procurement of AI technology involves unique risks and contractual considerations that differ from traditional software procurement. According to the *“Checklist for AI Use and Development Contracts”* (the *“AI Contract Checklist”*) published by the METI in February 2025, AI service procurement typically falls into three categories: *“General-Purpose AI Service Utilisation”*, *“Customised AI”*, and *“New Development”*. The AI Contract Checklist primarily addresses the following key areas:

- Input data processing – when input data is used for general AI learning purposes, organisations face potential risks including violations of data protection laws, confidential information leakage, breaches of confidentiality agreements with third parties, and IP rights infringement. Contracts should clearly specify data identification and definition, conditions for providing data to vendors, clarification of usage purposes and conditions, management and security protocols, retention periods, deletion requirements, and rights ownership.
- Output handling – for AI-generated outputs, contracts should clearly define the output specifications, vendor delivery obligations and conditions, warranty and information disclosure requirements, usage terms and conditions, third-party distribution permissions, and IP rights ownership.
- Data security – contracts should address AI system security standards, audit and information disclosure frameworks, and log retention protocols. Organisations are advised to

verify that AI services meet required security standards by reviewing architecture design documentation, Software Bills of Materials (SBOM), and vulnerability information.

- Personal information protection – when user inputs to AI services contain personal data, organisations must determine whether the APPI regulations on third-party transfers (Article 27) and cross-border transfers (Article 28) apply. Additionally, organisations must assess whether the data handling qualifies as *“outsourced processing”* (Article 27, paragraph 5, item 1), as this classification significantly affects compliance requirements. When applicable, organisations must obtain appropriate consent and implement required security measures.

Beyond the AI Contract Checklist, procurement contracts should address explainability and ethical governance based on risk levels and intended use.

13. AI in Employment

13.1 Hiring and Termination Practices

Advantages for employers using AI in hiring and termination include the fact that, unlike the subjective evaluations conducted by recruiters in the past, AI-based evaluations can be conducted fairly and objectively by setting certain standards, and the fact that the use of AI can make the recruitment process more efficient. On the other hand, the following points are relevant with regard to information that may be obtained through the hiring process and with regard to the exercise of the right to termination.

Hiring

In Japan, there are no laws that specifically restrict the use of AI in hiring or recruitment

activities. Additionally, even if an AI analysis is incorrect and the employer does not fully verify this analysis, this would not necessarily constitute a violation of applicable laws—given that companies have the freedom to hire under Japanese law and judicial precedent. However, it can be said that AI-based recruitment limits a company's freedom to hire to a certain extent.

Specifically, even in cases where AI is utilised in recruitment activities and information on jobseekers is automatically obtained, the information must be collected in a lawful and fair manner – for example, directly from the jobseeker, or from a person other than the jobseeker with the consent of the jobseeker – in accordance with Article 5-4 of the Employment Security Act and Article 4-1 (2) of the Employment Security Act Guidelines.

In addition, when using AI to obtain information on jobseekers, companies must be careful not to obtain certain prohibited information. Specifically, under Article 20 of the APPI, the company is typically prohibited from obtaining information requiring special care (eg, race, creed, social status, medical history, criminal record, and any facts related to the jobseeker being a victim of a crime) without the consent of the jobseeker. Also, under Article 5-4 of the Employment Security Act and Article 5-1 (2) of the Employment Security Act Guidelines, the company may not obtain certain information (eg, membership in labour union, or place of birth) even with the consent of the jobseeker.

In addition, there is a risk that – as a result of an erroneously high AI evaluation of a jobseeker – an offer may be made to a jobseeker or the jobseeker may be hired even though the jobseeker would not have been given an offer or hired if the company's original criteria were followed.

In such case, under Japanese law, the legality and validity of a decision to reject or dismiss the jobseeker will be determined based on how the recruitment process was conducted.

Termination

Situations in which the selection of the persons to be terminated may be problematic include termination as part of employment redundancy or voluntary resignations.

Under Japanese law, unilateral termination of employees by employers is restricted, and termination that constitutes an abuse of the right to terminate is considered invalid. Notably, in the case of termination as part of employment redundancy, the validity of termination is examined from the viewpoints of:

- the necessity of reducing the workforce;
- the necessity of terminating employees through employment redundancy;
- the validity of the selection of employees to be terminated; and
- the validity of the procedures for termination.

AI's use is mainly anticipated in the selection of employees to be terminated. It should be noted that these four perspectives are considered as factors rather than requirements and, even if AI is utilised to select an employee for termination in a reasonable and fair manner that eliminates subjectivity in the selection of the employee to be terminated, this does not necessarily mean that the termination is valid. Naturally, if the data on which the AI bases its judgement is erroneous or if the AI is unreasonably biased, there is a high possibility that the selection of the terminated employee will not be recognised as valid.

On the other hand, there is no law that specifically regulates voluntary resignations, given that the

Contributed by: Keiji Tonomura, Yukiko Konno, Minh Thi Cao Koike and Yoshiteru Matsuzaki,
Nagashima Ohno & Tsunematsu

resignation is made voluntarily by the employee. However, it is necessary for the voluntary resignations to take place in a manner that respects the voluntary decision of the employee; there are court cases that have held that a voluntary resignation resulting from an unreasonable act or conduct that may have impeded the employee's voluntary decision to resign constitutes a tort under Article 709 of the Civil Code. Therefore, even if the selection of employees subject to voluntary resignation is based on an objective and impartial evaluation by AI, the company should not approach the voluntary resignation with the attitude that the decision is based on the AI's judgment and that there is no room for negotiation. Instead, the company should provide a thorough explanation to the employee so that the employee understands the pros and cons of resigning and is able to make a voluntary decision. This recommendation to companies precedes the introduction of AI in the termination process.

13.2 Employee Evaluation and Monitoring

Personnel Evaluation

Generally, the items and standards of assessment in Japanese personnel evaluations are abstract, and supervisors have broad discretion in the assessments. AI-based personnel evaluations are expected to reduce the unfairness and uncertainty stemming from the discretion given to supervisors.

Legally, the following provisions regulate personnel evaluations:

- equal treatment (Article 3 of the Labour Standards Act);
- equal pay for men and women (Article 4 of the Labour Standards Act);

- equal treatment of men and women in promotions, etc (Article 6, paragraph 1 of the Equal Employment Opportunity Act); and
- unfair labour practices (Article 7 of the Labour Union Act).

In the case of a company that has the authority to evaluate an employee, courts have held that a tort is not established unless the employer violated the above-mentioned provisions or abused its discretionary power in violation of the purpose of the personnel evaluation system. Cases that would fall under abuse of discretion include factual errors, misapplication of evaluation criteria, arbitrary evaluation and discriminatory evaluation.

Therefore, even in the case of personnel evaluation using AI, if there is an error in the data on which the AI bases its judgement or if there is an error in the algorithm or learning method by which the AI evaluates such data, personnel evaluation based on such AI's judgement may constitute a tort.

Monitoring

One possible method of monitoring workers using AI would be for AI to check emails and automatically notify managers if there are suspicious emails. The question is whether this would infringe on the privacy rights of the workers with regard to being monitored – although monitoring is considered permissible as long as the company's authority to monitor is clearly defined in the internal rules. Courts have also held that, even if the authority is not clearly stated, monitoring is permissible as long as there is a reasonable business management need (such as when it is necessary to investigate whether or not there has been a violation of corporate order) and the means and methods used are reasonable.

Therefore, when conducting monitoring using AI, it would be advisable to:

- specify in the internal rules that managers ultimately have the authority to check the contents of employees' email exchanges; and
- communicate such rules to the employees.

14. AI in Industry Sectors

14.1 Digital Platform Companies

Ridesharing services were partially liberalised in Japan in 2024, but strict legal regulations still apply and ridesharing services such as Uber are not yet widespread in Japan. However, food delivery platforms – for example, Uber Eats, which uses an algorithm to guide delivery staff to deliver orders quickly and efficiently – are widely used. Many food delivery platforms do not have an employment relationship with the delivery staff, who work on a freelance basis. For the protection of freelancers, the Freelance Transaction Fairness Act entered into force on 1 November 2024. The Freelance Transaction Fairness Act obliges ordering businesses to clearly state contract terms, observe payment deadlines, refrain from abusing a superior bargaining position, and implement anti-harassment measures, thereby promoting fair transactions between companies and freelancers.

14.2 Financial Services

In the financial sector, AI is used by banks and lenders for credit decisions and by investment firms for investment decisions. In addition, the amended Instalment Sales Act (which came into effect in April 2021) enables credit card companies to determine credit limits through credit screening using AI and big data analysis.

The FSA's supervisory guidelines require banks, etc, when concluding a loan contract, to be prepared to explain the objective rationale for concluding a loan contract based on the customer's financial situation in relation to the provisions of the loan contract. This is true even if AI is used for credit operations. Therefore, it is necessary to be able to explain the rationale of credit decisions made by AI.

In addition, when credit scoring is used by AI to determine the loan amount available for personal loans, care should be taken to avoid discriminatory judgements (eg, different judgements of loan amounts available based on gender or other factors). *"Social Principles of Human-Centric AI"* (2019) also states: *"Under the AI design philosophy, all people must be treated fairly, without undue discrimination on the basis of their race, gender, nationality, age, political beliefs, religion, or other factors related to diversity of backgrounds."*

Financial instrument firms must not fail to protect investors by conducting inappropriate solicitation in light of the knowledge, experience and financial situation of the customer as well as the purpose of concluding the contract (the compliance principle). In addition, these firms are obligated to explain to customers the outline of the contract and the risks of investment in accordance with the compliance principle. Therefore, if the criteria for investment decisions by AI cannot be reasonably explained, problems may arise in relation to the compliance principle and the duty to explain.

14.3 Healthcare

If AI-based programs (such as diagnostic imaging software or health management wearable terminals) or devices equipped with such programs fall under the category of *"medical device"*

Contributed by: Keiji Tonomura, Yukiko Konno, Minh Thi Cao Koike and Yoshiteru Matsuzaki,
Nagashima Ohno & Tsunematsu

es” under the PMDA, approval is required for their manufacture and sale, and approval or certification is also required for individual medical device products. Whether AI-based diagnostic support software and other medical programs constitute “*medical devices*” must be determined on a case-by-case basis, but the MHLW has provided a basic framework for making such determinations.

According to this framework, the following two points should be considered.

- How much does the programmed medical device contribute to the treatment, diagnosis, etc., of diseases in view of the importance of the results obtained from the programmed medical device?
- What is the overall risk, including the risk of affecting human life and health in the event of impairment, etc., of the functions of the programmed medical device?

In addition, when a change procedure is required to change a part of the approved or certified content of a medical device, the product design for an AI-based medical device may be based on the assumption that its performance will constantly change as new data is obtained after the product is marketed. Given the characteristics of AI-based programs, which are subject to constant changes in performance and other aspects after their initial approval, the amended PMDA (which came into effect in September 2020) introduces a medical device approval review system that allows for continuous improvement.

Given that medical services such as diagnosis and treatment may only be performed by physicians, programs that provide AI-based diagnostic and treatment support may only serve as a tool to assist physicians in diagnosis and treat-

ment. Physicians will be responsible for making the final decision.

Medical history, physical and mental ailments, and the results of medical examinations conducted by physicians are considered “*personal information requiring special care*” under the APPI and, in principle, the consent of the patient must be obtained when obtaining such information. In many cases, medical institutions are required to provide personal data to medical device manufacturers for the development and verification of AI medical devices. In principle, the provision of personal information to a third party requires the consent of the individual, but it may be difficult to obtain prior consent from the patient. An opt-out system is also in place. However, it cannot be used for personal information requiring special care.

Anonymised information, which is irreversibly processed so that a specific individual cannot be identified from the personal information, can be freely provided to a third party. However, it has been noted that it is practically difficult for medical institutions to create anonymised information. In addition, the Next-Generation Medical Infrastructure Act allows authorised business operators to receive medical information from medical information handlers (hospitals, etc) and anonymise it through an opt-out method. However, it is not widely used.

Effective 1 April 2024, the revised Next-Generation Medical Infrastructure Act introduced the new category of pseudonymised medical information. Unlike fully anonymised data, these datasets retain all clinical detail while removing only direct identifiers such as names and chart numbers; they are created under strict safeguards by government-certified data-creation entities and may be accessed solely by certified

data-use entities within a pre-publicised framework of joint use. Patients need only be informed and given the opportunity to opt out, allowing large-scale, real-world data to accelerate medical research and development.

14.4 Autonomous Vehicles

Regarding traffic rules, amendments to the Road Traffic Act have already been enacted to permit Level 3 (conditional automated driving) and Level 4 (unmanned automated driving). In 2024, pilot projects and commercial services featuring Level 4 fully driverless mobility solutions gathered pace in regional public-transport settings, and the government announced that it would streamline regulatory procedures and widen the geographic scope in which such services may operate.

Regarding liability in the event of an accident, there are no specific regulations that determine liability when an autonomous vehicle causes an accident; currently, the existing legal framework applies. Under the current law, the entities liable in the event of an accident involving an autonomous vehicle include the driver, the operator (a concept that includes the owner of the vehicle and the transport business operator, in addition to the driver) and the manufacturer of the vehicle.

As for the driver's liability, under the amended Road Traffic Act, at Level 3, the driver is not required to be vigilant if not requested to override and take over the autonomous driving system; thus, liability for accidents occurring without an override request is limited to exceptional circumstances. At Level 4, given that intervention by a person riding in the car is not requested at all, the person in the car will not bear any responsibility if an accident occurs.

Regarding the manufacturer's liability, under the Product Liability Act, there is currently an active discussion on how to define the autonomous vehicle's "defect" that must be proven by the victim. But, generally, it is considered very challenging to hold manufacturers liable under the Product Liability Act when an autonomous vehicle causes an accident.

In light of this, the government has a policy to ensure the protection of a traffic accident victim by clarifying that the operator's liability applies to autonomous driving for the time being. In Japan, when a personal injury accident occurs, the operator is subject to almost strict liability. When the operator is held liable, victims are compensated through the compulsory automobile liability insurance that comes with the vehicle.

14.5 Manufacturing

There are currently no specific regulations or government guidelines for the use of AI in manufacturing. Nevertheless, the "AI Guidelines for Businesses" are broadly applicable to the use of AI in the manufacturing sector. Interestingly, a document released in June 2020 by the Regulatory Reform Promotion Council – an advisory body to the Cabinet Office – suggests that existing regulations regarding the inspection of products at manufacturing facilities could be relaxed if AI is used to assist in the inspection. It states: *"If precise risk management is carried out using digital technologies during the manufacturing process, inspections themselves should be considered unnecessary"*.

14.6 Professional Services

In addition to legal services (see 9. Legal Tech), when AI assists with professional services such as tax and accounting work, individual professional regulations must be observed. By way of example, as stated in Article 72 of the Attorneys

Act, non-lawyers or entities other than law firms are not permitted to engage in the practice of law as a business. Nevertheless, a violation will not occur if the relevant AI services are intended to assist lawyers and are designed so that the output of AI services must be reviewed by lawyers and then provided to clients as the lawyers' own work product. However, if the output of the AI services is provided directly to clients, there may be a problem under the Attorney Act. As there are many such restrictions under current laws applicable to professional services, it is necessary to ensure that AI performing certain professional tasks does not violate these professional regulations.

15. Intellectual Property

15.1 IP and Generative AI IP Protection of the AI Process

Generative AI processes involve:

- training the AI model using a training dataset; and
- generating outputs by providing prompts to the trained model.

These processes may yield valuable assets such as the AI model, training datasets, input prompts, and output. These assets may be protected under IP law, as follows.

AI model

Mathematical or theoretical AI models are generally not eligible for patent protection, as they are often viewed as discoveries of natural laws. However, if the learning methods of an AI model provide innovative solutions to existing problems, they can be patented. If not patented, these innovations can be treated as trade secrets, provided they meet the requirements for

trade secrets. It is unclear whether AI models can be recognised as “*database works*” or “*program works*” under copyright law.

Training dataset

Training datasets typically do not qualify for patent protection; however, the methods used to generate them, unique selections, and combinations of data items and pre-processing techniques that effectively train specific AI models can be subjects of patent protection. If the components of the datasets (eg, images, videos and music) qualify as works of authorship, they are individually protected by copyright. Additionally, if these datasets meet the criteria for trade secrets or are offered on a limited basis, they can be protected under the Unfair Competition Prevention Act.

Input (prompts)

Innovations in prompt-generation methods can be patented if they enhance AI system inputs or are designed to elicit specific responses. Additionally, prompts that include copyrighted elements such as images, videos and music are protected under copyright law.

Output

The “*Interim Report of the Study Group on Intellectual Property Rights in the AI Era*” (JPO, May 2024) indicates that, for inventions using AI, natural persons who are creatively involved in the invention's distinctive elements should be recognised as inventors. This suggests that outputs from AI processes can be protected by patents if they meet the requirements for patentability and if there was creative contribution from natural persons in the invention's distinctive elements.

From a copyright perspective, the “*General Understanding on AI and Copyright in Japan*” (Agency for Cultural Affairs, May 2024) states

Contributed by: Keiji Tonomura, Yukiko Konno, Minh Thi Cao Koike and Yoshiteru Matsuzaki,
Nagashima Ohno & Tsunematsu

that materials autonomously generated by AI are not considered “works” under copyright law, as they do not constitute “creatively produced expressions of thoughts or sentiments”. However, if AI is used as a tool with sufficient “creative contributions” from the user, such material may be considered “work”, with the user as the “author”.

AI Terms for Input and Output Rights

Generative AI providers typically offer users the option to opt out of using their input data for model training. Users usually retain ownership of outputs generated by these AI tools, per the terms of service. However, these terms do not guarantee the legal protectability of these outputs, as protectability depends on factors outlined in the “General Understanding on AI and Copyright in Japan”.

15.2 Applicability of Patent and Copyright Law

Discussions regarding whether AI technology can be recognised as an inventor or co-inventor for patent purposes, as an author or co-author for copyright purposes, or as a moral right-holder are also taking place in Japan. Under current Japanese law, AI is not considered a natural person and therefore cannot be recognised as the inventor for patent purposes, as the author for copyright purposes, or as the holder of moral rights.

In this regard, on 16 May 2024, the Tokyo District Court ruled that an “inventor” as defined in the Patent Act is limited to natural persons and does not include AI, in a case where the JPO in its decision dismissed the patent application related to an AI-generated invention because only “DABAS (an AI that invented the invention autonomously)” was listed as the inventor’s name in the national phase documents of the

Patent Co-operation Treaty application and the plaintiff filed a lawsuit to seek the revocation of the JPO decision. On 30 January 2025, the IP High Court (court of appeal) reached the same conclusion that AI cannot be listed as an inventor under current Japanese patent law; however, the reasoning differed from that of the Tokyo District Court, which initially focused on the interpretation of the concept of “inventor” under the Patent Act. The IP High Court held that the current Patent Act only provides a framework for granting patents for inventions made by natural persons, both in terms of rights and procedures.

However, if a person who used AI to create a work had the intention to create a work and made a creative contribution, then the resulting work may be recognised as having been created by the person who used the AI as a tool, rather than by the AI itself. In such a case, the natural person who had the creative intention and made the creative contribution is considered to be the author. While it is controversial whether AI should be given judicial personality, such a legal system is not being considered at this point.

15.3 Applicability of Trade Secrecy and Similar Protection

AI technology and (big) data utilised in the development and use of AI are protected as trade secrets just like other informational assets (Article 2 (6) of the Unfair Competition Prevention Act (the UCPA)) as long as they are:

- kept confidential;
- not publicly known; and
- are useful for business activities.

In relation to the requirement, the latest version of the “Trade Secret Management Guideline” (METI, March 2025) – which is not legally binding but is intended to indicate the minimum level

Contributed by: Keiji Tonomura, Yukiko Konno, Minh Thi Cao Koike and Yoshiteru Matsuzaki,
Nagashima Ohno & Tsunematsu

of measures required to protect trade secrets – states that, even if the information managed as confidential by Management Unit A is input for generative AI at Management Unit A, the mere fact that such information is subsequently generated and output by generative AI at Management Unit B does not negate that such information is kept confidential by Management Unit A.

The trade secret holder can seek an injunction against unauthorised use by a third party and can also claim damages for unauthorised use. In addition, criminal penalties may also apply for acts of unfair competition, etc, for the purpose of wrongful gain or causing damage (Article 21 of the UCPA).

Moreover, even if the data does not qualify as a trade secret because it is not kept secret as it is intended to be provided to a third party in the course of the development or use of AI, if the data constitutes technical or business information that is accumulated to a significant extent and is managed by electromagnetic means as information to be provided to a specific party on a regular basis, it is protected as “*shared data with limited access*” (Article 2 (7) of the UCPA). The holder of the rights to shared data with limited access can seek an injunction against unauthorised use by a third party and can also claim damages for unauthorised use. However, unlike trade secrets, there are currently no criminal penalties with regard to shared data with limited access.

Protection Based on Judicial Precedents

Even if not protected by the UCPA, unauthorised use of data may constitute a tort under Article 709 of the Civil Code if there are special circumstances, such as infringing on legally protected interests (Supreme Court judgment, 8 December 2011, Minshu 65 (9)3275 (2012)). Legally pro-

tected interests include business interests in business activities (a case in which incorporating another company’s database into one’s own database for sale was considered to constitute a tort (Tokyo District Court judgment, 25 May 2001, Hanta 1081, 267 (2002))).

Protection Through Contracts

Even if not protected by the UCPA, it is possible to set rights and obligations related to data between parties in data transaction contracts and protect valuable data. However, in current Japanese law, data – which is an intangible asset – is not recognised as an object of ownership and remains a subject of the right to use under the contract. Especially for programs or models and their source code, it is reasonable to expect that they should be treated separately, so it is desirable to explicitly agree on the handling of the source code in cases where the transfer of the source code is an issue.

15.4 AI-Generated Works of Art and Works of Authorship

Copyright Law

Works created autonomously by AI are not protected by copyright, given that AI lacks ideas or emotions. However, if the user of AI (a human being) has creative intent in the process of generating the work and contributes creatively to obtaining the AI-generated work through instructions or other means, the user can be considered to have creatively expressed their thoughts or sentiments using AI as a tool and the work can be protected as a copyrighted work.

Using third-party copyrighted works for the purpose of “*AI learning*” before generating AI-created work does not constitute copyright infringement. This is because, in certain cases where the use is not intended for enjoying the expression of thoughts or sentiments in the copyrighted

Contributed by: Keiji Tonomura, Yukiko Konno, Minh Thi Cao Koike and Yoshiteru Matsuzaki,
Nagashima Ohno & Tsunematsu

work (Article 30-4 (ii) of the Copyright Act), copyright protection does not apply and such use is not considered copyright infringement. However, if one tries to use the copyrighted works as they are for a database rather than as data for AI-learning purposes, such use may constitute copyright infringement, even under the above-mentioned conditions.

Copyright infringement is established when someone relies on and uses another's copyrighted work (in other words, someone's work is derived from the copyrighted work). However, it is controversial whether the reliance requirement is satisfied in the case where AI that is developed using another's copyrighted work as AI-learning data produces its own work that resembles another's copyrighted work that was used as AI-learning data; there is no established view on this matter.

Patent Law

AI-related technologies, including inventions of methods for AI to produce works and works produced by AI, are eligible to receive patents as long as they meet the general patent requirements. Under Japanese law, data and pre-trained models are not considered excluded from eligibility for patent protection, as long as they are considered programs or program equivalents (ie, data with structure and data structure). On the other hand, data or datasets that are merely presented as information are not eligible for patent protection.

15.5 OpenAI

As mentioned in **15.3 Applicability of Trade Secrecy and Similar Protection**, if the user of AI has creative intent in the process of generating the work and contributes creatively to obtaining the AI-generated work through instructions or other means, the user can be considered to

have creatively expressed their ideas or emotions using AI as a tool. In such cases, the AI-generated work is protected as a copyrighted work. This also applies to creating works and products using OpenAI and there is no difference in protection whether the product is an image or text.

However, the extent to which creative contribution must be made in order to qualify for copyright protection is determined on a case-by-case basis and is still controversial. Under the Copyright Act, it is likely that the prompts used to generate high-quality output can be protected as copyrighted works unless they are mere ideas since the copyright protects expressions not ideas. On the other hand, even if the prompt can be protected by the copyright, it is likely that the work generated by/with OpenAI is not a derivative work of the prompts if creativity in the prompts is difficult to find in the generated work.

16. Antitrust

16.1 Emerging Antitrust Issues in AI

Key emerging antitrust issues in AI are being addressed by the JFTC, in a similar way as by competition authorities worldwide. The JFTC published *"Report on Algorithms/AI and Competition Policy"* in March 2021 (the *"JFTC's 2021 Report"*) and a discussion paper on *"Competition in Generative AI"* in October 2024 (the *"JFTC's 2024 Paper"*). These documents identify several critical concerns associated with the use of AI.

Acqui-hires (Partnerships for Specialised Talent Acquisition)

The JFTC's 2024 Paper addresses how companies use partnerships to acquire specialised talent. The document points out that when companies recruit executives or employees from

Contributed by: Keiji Tonomura, Yukiko Konno, Minh Thi Cao Koike and Yoshiteru Matsuzaki,
Nagashima Ohno & Tsunematsu

competitors or promising start-ups as teams or departments, such acts can have effects similar to business transfers and potentially impact competition. This is particularly significant in the generative AI market, where specialised talent drives innovation and creates value in AI products, making talent acquisition a key competitive factor in the development of AI models and products.

Price Fixing and Algorithmic Collusion

The JFTC's 2021 Report categorises algorithmic collusion into four types: monitoring algorithms, parallel use of algorithms, signalling algorithms, and self-learning algorithms. It identifies specific scenarios where algorithmic co-ordination may constitute illegal co-ordination – for example, when multiple competitors use pricing algorithms from the same vendor while aware that prices will be synchronised, or when platform providers set identical discount rate limits for all users who knowingly use these systems. The 2024 Paper indicates that, when multiple developers use the same generative AI model or when businesses adopt identical AI-powered applications, situations may arise where pricing strategies and production targets become identical or similar due to matching underlying data and algorithms, potentially affecting competition.

Abuse of Data-Driven Market Power

Both JFTC documents highlight concerns about market power abuse through:

- data access restrictions that prevent new market entry;
- self-preferencing by platforms operating in dual roles;
- the manipulation of ranking algorithms to favour affiliated services; and

- tying practices, such as cloud service providers requiring customers to use their AI models.

A notable Japanese case involved a restaurant claiming a rating platform unfairly lowered its ranking through algorithm changes. Although a Tokyo District Court initially awarded damages in 2022, the High Court overturned this decision in 2024, with an appeal now pending before the Supreme Court.

While the JFTC's 2021 Report states that algorithmic co-ordination can be addressed under existing antitrust law in many cases, the JFTC has recognised that the rapidly evolving nature of generative AI markets necessitates continued vigilance. In its 2024 Paper, recognising the rapidly evolving nature of generative AI markets, the JFTC is actively collecting information and conducting market surveys through hearings with relevant stakeholders. The commission plans to proceed with investigations in an agile manner, given the fluid state of AI markets – organising facts in a timely way and, when necessary, providing perspectives on the application of anti-monopoly law and competition policy to these emerging issues.

17. Cybersecurity

17.1 Applicability of Cybersecurity Legislation to AI

Emerging Risk of AI-Enabled Cyber-Attacks

The annual report of Japan's National Police Agency (published in March 2025) points out that malicious programs and phishing emails generated using AI have been observed. It also notes that the risk of cyber-attacks exploiting AI is increasing.

Contributed by: Keiji Tonomura, Yukiko Konno, Minh Thi Cao Koike and Yoshiteru Matsuzaki,
Nagashima Ohno & Tsunematsu

Legal Framework for Cybersecurity

Japan does not have a comprehensive legal framework dedicated to cybersecurity at the moment. Instead, cybersecurity-related requirements are established through various individual laws. By way of example, the APPI imposes an obligation on business operators handling personal information to implement security measures to address risks such as data breaches.

Future Policy Direction for AI-Driven Cyberdefence

In the supplementary resolution attached to the “*Bill on the Prevention of Damage Caused by Unauthorised Activities Against Critical Computers*” (the “*Active Cyberdefence Bill*”) currently being discussed in the National Diet, it was stated that “[t]aking into account the initiatives and needs of the private sector and others, necessary measures should be studied and promoted through public-private collaboration to improve the efficiency of cyberdefence operations by utilising new technologies such as AI”. Accordingly, it is expected that measures to counter cyberattacks leveraging AI will be developed going forward.

18. ESG

18.1 ESG Dimensions of AI

The Ordinance on Disclosure of Corporate Information, etc. has been revised and, as of the fiscal year ending March 2023, companies are required to disclose their approach to and initiatives regarding sustainability in their securities reports and other documents. Additionally, on 5 March 2025, the Sustainability Standards Board of Japan (SSBJ) published sustainability disclosure standards, including the universal standard “*Application of Sustainability Disclosure Standards*”, the first thematic standard “*General Dis-*

closure Standards,” and the second thematic standard “*Climate-Related Disclosure Standards*”. The use of AI to streamline the collection and analysis of data related to these reports is not prohibited by law.

The proliferation of AI and data centres is generating significant electricity demand, reigniting discussions about the necessity of nuclear power plants.

19. AI Governance and Compliance

19.1 AI Governance and Best Practice Compliance Strategies

Given that there is no comprehensive AI regulation in Japan, best practice includes:

- compliance with existing laws in specific areas;
- building a robust AI governance framework;
- contractual measures; and
- technical measures.

The following discussion focuses on the first three points.

Legal Compliance

When developing, providing or using AI, it is necessary to comply with existing laws, especially both the Copyright Act and the APPI. These issues are discussed in more detail in other sections of this chapter.

Risk Management and Governance Framework (Building an AI Governance System)

Given that there is no comprehensive AI regulation in Japan, there is a need to address risks not necessarily covered by law, such as bias and

Contributed by: Keiji Tonomura, Yukiko Konno, Minh Thi Cao Koike and Yoshiteru Matsuzaki,
Nagashima Ohno & Tsunematsu

fairness issues. In this regard, mere compliance with existing regulations is not sufficient. Therefore, companies developing high-risk AI systems in particular are increasingly considering establishing a comprehensive AI governance framework across their organisations. Such AI governance frameworks mainly consist of an internal process to identify and address AI risks, as well as the organisations and personnel that develop and operate these processes.

Guidance that can be useful in this context includes the “*AI Guidelines for Businesses*”. Although these guidelines are not legally binding and non-compliance does not incur penalties, Japanese case law suggests that widely adopted guidelines could be considered when determining important issues such as breaches of duty of directors. Consequently, industry participants are advised to review these guidelines to ensure that their systems are not significantly below industry standards.

Contractual Measures

Given that multiple parties are involved in the process of developing, providing or using AI, it is worth considering contractually allocating appropriate risk distribution and responsibility sharing. In this context, the AI Contract Checklist published by the METI in February 2025 (see **12.1 Procurement of AI Technology**), and the “*Contract Guidelines on the Utilisation of AI and Data*” published by the METI in June 2018 can serve as a useful reference. However, it is important to be cautious of regulations found in other applicable laws, such as the Subcontract Act, the Consumer Contract Act, and the standard terms of contract provisions under the Civil Code, which invalidate certain contract clauses that unilaterally impose a disadvantage on a counterparty.

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