JEITA Japan Electronics and Information Technology Industries Association

5 August 2021

JEITA Position Paper on the European Commission's Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS

The Japan Electronics and Information Technology Industries Association (JEITA) is Japan's leading ICT association, with around 400 members from Japan and abroad and a Europe office in Brussels. JEITA serves as a platform for connecting industries such as electronic components and devices, electronic equipment, and IT solutions and services, as well as stakeholders in those industries.

We appreciate this opportunity to share our views on the European Commission's "Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts" (below, "Regulation").

In May 2018, JEITA released a set of recommendations on a basic approach to the use of artificial intelligence (AI). Entitled "Towards the Implementation of an Artificial Intelligence Society to Realize the SDGs and Society 5" (https://home.jeita.or.jp/press_file/20181002154214_5ArIOKGNLH.pdf), these recommendations emphasized the following five points:

(1) AI exists for the sake of society so therefore it should be actively used.
(2) Importance of a wide and accurate understanding of AI by the general public
(3) Necessity of creating social systems for practical use of AI
(4) International cooperation to promote the societal implementation of AI
(5) Need for a broad perspective in HR development in the era of AI

This approach, which we believe has much in common with the approach taken in Commission's explanatory memorandum on the proposed Regulation, forms the basis for our comments below.

The first three sections address the proposed Regulation as a whole, with the subsequent four sections addressing specific articles.

1. Risk assessment of AI introduction under a risk-based approach

JEITA understands the specific objectives of the Commission's AI policy package to be:
- to ensure that AI systems are safe to use and respect fundamental rights and European Union values;
- to develop the legislative systems to promote innovation and AI industry development;

- to enhance governance and effective enforcement of existing law on fundamental rights and safety requirements applicable to AI systems; and
- to introduce regulations for lawful, safe and trustworthy AI applications, thereby facilitating the development of a single market in the EU.

We understand that these objectives are designed to promote the development and use of trustworthy AI systems in order to use new data and cross-sectoral data to resolve social challenges and ensure national security. JEITA respects and endorses these objectives.

We also support the EC's adoption of a regulatory approach that introduces only the minimum necessary requirements based on the degree of risk entailed by AI system use and harmonized with existing regulations so as not to constrain the placement of AI solutions.

We do believe, however, that a risk-based approach requires undertaking an appropriate comparative risk assessment before and after the use of AI. Given the growing number of cases in which AI judgement surpasses human judgement—automated driving systems and medical systems, for example—the minimum necessary new regulations should be designed and introduced for AI systems based on the said comparative analysis of the risks.

2. Balancing innovation and regulation

Sound market formation and growth in areas where technology is rapidly evolving will require balancing the development of an attractive environment that promotes local innovation, draws foreign firms to Europe, nurtures and grows new companies, and accelerates investment with a regulatory framework that ensures use of safe and secure technology and respect for EU values.

2.1 Design and introduction of swift governance and regulation matched to the pace of technological advance

Positioning the EU as a global AI development hub will require creating a framework whereby humans set outcomes geared to objectives, problems, and uses, with diverse data then used cross-border in a rapid cycle of experimentation and learning, while updating evaluation criteria as appropriate. Speed is critical when upgrading AI systems and applying the latest technologies, and over-application of conventional regulatory instruments such as third-party certification (Article 43) and CE marking (Article 49) may delay market placement and dissemination. Governance and regulations must be designed and introduced swiftly enough to keep pace with technological advance.

2.2 Correcting the balance between the compliance effect and the cost burden to ensure industrial competitiveness

The raft of pre- and post-market requirements for high-risk AI inflict heavy compliance costs (time, labor) each time a new technology is introduced or an upgrade undertaken. This will pose a major barrier to innovation by AI system providers, and particularly SMEs and ventures that have limited capacity to deal with such costs compared to mega platforms. It could also reduce incentive to invest in Europe and hamper the development and strengthening of AI firms. To ensure industrial competitiveness within Europe, high-risk AI

requirements need to be adjusted and minimized. Pre-market regulations should also be kept to the minimum, with users of products and services using AI systems required to create, implement, and announce plans for post-market monitoring and issues dealt with as they arise.

3. Definition of prohibited and high-risk AI systems and requirements based on use case (area)

Certain AI technologies have been designated as prohibited or high-risk, but the same AI technology will have a different risk according to the method of application and use case (area). AI systems are also not necessarily used in isolation; there are many cases where the product or service provider as the user in fact combines and uses multiple different AI systems. It is neither appropriate nor realistic to lay down blanket requirements for high-risk AI comprehensively in the Regulation (particularly risk management systems (Article 9), data and data governance (Article 10), record-keeping (Article 12), and human oversight (Article 14)). The regulatory scope and application of requirements to AI systems should be determined based on the risk for the particular use case, and it will therefore be critical to create effective AI system guidelines for each use case in conjunction with the relevant industries.

For example, while AI systems exclusively developed or used for military purposes are excluded from the scope of the Regulation, the reality is that private-sector systems too can be attacked, and consequently need to be equipped with legitimate defense functions against such attacks. However, defining such AI systems as high-risk would not only be unfair but could also boost private-sector system risk. Prior thought should therefore be given to extending the same treatment in such cases as for systems for military purposes.

4. Views on key articles

Our views and suggestions in relation to individual articles are as follows.

TITLE I: GENERAL PROVISIONS

▪ Article 2: Scope

Obligations in the case of 1(c) providers and users of AI systems that are located in a third country, where the output produced by the system is used in the EU

The scope of obligations in the case of 1(c) need to be further clarified. For example, under Article 52.3, if a firm outside the EU uses AI systems to create video content (“output”) which is transferred to a party showing content within the EU who shows the video content in question, disclosing that the content has been artificially generated or manipulated can in some cases be beyond the capacity of AI system users outside the EU. The disclosure obligation should therefore be placed on the EU operator showing the content.

▪ Article 3: Definitions

(36) Definition of remote biometric identification systems classified as high-risk AI systems

In defining remote biometric identification systems, specific guidance should be prepared as to what type of entity constitutes a “user,” what distance constitutes “at a distance,” and what the criteria is for determining whether there has been effective consent of the person to be

identified. If “at a distance” constitutes only the physical distance between the target and the device acquiring biometric information, this should be clearly stated. The current wording also leaves open the possibility that applications and technologies posing a comparatively low risk from a user perspective could be interpreted as falling within this definition. Consideration should therefore be given to eliminating ambiguity as to what constitutes a high-risk AI system, envisaging specific applications.

If this definition intends to address whether the target is aware that biometric identification is being conducted, that should be specified.

Use cases should be specified, including what methods of use would constitute “without prior knowledge of the user of the AI system.”

TITLE II: PROHIBITED ARTIFICIAL INTELLIGENCE PRACTICES

▪ Article 5

The regulatory scope of “prohibited AI” must be clearly restricted to that truly necessary from the perspective of legal certainty and predictability, and the grounds for that scope as well as risk measurement and assessment methods should be further clarified.

For example, while AI systems that deploy subliminal techniques are defined as “prohibited AI,” it is not always easy to determine what constitutes a subliminal effect. The scope here should be limited to the deliberate use of subliminal techniques and exclude those AI systems used for audiovisual content, gaming, and marketing commercials, etc., that could have an unintentional subliminal effect.

The use of “real-time” remote biometric identification systems for the purpose of law enforcement is deemed as “prohibited AI.” However, the scope needs to be made clearer based on consideration of the danger posed by each particular use case, including specific examples of “publicly accessible spaces” (the scope of which is unclear in the current draft). Clarification is also needed in relation to, for example, whether this applies when law enforcement institutions use AI systems to police their own facilities. To give another example, does partnership between law enforcement institutions and the private sector whereby a private-sector AI system detects suspicious materials/activities and notifies the law enforcement institution constitute “prohibited AI”?

The use of “real-time” remote biometric identification systems for the purpose of law enforcement is already covered under Article 10 of the Data Protection Directive (EU) 2016/680 for police and criminal justice authorities, and there are also requirements under EU laws and domestic laws concerning the need for confidentiality and appropriate protection measures for the rights and freedoms of the data subject. We therefore believe that the issue would be better handled by clarifying the guidelines in the Data Protection Directive rather than addressing it in this Regulation.

TITLE III: HIGH-RISK AI SYSTEMS

CHAPTER 1: CLASSIFICATION OF AI SYSTEMS AS HIGH-RISK

▪ Articles 6-7 and Annex IIA/B, III
Making the scope of "high-risk AI" too broad could impede innovation in the EU. The regulatory scope must be clearly restricted to that truly necessary from the perspective of legal certainty and predictability, and the grounds for that scope as well as risk measurement and assessment methods should be further clarified. For example, we believe that the following revisions and considerations are needed:

- Clarification of the definition of remote biometric identification systems considered high-risk
It should be clarified based on the danger posed by particular AI systems whether systems that extract face and body features and classify them on a temporary basis, such as facial recognition on smart phones that recognize their owners, facial recognition-based payments, identity verification at customs/immigration, and in-store private-sector AI systems determining customers' lines of movement for marketing purposes, constitute high-risk remote biometric identification systems.

- Exclusion from high-risk AI classification when the risk of adverse impact on fundamental rights is sufficiently low
One cutting-edge technology which is gradually being standardized is template protection, whereby biometric information can be registered and checked while retaining anonymity. Biometric identification by an AI system applying this technology to input data can only produce results for specific applications and does not allow any inference of attributes such as gender, ethnicity, or age. Where it has been confirmed that AI systems designed for biometric identification and categorization of natural persons have engaged in sufficient learning using proper data and that the data will not lead to attribute-based discrimination, such systems should be excluded from high-risk classification.

In terms of the handling of the personal data included in industry data (operating history, etc.), where it has been confirmed in an AI regulatory sandbox that the risk of fundamental rights being infringed is sufficiently low, all or some of the requirements should be eased for the purpose of having AI technologies use data to solve social problems.

- Exclusion from high-risk AI classification or easing of requirements in cases where safety and fairness have been sufficiently ensured under existing laws and regulations in the particular area (critical infrastructure, medical devices, etc.), operational consistency with related sectoral regulations
Where AI is used in safety-related areas in relation to the management and operation of critical infrastructure, most management and operation systems are designed to also ensure safety through means other than an AI system. In cases where systems have been designed to eliminate risk, such as failsafe and fault-tolerant systems, and where the risk has been deemed sufficiently low using, for example, an AI regulatory sandbox, the use of AI presents no specific risk.

In the case of infrastructure, the AI risk presumably differs across safety equipment and operations and maintenance systems, so high-risk AI classification should be restricted from

the perspective also of devices and systems. Specific examples and greater clarification for the various technological domains are needed in relation to safety components. For example, home AI camera monitoring system applications run the gamut from fire detection and baby monitoring to crime prevention. Because the extent of what comprises a safety component is unclear in this proposed Regulation, further clarification needs to be provided through guidelines, etc.

In the case of medical devices, the medical sector is already covered by EU-MDR (EU 2017/745). The requirements of the Regulation should be in line with and complementary to those of EU-MDR (EU 2017/745).

- Providing compliance incentives to simultaneously reduce the cost burden on companies and boost legal effectiveness

Incentives should be designed and applied at the same time as the Regulation goes into effect. In the context of public procurement by the Commission or EU member countries, this could mean assessing companies that create appropriate codes of conduct and consistently comply with AI regulations and, according to the assessment results, reducing the burden of AI-related requirements. Such an approach would simultaneously reduce the compliance burden borne by companies as well as increasing legal effectiveness.

Additionally, in the case of diagnostic AI that supports safety component maintenance, the AI-based risk can be alleviated because a human makes the final decision based on the AI information output. Consequently, a measure would be possible whereby all or part of the necessary requirements are eased or eliminated.

CHAPTER 2: REQUIREMENTS FOR HIGH-RISK AI SYSTEMS (Articles 8-15)

▪ Article 9: Risk management system

- Paragraph 2(a) calls for identification and analysis of the “known and foreseeable risk” associated with each high-risk AI system, and Paragraph 2(b) calls for estimation and evaluation of the risks that may emerge when the high-risk AI system is used in accordance with its intended purpose and under conditions of reasonably foreseeable misuse.

However, not only in the case of these requirements but in general, the responsibility for deliberate or unintended misuse should be laid not on the provider but on the user engaging in said deliberate or unintended misuse, just as in the case of deliberate or unintended misuse of a chopping knife or a car.

- The requirement in paragraph 4(a) of “elimination or reduction of risks as far as possible through adequate design and development” needs clarification. In addition, given that there could be multiple risks and potentially also trade-offs, guidelines need to be provided.

▪ Article 10: Data and data governance

- The data set requirements in paragraph 3 (“relevant, representative, free of errors and complete”) are not realistic from a data science perspective. If requirements are to be made in

this context, they must be achievable and a method needs to be indicated for proving compliance.

- The provision requiring the use of complete data is unclear; it would be more realistic to promote the use of reliable data. For example, it could be recommended that data acquired from trustworthy institutions such as data exchanges and data banks be used for training, validation and testing data. Applying consent management technology (technology for managing data on the reasoning behind predicted results) and data history indicating that data can be trusted would contribute to better management of the process from data processing to machine learning and the utilization of the results from that learning, ensuring the transparency of data sources. Enabling data sources to be searched would be another method.

- Paragraph 4 requires taking into account the geographical setting. Such requirement would make learning from globally integrated data virtually impossible and the cost of such learning, if possible, would be phenomenal. Moreover, the very act of assessing particular characteristics or elements would run the risk of creating bias.

- Paragraph 5 notes that "To the extent that it is strictly necessary for the purposes of ensuring bias monitoring, detection and correction in relation to the high-risk AI systems, the providers of such systems may process special categories of personal data … , subject to appropriate safeguards for the fundamental rights and freedoms of natural persons, including technical limitations on the re-use and use of state-of-the-art security and privacy-preserving measures, such as pseudonymisation, or encryption where anonymisation may significantly affect the purpose pursued." However, the consistency of this with pseudonymization and encryption required in the context of Article 25 (Data protection by design and by default) and Article 32 (Security of processing) in the General Data Protection Regulation (GDPR) is unclear. Particularly in relation to remote biometric identification and the use of high-risk AI to which GDPR pseudonymization and encryption requirements could potentially apply, clear guidance harmonized with the GDPR must be formulated and provided as soon as possible.

▪ Article 11: Technical documentation
The Paragraph 1 requirement to "provide national competent authorities and notified bodies with all the necessary information to assess the compliance of the AI system with those requirements" presents dangers from the perspective of respecting confidentiality. While Article 70, etc., note that competent authorities and notified bodies are obliged to respect confidentiality, the information to be provided needs to be determined on the basis of discussion with multiple stakeholders, including industry and AI experts.

▪ Article 12: Record-keeping
- Providers are required to store log data and engage in data-based monitoring after market placement, but this will be impossible unless the provision of information from users to providers is mandated under law. From the perspective of protecting personal data and trade secrets, providers should not receive any more data, log data included, than is necessary.

▪ Article 13: Transparency and provision of information to users

- This article requires transparent operation of high-risk AI systems and provision of information to users. However, the nature and extent of the information required is unclear and guidelines must be provided that include specific and achievable instructions.

▪ Article 14: Human oversight
- While we understand the need for this requirement, we would prefer to see monitoring requirements that are practical for companies, such as carefully considering the level of human involvement required based on the respective strengths and weaknesses of human and AI monitoring.

- The requirement is clearly impossible in the case of closed-loop AI operation (no human involvement) and should be eased or eliminated in such cases to the extent that risk elimination such as independent redundant safety systems have been built into the system from the design stage. For example, because high speed processing of 10ms or less is only possible for a machine, where it is confirmed that the risk to the system as a whole is sufficiently low, this should be excluded from regulation regardless of the sector.

- In those sectors where AI judgement surpasses human capacity, this requirement should be eliminated or eased for cases in which high precision and no automation bias can be proved.

▪ Article 15: Accuracy, robustness and cybersecurity
- While it is the providers who developed those systems that can take mitigation measures, users are the ones who know the current condition/performance of AI systems. To institute the mitigation measures for AI systems that continue to learn so as to properly address possibly biased outputs after market placement as noted in Paragraph 3, contracts would need to be concluded with a wide range of companies in the supply chain. The massive cost that this would entail could pose a barrier to market participation by providers and users.

<u>CHAPTER 3: OBLIGATIONS OF PROVIDERS AND USERS OF HIGH-RISK AI SYSTEMS AND OTHER PARTIES (Articles 16-29)</u>
▪ Articles 16-29: Appropriate distribution of obligations between AI system providers and users
- These articles need to be revised to clarify that, in order to ensure that providers meet their obligations, users too are required to engage in proper usage and cooperate with providers so that, for example, data sources can be managed, bearing in mind consistency also with the division of obligations in the GDPR and other existing laws and regulations.

- Distinguishing AI providers and AI users and imposing strict regulations on the former could conversely impede the formation of a trustworthy ecosystem. To ensure proper use of AI, rather than requiring efforts from providers alone, it would heighten legal effectiveness to make it clear that efforts are required across the ecosystem, encouraging users too to take the appropriate steps.

▪ Article 16: Obligations of providers of high-risk AI systems

- There should be a mechanism here whereby providers who undertake a certain level of risk scrutiny are entitled to a certain level of exemption. For example, if a user makes a change, without provider involvement, to the usage method that does not fall within reasons for exemption from prohibited AI categorization of a product or service supplied by a provider, it would be unreasonable to hold the provider responsible for such change.

- It should be clarified that the obligations on providers noted in Article 16 are to be undertaken with user cooperation. It should also be made clear that where a user uses a product or service in a manner that contravenes the manual, the provider will not be deemed to be at fault.

▪ Article 20: Automatically generated logs
- The reference in Paragraph 1 to keeping logs that are within the provider's control lacks clarity and could result in big companies and other providers with significant control capacity being required to keep all logs. The specifications for those automatically generated logs that should be kept, including categories (errors and warnings only, data not required to be kept, etc.) and storage periods (five years from the event in the case of errors, one year in the case of warnings, etc.), should be specified in harmonized standards, etc.

▪ Article 25: Authorised representatives
- Ensuring fairness for participation by companies outside the EU: To ensure that conformity assessment does not become a barrier to market participation by companies outside the EU, the conformance mechanism should be disclosed as soon as possible, with that mechanism enabling non-EU companies to engage in prior consultations and receive official certification in relation to the Regulation and related laws and regulations (for example, online certification for companies outside the EU without appointing authorized representatives).

- Certain regulations should be added on post-market placement monitoring based on templates, etc., to make it easy for AI providers to acquire log data from users.

<u>CHAPTER 5: STANDARDS, CONFORMITY ASSESSMENT, CERTIFICATES, REGISTRATION</u>
▪ Article 43: Conformity assessment
- Paragraph 4 calls for high-risk AI systems to undergo a new conformity assessment procedure whenever they are substantially modified. AI systems are by nature improved agilely over time through software upgrades and learning. Requiring conformity assessment each time would impose an excessive burden on providers and would not be realistic. The standard for "substantially modified" as defined in Article 3 (23) must be clarified so as not to impose an excessive burden on providers.

▪ Article 49: CE marking of conformity
- See comment on Article 2.1.

TITLE IV: TRANPARENCY OBLIGATIONS FOR CERTAIN AI SYSTEMS (Article 52)

▪ Article 52: Transparency obligations for certain AI systems

- This provision needs to be made clearer in terms of the scope and requirements in relation to AI systems intended to interact with natural persons.

- The provision calls for users of an AI system that generates or manipulates image, audio or video content to disclose that the content has been artificially generated or manipulated. Does this include films, music videos, video content (including game and marketing materials) that have traditionally used computer-generated imagery (CGI) but not for the purpose of deceiving people (like deep fakes)? If so, the disclosure method must be clarified.

TITLE VI: GOVERNANCE (Articles 56-59)

▪ Articles 56-58: Establishment of AI governance through multi-stakeholder and international collaboration

- When the European Artificial Intelligence Board (EAIB) and other bodies engage in detailed consideration of requirements in relation to the entry into force of this Regulation, multiple stakeholders including industry and AI experts should also participate so as to boost legal stability and predictability and ensure that the content is effective and realistic. Commission members and staff should review said content on an ongoing basis in line with technological advance and development. International collaboration and partnership, Japan included, will also be important in establishing and maintaining a governance framework with a high level of global commonality. Fairness should also be ensured so that conformity assessment does not become a barrier to non-EU firms' participation in the EU market.

- If there are technologies found to meet the requirements of this Regulation as a result of considerations at the EAIB, etc., or application of such technologies make considerations at the EAIB, etc. unwarranted, these technologies should be noted in guidelines as examples of recommended technologies and a compliance mark equivalent to CE marking should be available and displayed on the product. The foregoing arrangements should also be provided to technologies, if any, on which EU members adopt a unified rules for market placement.

- Because this Regulation will have a major impact on organizations with global business operations, regardless of location, ongoing discussion must be conducted in international frameworks even after the Regulation has been introduced. A transparent multi-stakeholder approach, and particularly participation by business entities and private companies, should be encouraged in discussion at the EAIB and the High-Level Expert Group on Artificial Intelligence as well as related discussion.

TITLE VII: EU DATABASE FOR STAND-ALONE HIGH-RISK AI SYSTEMS (Article 60)

▪ Article 60: EU database for stand-alone high-risk AI systems

- Paragraph 3 notes that information contained in the EU database shall be accessible to the public. While clarifying the definition of what is deemed high-risk AI, not only sharing a database/collection of cases that do constitute high-risk AI but also sharing a database/collection of cases that do not constitute high-risk AI will help providers and other

parties make judgements in this regard and further increase the transparency of such determinations. Creating a mechanism to answer questions from providers, etc., as to whether a system constitutes high-risk AI and adding those answers to the above-mentioned database on a regular basis would boost the effectiveness of the Regulation.

TITLE VIII: POST-MARKET MONITORING, INFORMATION SHARING, MARKET SURVEIILLANCE (Articles 61-68)

▪ Article 61: Post-market monitoring

- Regulations on post-market monitoring systems should be designed with due consideration to the scale and number of the AI systems covered.

▪ Article 64: Access to data and documentation

- Companies should not be required to provide market monitoring institutions access to their source code for a conformity assessment, as source code constitutes an important proprietary asset of the companies driving corporate competitiveness. Consideration needs to be given to an appropriate method of dealing with any suspicions requiring investigation, should these arise, without requiring source code disclosure, such as first using fair standards to call companies to account whether they are EU or non-EU companies.

- A blanket source code disclosure requirement could lead to an outflow of intellectual property and dampen the motivation to innovate. Disclosure should be strictly limited to those entities among the Commission, EU member country authorities, and designated conformance institutions truly necessary in terms of achieving the objective of market monitoring, such as serious legal infringements, similar to the approach in Article 70, and should be implemented within an extremely limited scope so as to prevent abuses of power.

- Article 73, Chapter 8 of the EU-Japan Economic Partnership Agreement (EPA) explicitly bans source code disclosure requirements between Japan and the EU. We assume that priority would be given to the EPA provision but call for consistency with this provision.

TITLE X: CONFIDENTIALITY AND PENALTIES (Articles 70-72)

▪ Article 71: Rectification of penalties

- The broad penalty scope, application of penalties to virtually all obligations in the Regulation, and the extremely high penalties proposed here could needlessly heighten the activity risk for EU and non-EU companies (and particularly start-ups) operating in the EU market. This provision notes that due regard shall be given to the “nature, gravity and duration of the infringement and of its consequences” in deciding on the amount of the administrative fine in each individual case. The amount of the penalty will presumably therefore differ in cases where there is an actual infringement of fundamental rights or where such an infringement could occur, as opposed to cases where the infringement is nominal and poses no possibility of a fundamental rights infringement. More detailed information should be provided on penalty standards and penalty breadth to ensure transparency of these administrative actions.

- For unintentional infringements and accidents, rather than immediately applying the excessive penalties stipulated in Article 71, the Commission should spearhead the establishment of a committee to investigate and identify causes, and prevent the reoccurrence of said infringements and accidents by announcing results of the investigation. With the public and private sector cooperating together, this approach will promote trustworthy AI innovation.

- Detailed guidelines should be provided for companies as well as relevant authorities on retention of documents/materials necessary or used to assess compliance with the Regulation. The retention periods for certain items should be sufficiently longer (longer than for logs in Article 20, etc.).

TITLE XI: DELEGATION OF POWER AND COMMITTEE PROCEDURE (Articles 73-74)

▪ Article 73

- According to this provision, in considering a delegated act for amending the list in Annex III, the European Commission will look at the scope of existing EU legislation as noted in Article 7.2(h). Multi-stakeholder participation, including from areas to be added and industries related to AI systems, will be vital in this context so as to increase legal stability and predictability and ensure effective and realistic content. It will also be important to establish and maintain a governance framework with high global commonality through international collaboration and partnership, Japan included.

TITLE XII: FINAL PROVISIONS (Articles 75-85)

▪ Article 84

- Multi-stakeholder participation, including industry and AI experts, will be vital in evaluating and reviewing the Regulation following implementation so as to increase legal stability and predictability and ensure effective and realistic content. It will also be important to establish and maintain a governance framework with high global commonality through international collaboration and partnership, Japan included.