EU-Japan Centre
for Industrial Cooperation
一般財団法人
日欧産業協力センター

Japanese policy and regulatory developments

December 2025

Prepared by
Nishimura & Asahi Europe Rechtsanwaltsgesellschaft mbH

NISHIMURA
& ASAHI

Noriya Ishikawa
Yumiko Kato
Kei Hattori
Renato Yamazaki

For further inquiries: https://www.eu-japan.eu/be-informed

Table of Contents

Digital-Related Matters

The Second Study Group on the Civil Liability Framework for the Utilization of AI[1]

(Ministry of Economy, Trade and Industry, October 1)

- On October 1, 2025, the Ministry of Economy, Trade and Industry (METI) held the Second Study Group on the Civil Liability Framework for the Utilization of AI. This meeting followed the first session, which was held on August 19 of the same year and reported in the October issue of this monthly report.[2]
- At this session, in addition to the two types of use cases examined at the first meeting, Use Cases 3 and 4 were discussed.
- Use Case 3: Company B, which provides outsourced inspection services for manufactured products, offered an inspection service to Company C using Company A's image-recognition AI. The service had been operated without issue for several years, but in the fourth year, the AI failed to detect a cutter blade mixed into the products, resulting in consumer injury. The contract only required that inspections be conducted "with commercially reasonable care and skill," with no specific agreement on the accuracy level of the service.
  - Key issues discussed:
    (1) Whether Company B, which provided a service using high-precision AI, could be found negligent.
    (2) If negligence can be established, in what types of AI utilization scenarios such a finding would be justified.
    (3) In cases such as this, where AI judgments are directly used as operational judgment within a certain scope, whether AI developers may owe a higher duty of care than in cases in which AI is used merely as a support tool.
- Use Case 4: Company D, an AI developer, provided an image-generation AI trained on publicly available datasets. Company E, an apparel company, used one of the generated images in an advertisement. The image closely resembled a nationally known celebrity, V, who then claimed infringement of her right of publicity. However, Company E did not intentionally generate the image, and Company D had implemented measures to prevent the direct reflection of source datasets. Moreover, there had been no prior reports of similar images resembling V being generated.
  - Key issues discussed:
    (1) How to assess the liability of Company E, the AI user, for using an image resembling celebrity V in advertising.
    (2) How to assess the liability of Company D, the AI developer and provider.

---

[1] https://www.meti.go.jp/shingikai/mono_info_service/ai_utilization_civil/002.html (in Japanese)

[2] https://www.eu-japan.eu/publications/monthly-japanese-policy-and-regulatory-developments-news-october-2025

(3) Considering that AI involves specialized technical domains and that evidence necessary for verification is often held only by developers, whether factual presumptions of negligence may apply based on certain established facts or empirical rules.
(4) Given that documents held by AI developers or providers may be subject to court orders for document production, for what types of evidence disclosure issues should be raised in relation to the developer's potential liability.

Takeaway: At the first study group, discussions focused on cases in which AI should be used as an auxiliary tool for business decision-making. In contrast, the second study group reviewed cases in which highly accurate AI systems are actually used in business operations, and considered key issues regarding negligence liability and the burden of proof in situations where negligence is less likely to be recognized. The perspectives developed in these discussions are expected to be highly useful in future dispute and litigation involving the use of AI in business processes. It is notable that in relation to highly accurate AI systems, the view that the focus of negligence assessment is shifting from checking individual test results to system design and operation that ensure the desirable AI functions was widely supported.

Ministry of Economy, Trade and Industry Publishes Outline of the Direction for the AI Robotics Strategy[3]

(Ministry of Economy, Trade and Industry, October 14)

- In Japan, the implementation of AI in society has become increasingly urgent in order to address the structural labor shortage caused by population decline. In addition, to ensure economic security, it is essential to establish an autonomous technological foundation and resilient supply system for AI robotics.
- On October 14, 2025, the Ministry of Economy, Trade and Industry ("METI") published the "Outline of the Direction for the AI Robotics Strategy". Based on this outline, further discussions will be held, and METI aims to finalize the "AI Robotics Strategy" by the end of March 2026.
- While the strategy will focus primarily on multi-purpose robots, it also will cover AI-equipped machine systems capable of autonomous control, such as automated vehicles, drones, and unmanned aircraft.
- In formulating the strategy, METI will identify and organize the key actions for each phase, focusing on both the supply side and the demand side to promote the development, implementation, and market entry of multi-purpose robots. In particular, the following points will be reviewed.
  - **Supply Chain Transformation**: In light of AI advancement and the trend toward

[3] https://www.meti.go.jp/shingikai/mono_info_service/ai_robotics/20251008_report.html (in Japanese)

Software Defined Robotics (SDR), the strategy aims to gradually transition to a supply system with high versatility and scalability through the use of open-source technologies, not only for specific clients, but also for broader applications.

- **Achieving World-Leading AI Robotics**: Initially, the development of foundational domestic robot models will be promoted in training environments. Based on these models, measures to accelerate the development cycle towards implementation will be reviewed.
- **Identification of Key Industrial Domains and Support for Implementation**: In light of significance of economic impact and high feasibility of adoption industrial domains and tasks which should be prioritized in a long term will be identified and supported. A roadmap for the introduction of multi-purpose robots will be developed, and tailored support will be provided based on the characteristics of each domain.
- **Establishment of Centers of Excellence (CoE)**: The strategy promotes the creation of hubs in Japan where top-tier talent and information can gather, enabling development and demonstration activities, as well as fostering talent through collaboration between industry, academia, and the government.

Takeaway: Based on this outline, the AI Robotics Strategy is scheduled to be finalized by the end of March 2026. EU companies involved in Japan's AI robotics market should monitor these discussions closely.

The 18th Japan-ASEAN Cybersecurity Policy Meeting was held[4]

(Ministry of Internal Affairs and Communications, National Cybersecurity Center, Ministry of Economy, Trade and Industry, October 16)

- The 18th Japan-ASEAN Cybersecurity Policy Meeting was held in Tokyo, Japan, over two days on October 8 and 9, 2025. Since its inception in 2009, this annual meeting has served as a key platform to strengthen international cooperation and joint initiatives between Japan and ASEAN Member States in the field of cybersecurity.
- At this year's meeting, participants exchanged views on the direction of national cybersecurity policies, reviewed progress in the ongoing Japan-ASEAN collaborative initiatives, and discussed approaches to further enhance future cooperation.
- Representatives from ASEAN Member States, the ASEAN Secretariat, and relevant Japanese government ministries shared their respective policy priorities and future initiatives. The meeting also reviewed the outcomes of the cooperative activities agreed upon at the previous session, reaffirming the commitment to deepen Japan-ASEAN collaboration, both on governmental and multi-stakeholder (public-private-academic)

[4] https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00262.html (in Japanese)

levels. Key areas of cooperation include:

- Development of the Japan-ASEAN Cybersecurity Policy Handbook
- Workshops on Critical Infrastructure Protection
- Public-Private-Academic Collaboration
- Mutual Notification Mechanisms
- Japan-ASEAN Cyber Exercises
- Joint Awareness-Raising Initiatives
- Capacity Building Programs
- Operation of Working Groups

Takeaway: Participants reaffirmed their shared commitment to advancing these initiatives and further strengthening Japan-ASEAN cybersecurity cooperation. The 19th Japan-ASEAN Cybersecurity Policy Meeting is scheduled to be held in Thailand in October 2026.

Industry

Japan Publishes OT Security Guidelines for Semiconductor Device Factories – Finalized after Public Consultation[5]

(Ministry of Economy, Trade and Industry, October 24)

- On October 24, 2025, Japan's Ministry of Economy, Trade and Industry (METI) finalized and published the OT Security Guidelines for Semiconductor Device Factories in both Japanese and English. After a 60-day public consultation period starting on June 27, 2025, METI reviewed stakeholder feedback and made the necessary revisions before finalizing the guidelines.
- Based on the economic and national security importance of the semiconductor industry, as well as the increasing amount of cyberthreats and risks, and to ensure international consistency, the guidelines provide comprehensive security measures designed to strengthen operational technology (OT) cybersecurity in semiconductor manufacturing, in alignment with overseas security standards such as SEMI E187/E188 and NIST CSF 2.0.
- The contents of the guidelines are generally the same as the draft guidelines previously introduced in "Japan Publishes Draft OT Security Guidelines for Semiconductor Factories – Open for Public Consultation".[6] While most aspects remain unchanged, Chapter 3 has been updated to identify not only risk sources (i.e., threats, vulnerabilities, and vulnerability IDs), but also to identify and address security incidents specific to semiconductor device factories by leveraging risk management frameworks (such as CPSF and NIST CSF 2.0).
- Looking ahead, METI plans to explore linking the security measure standards outlined in the guidelines to the requirements of its investment promotion policies for the semiconductor industry.

Takeaway: The primary target of these guidelines is manufacturing departments of semiconductor device manufacturers. European companies operating in this sector and having manufacturing establishment in Japan are encouraged to pay close attention to and implement compliance of the guidelines.

[5] https://www.meti.go.jp/press/2025/10/20251024002/20251024002.html (in Japanese)
[6] https://www.eu-japan.eu/publications/monthly-japanese-policy-and-regulatory-developments-news-august-2025

Public Consultation on the Draft Guidelines on the Roles Expected of Cyber Infrastructure Providers[7] [8]

(Ministry of Economy, Trade and Industry, October 30)

- On October 30, the Ministry of Economy, Trade and Industry (METI) and the National Cybersecurity Office (NCO) published draft guidelines on the roles expected of cyber infrastructure providers. To obtain feedback from domestic and international stakeholders, a 60-day public consultation period was announced, with a deadline of December 30, 2025.
- In response to the increasing number of cyberattacks targeting vulnerabilities across the software supply chain, concepts such as "Secure by Design" and "Secure by Default" have been gaining support. There is also increasing activity in the EU and US in regard to enacting and implementing legislation, such as the adoption of the Cyber Resilience Act (CRA) in the EU, and establishing new standards and guidelines in the US. In addition, Japan's Basic Act on Cybersecurity was amended in July 2025 to require suppliers of information systems to make efforts to support users in securing their systems. Following the amendment, the guidelines were drafted to specify the roles and responsibilities of cyber infrastructure providers in enhancing cybersecurity resilience and to promote the fundamental assurances granted by cybersecurity.
- The draft guidelines organize the responsibilities and specific actions of cyber infrastructure providers and their customers into six categories, with the goal of enhancing cybersecurity resilience in the software supply chain. Cyber infrastructure providers can use the guidelines as a checklist to assess their own efforts and efforts of providers to ensure the security of software supply chains, while customers can use it as a means of selecting the appropriate vendors and implementing effective risk management measures.
- Based on the feedback received from the public consultation, METI and NCO are planning to finalize the guidelines around by the end of this year, and thereafter to expand the accompanying checklist and other related materials to promote effective use of the guidelines.

[7] https://www.meti.go.jp/press/2025/10/20251030002/20251030002.html (in Japanese)

[8] https://public-comment.e-gov.go.jp/pcm/detail?CLASSNAME=PCMMSTDETAIL&id=595225040&Mode=0 (in Japanese)

Human Rights/Environment/Climate

7th International Conference on Carbon Recycling 2025[9]

(Ministry of Economy, Trade and Industry; October 10)

- On October 10, the Ministry of Economy, Trade and Industry (METI) and the New Energy and Industrial Technology Development Organization (NEDO) jointly held the Seventh International Conference on Carbon Recycling (the "Conference").
- International collaboration, challenges in technological development, and future prospects aiming at carbon recycling were the main agenda items of the Conference.
- Participants from industry, academia, and government reaffirmed their commitment to develop carbon recycling technologies.
- Cooperation in developing carbon recycling technologies across industries and developing business models for forming a carbon recycling market were encouraged.
- Expanding the production scale, lowering the procurement cost of CO_2 as a raw material, and improving efficiency throughout the supply chain are keys to the success of promoting carbon recycling.
- A summary document of the Conference can be found on this website: https://www.meti.go.jp/english/press/2025/pdf/1010_001a.pdf

Takeaway: Japan is continuously looking for collaboration opportunities to develop carbon recycling technologies.

12th Annual Meeting of the Innovation for Cool Earth Forum[10]

(Ministry of Economy, Trade and Industry; October 10)

- On October 8 and 9, METI and NEDO hosted the 12th annual meeting of the Innovation for Cool Earth Forum (ICEF).
- ICEF is an international platform for experts and leaders from different fields around the world to promote collaboration among academia, industry, and government officials to develop energy and environmental–related innovations to solve climate change.
- The main agenda item for this year was "Innovation for Green Transformation (GX) and Security."
- It was affirmed that energy security, supply chain resilience, and access to critical materials are front-line concerns and that a new innovation ecosystem for global decarbonization is important.
- The statement published by ICEF can be found on this website: https://www.meti.go.jp/press/2025/10/20251010004/20251010004-a.pdf

9 https://www.meti.go.jp/english/press/2025/1010_001.html
10 https://www.meti.go.jp/english/press/2025/1010_002.html

Takeaway: Global collaboration for innovation in the field of emissions reduction is key to achieve sustainable economic growth and energy security.

DISCLAIMER: The information contained in this report has been compiled by one or several independent experts and reflects the views of the author(s) indicated on the front page and above, and not necessarily the views of the EU-Japan Centre for Industrial Cooperation nor the views of the European Authorities. It is made available for general information and non-commercial purposes only. It does not claim to be comprehensive or up to date and is not intended to provide legal or other advice. No person should rely on the contents of this report – or of internet web sites or other information sources indicated in this report – without first obtaining advice from a qualified professional person. This report is made available on the terms and understanding that the EU- Japan Centre for Industrial Cooperation and the European Authorities, which have not verified its content, are not responsible for the results of any actions taken - or omitted to be taken - on the basis of information in this report, nor for any error in or omission from this report, or for any plagiarism. The EU-Japan Centre for Industrial Cooperation and the European Authorities expressly disclaim all and any liability and responsibility to any person in respect of anything and the consequences of anything, done or omitted to be done by any such person in reliance, whether wholly or partially, upon the whole or any part of the contents of this report. Without limiting the generality of the above neither the EU-Japan Centre for Industrial Cooperation nor the European Authorities shall have any responsibility for any act or omission of the author(s) of this report.
Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Innovation Council and SMEs Executive Agency (EISMEA). Neither the European Union nor the granting authority can be held responsible for them.

COPYRIGHT: The contents of this report are protected by copyright under international conventions. Reproduction is authorized for non-commercial purposes, provided that (i) the name of the author(s) is indicated and the EU-Japan Centre for Industrial Cooperation is acknowledged as the source, (ii) the text is not altered in any way and (iii) the attention of recipients is drawn to this warning. All other use and copying of any of the contents of this report is prohibited unless the prior, written and express consent of the EU-Japan Centre for Industrial Cooperation is obtained. All logos and figures published in this report are copyrighted and may not be reproduced without the full consent of their respective author(s).
GOVERNING LAW AND JURISDICTION: Any dispute arising from or related to the use of this report and/or the information in this report shall be submitted to the exclusive jurisdiction of the competent courts in Brussels, Belgium, which will apply Belgian law, with the exclusion of private international law rules.

Published by the EU-Japan Centre for Industrial Cooperation.