Japan Business Council in Europe

6 August 2021

JBCE Views on the European Commission's AI Act

Japan Business Council in Europe (JBCE) welcomes the proposal for a Regulation on a European approach for Artificial Intelligence ("AI Act").

JBCE supports the objectives of setting a horizontal framework for trustworthy development, deployment and use of AI, for both providers and users. We would, however, caution against excessive regulation, and relatively excessive sanctions for violations while it remains unclear what constitutes high-risk AI and which AI systems are prohibited. This could stifle innovation in AI and risk hollowing out the EU's competitiveness in this sphere. It may also mean that companies are more reluctant to enter the EU market.

Thus, JBCE advocates finding an appropriate balance between regulation and innovation. In this light, JBCE members would like to propose the following recommendations:

1. General provisions

- JBCE has concerns regarding the definition of an AI system (art.3(1)), and the AI techniques listed in Annex 1. The broad definition and wide range of techniques listed may lead to enforcement authorities in member states interpretating systems generally not considered as AI to be within the scope of the act. This will cause uncertainty and leads us to question if the envisaged benefits outweighs the costs and burdens. We therefore believe the definition of an AI system should be more specific and fit-for-purpose.
- A clear definition of AI represents the basis for the correct and effective interpretation and "use" of this Regulation. We understand the intention of adopting a broad definition of AI, but would encourage continued work with International Organisations such as the OECD to find consensus on what is meant by AI. These efforts should aim to find a universal understanding of AI systems, thus providing legal certainty. Without this, there will be different rules in different regions, creating significant legislative discrepancies and excessive burdens for industry, which risks discouraging innovation.
- Regarding art.3(14), which defines 'safety component of a product or system', it is not clear who will be responsible for judging what is a safety component. In our view, the provider is best positioned to make such a judgement - based on clear and comprehensive criteria, provided and maintained in a dedicated delegated act that should be adopted under the AI Regulation.

- According to art.3(36), one of the conditions for a system to be classified as a remote biometric identification system (RBI) is that the user of the system must not have any prior knowledge of whether the person identified by the system would be present and could be identified. However, it is not always easy to determine whether or not the user has such prior knowledge in each use case. Clarity on what constitutes prior knowledge would therefore be welcome. Further, if the term "at a distance" merely indicates physical distance between the device that reads the biometric data and the person whose biometric data is captured, JBCE recommends that this is clearly stated in its definition of RBI.

- The definition of 'publicly accessible space' in art.3(39) is very vague; recital 9 tries to clarify the term, but with little success. The term is crucial when it comes to determining whether the use of a particular RBI AI system for law enforcement purposes is prohibited or not under art.5(1)(d) and should thus be defined much more clearly in the main body of the Regulation.

2. Prohibited AI systems

- The term 'subliminal techniques beyond a person's consciousness' must be clarified (art.5(1)(a)). Further guidance is needed as to whether AI technologies used in immersive video games would be prohibited under this provision – one could argue that every immersive video game uses subliminal techniques.

- Even though in principle we support the idea of regulating the use of RBI in publicly accessible spaces for the purpose of law enforcement, we would like to ensure that art.5(1)(d) does not restrict the use of RBI in situations where the RBI technology poses minimal or no risk to the fundamental rights, health or safety of natural persons, or where it does pose a risk but that risk is outweighed by public safety concerns. The following two examples illustrate these points:
    - We believe that the use of RBI by law enforcement authorities for the purpose of guarding their facilities (e.g. a police station), including through the use of cameras within field of view (FoV), should be allowed.
    - It is not clear from reading the proposed Regulation whether private entities are allowed to report to law enforcement authorities' suspicious activity that they have detected using RBI AI systems. For example, would a shop owner be allowed to share data from a camera installed in their store which locates an individual suspected of shop lifting with law enforcement authorities?

3. High-risk AI systems

Reflections on the criterion of 'intended to be used'

- A crucial element of Annex III is whether an AI system is 'intended to be used' for a specific purpose, e.g. whether it is intended to be used by law enforcement authorities. As such, the 'intended use' determines whether an AI system falls

under one of the high-risk categories in Annex III. However, in reality some AI systems do not specify dedicated use cases, and whether such AI systems pose significant risk or not is dependent on how they are used. For instance, speech synthesis AI technologies (which artificially produce human speech) are typically purpose-agnostic; depending on how they are used, they may pose no risk, low risk or high risk.

- If the adopted version of the AI Regulation pegs whether an AI system is high-risk on the system's 'intended use', then the extensive compliance obligations imposed on providers (i.e. developers) in articles 9-15 become disproportionately onerous. In the case of providers of general-purpose AI systems, such providers may not be able to foresee all the high-risk use cases of the system they have created. At the same time, we should note that placing more obligations on users (rather than on providers) is not the solution to problems created by the 'intended use' criterion either. For instance, a user of an AI system classified as high-risk under the 'intended use' criterion of Annex III may not have much insight or power to address the fairness and robustness shortcomings of the system if they have adapted a general-purpose model provided by another company.

Classification of AI systems as high-risk

- We support the approach defined in Article 7(2) utilizing a narrow definition of high-risk systems that considers damages to health, safety and fundamental rights of persons but also severity, likelihood of their occurrence and plurality of potentially affected individuals.

- We also support the idea of dividing some categories listed in Annex II (where sectorial legislation will continue to be applied) and Annex III. However, we would encourage the European Commission and co-legislators to clarify both how Article 7(2) is going to be applied to the categories listed in Annex III, and how these categories (e.g. education, law enforcement) are going to be defined and periodically reassessed. We recommend that lawmakers further clarify and narrow the language in Annex III, taking into account the diversity of applications that may fall under some of the definitions. Equally important would be to clarify the procedure (Art 7) to update the list in order to give more clarity to AI providers and allow open discussion between Institutions and AI stakeholders (including industry).

- We appreciate the effort the European Commission makes in Chapter 2 to provide a detailed list of requirements for high-risk AI systems. However, we believe that is crucial to have flexible tools to help companies to easily and effectively provide the necessary documentation. For instance, a software produced by a company as a basic system that is later customized for different needs - without changing the fundamental architecture and purpose – should not be required to go through the same obligations it completed initially all over again.

- In some cases, a "one-size fits all approach" cannot be conducive for obligations

on different companies working across different sectors. It would be preferable to focus on the provision of the necessary information for that specific sector - in particular on Article 11 (Technical Documentation) and Article 12 (Record Keeping) – and to reduce administration as much as possible.

- JBCE calls for specific guidelines which would facilitate adherence to obligations, including on Data Governance, Transparency and Human Oversight (as is happening with GDPR).
- Regarding obligations for operators, the separation of "AI providers" and "AI users" (Chapter 3) and the strict regulation of the former may hinder the formation of a trustworthy ecosystem. In order to ensure safe deployment of AI, it is important to clarify that efforts must be undertaken not only by providers but by the entire ecosystem, including users.
- We welcome that the European Commission assessed existing EU regulatory frameworks for safety components and correctly identified the legislations listed on Section B of Annex II. These cover many of the most common areas of concern.
- It would be preferable to further limit the scope of high-risk AI in Annex III by categorizing it in detail, taking risks into consideration for each use case. For example, AI systems for electricity supply can be broadly categorized into business support systems and control systems, each of which has a different degree of risk. In the case of business support systems, even if there is a malfunction or misjudgment, the risk is limited or minimal. On the other hand, control systems pose a substantial risk that could lead to major power outages.
- In addition, going one step further, JBCE would suggest that “2. Management and operation of critical infrastructure” is deleted from Annex III, considering the fact that such applications should be under the scope of existing regulations (in Annex II). In cases where management and operation of critical infrastructure are not covered by existing regulations, then they would be assumed to not be critical from the safety point of view, even if a system error or human error occurs. In this regard, it would not be reasonable to introduce new regulations just because AI is used.
- In art.6(1), AI systems which are intended to be used as a safety component of a product are classified as high-risk. However, we would ask for greater clarity on criteria for a safety component (beyond the definition in art.3(14)). For example, electricity demand forecasting and PV power generation forecasting do not directly affect the safety of the power grid operation, but they are technologies that indirectly contribute to the stable supply of electric power and are systems for managing the power grid. From this perspective, it may be seen as a necessary component to ensure safety (stabilization of electric power). Would this mean these forecasting technologies are considered high-risk?
- Further, we believe that if a minimum level of safety and fairness is ensured or obliged by means other than AI, it should be excluded from the scope of high-risk AI. For example, when AI is used for safety-related aspects of the management

and operation of critical infrastructure, the majority of management and operation systems are designed to be safe by means of Failsafe concepts (ISO61508 or ISO26262) other than AI. In such cases, there is no specific risk that arises from the application of AI itself and, therefore, they should not be covered by this act.

- Within infrastructure AI applications, the risks of AI should be differentiated between safety devices and operational management systems. We also believe that the scope of high-risk AI should be limited from the perspective of devices and systems as well (as safety and fairness should not be overly dependent on AI.)
- In terms of the standalone AI uses listed in Art.6(2) & Annex III, we are concerned the scope remains unclear and leaves significant room for divergent interpretations. For instance, while Annex III designates AI uses for safety components in electricity supply as high-risk, it does not touch upon its exact scope and the specific risk which needs to be eliminated. We therefore strongly recommend the European Commission further clarifies the scope of Annex III, in a joint effort with businesses.
- Regarding art.7(2), we strongly recommend that industry is consulted when the Commission makes amendments to Annex III to update the high-risk AI systems list through delegated acts. Given that AI is a technology which continues to evolve rapidly, and its risks vary depending on context and purpose of use, policy discussions without industry would inhibit the capacity of authorities to flexibly adapt the regulations to the evolution of AI in the future.
- Art.7(2)(h)(ii) says Annex III can be updated when there is “effective measures to prevent or substantially minimize” risks in existing Union legislation. This should be widened to include when potential risks posed by a high-risk AI system are sufficiently eliminated or mitigated by technical or operational countermeasures (e.g. autonomous train systems with digital signaling systems that control train position to ensure safe distances between each train). It would then be appropriate to no longer consider the AI system as high-risk. As such, we suggest this should be a provision for updating Annex III accordingly.

Risk management system

- Art.9(2)(a) and (b) state that the provider of a high-risk system must identify and analyse the known and foreseeable risks associated with each high-risk AI system, and must also estimate and evaluate the risk that may emerge when the AI system is used in accordance with its intended purpose and under conditions of reasonably foreseeable misuse. Even though we agree that these obligations should be imposed on providers, we also believe that the user (rather than the provider) of the high-risk AI system should be held responsible if they misuse, negligently or intentionally, the AI system. Art.29(1) is a positive step in this direction, as it states that users must deploy high-risk systems in accordance with the instructions of use accompanying the systems. However, we believe that the language of that provision should be strengthened to clarify that the user should be held responsible for any instances of misuse. There should also be greater clarity on the type of

information, analysis, evaluation, and/or measures that providers should share with users regarding the risks posed by AI.

- The obligation to ensure the “elimination or reduction of risks as far as possible through adequate design and development” (art.9(4)(a)) is too broad and does not provide guidance in cases where there are trade-offs between reducing one type of risk and increasing another.
- We believe that the pass/fail criteria for AI system testing in art.9(5)&(6) should be clarified according to the purpose, target, and the foreseen impact the system will have.

Data and data governance

- In our view, special attention must be given to data governance requirements. Data governance is key for both innovation during the testing and implementation phases, and deployment of AI systems utilizing high quality data. Art.10 should therefore be better designed to make it possible for companies to test their AI systems without being subject to too many ex-ante obligations for “free of error” data. It is important for innovative AI applications to have ‘safe environments’ in which mistakes can be made (without affecting fundamental rights or principles, and while complying with GDPR requirements). The focus should therefore be on safety of the final AI system rather than the testing or training phases.
- Overall, art.10 should be more clearly drafted. It contains terms such as ‘relevance’, ‘representative’ and ‘appropriate data governance and management practices’, which exist on a spectrum. We need additional guidance on what the acceptable bar is for each of these terms. This should ideally be provided jointly by the EDPB and the European AI Board.
- In art. 10(2)(d), the definitions for 'the formulation of relevant assumptions' and 'the target data' would need to be clarified.
- Art. 10(3) stipulates that training/validation/testing data sets must be ‘free of errors’. This is impossible to guarantee in practice, especially as an ‘error’ is neither defined in general nor in the context of the AI system resilience / robustness required by Art. 15(3). As such, the Regulation should provide clear guidelines on what an acceptable level of errors in the data would be. This should include having the procedures for ensuring data quality outlined, depending on the subject. The same applies to AI systems already placed on the market; we believe that confirmation through prior evaluation should be done based not on possible biases, but an identified item (given that the cost of generating, training and testing data is so significant).
- It is not always ideal from a fairness perspective for a dataset to be ‘representative’ (see art.10(3)). For example, for facial analysis algorithms, having over-representation of minorities is key to prevent bias. Simply having 5% of your facial image dataset consisting of ethnic group A, or 10-15% of ethnic group B, even if

that is the proportion of those populations in the deployment context, will likely not be enough to train the algorithm to properly recognize individuals from those groups. We therefore suggest that, instead of mandating that datasets should be representative, art.10(3) should provide that datasets must be sufficiently diverse to mitigate bias.

- Art. 10(4) states that datasets shall consider the characteristics or elements that are particular to the specific geographical, behavioral or functional setting within which the high-risk AI system is intended to be used. Complying with such an obligation would mean that companies would not be able to use the same datasets in different regions, and in turn this would mean that the costs of developing AI systems would become enormous. For example, in cases where training AI requires personal data from other regions, it often triggers burdensome manual work by engineers to mask personal features in datasets in order to comply with privacy protection rules in different regions. Hence, we suggest the Commission and the EAIB continuously monitor for developments in state-of-the-art technologies which enable companies to efficiently transfer datasets between regions, and take these into consideration for the common specification.

- We welcome the possibility to process special categories of personal data referred to in the GDPR, as set in Article 10(5). However, as the consistency with the obligation imposed on processors by GDPR remains unclear, we recommend giving clear guidance on the data and data governance requirements, especially for remote biometric identification. It is also crucial to pose appropriate state-of-the-art security and privacy-preserving measures. In addition to pseudonymization or encryption, we recommend adding “biometric template protection”, as stated in ISO/IEC 24745, 30136 – particularly given that it is already obligatory that this technology is used under NIST SP800-63(B) when the biometric comparison is performed at a central verifier, since the potential for attacks on a larger scale is greater in central verifiers.

Technical documentation

- Overall, the level of documentation required under art.11(1) and Annex IV is difficult to provide. There may be confidentiality and IP concerns when sharing documentation with notified bodies. For instance, providing a detailed description of ‘the methods and steps performed for the development of the AI system’ and of ‘the design specifications of the system, namely the general logic of the AI system and of the algorithms’ (Annex IV, 2(a) and (b)) would likely entail disclosing confidential information (precise methods and design choices are arguably trade secrets). It is also important to define “general logic”; there are four elements listed here, but it is unclear whether this is the definition. This should be clarified.

- According to Annex IV 2. (b), as a technical documentation referred to in Article 11(1), a detailed description of the element of AI systems should include "the decisions about any possible trade-off made regarding the technical solutions.”

However, based on the fact that optimization, verification and trade-offs are often decided in consultation with users, it would be necessary to clearly specify that the detailed description should be limited to information that has been discussed with users.

Record-keeping

- The logging requirement (art.12) is onerous, may conflict with data protection rules, and requires significant storage. On data protection specifically, the logged information may contain data which is legislated under GDPR. Therefore, how these logging requirements relate to other legislation, and what kind of responsibilities and divisions should be decided by contract, should be explained.
- In this light, we would like the European Commission and EAIB to define practical standards and common specifications for record keeping, considering the actual practices in each sector, under art.12(2). For example, in ensuring traceability of high-risk AI, it is important to seek technological measures which enable detection of key input data that leads to certain outcomes (in case required).
- Under art. 12(3), it is necessary to define which data should be collected and stored within a range that can be assumed and verified by a provider in advance; it is not possible to log for all unexpected events. More specifically, it is also important to clarify the definition of "substantial modification"; the definition mentions “a change to the AI system following its placing on the market or putting into service which affects the compliance of the AI system with the requirements set out in Title III, Chapter 2 of this Regulation”. However, Title III, Chapter 2 of this Regulation includes article 9(risk management system), 10 (data and data governance), 11 (technical documentation), 12 (record-keeping), 13 (Transparency and provision of information to users), 14 (human oversight) and 15 (accuracy, robustness and cybersecurity). If the change is not directly affecting AI function but changes the collecting logs or human oversight, is this classified as a substantial modification?

Transparency and provision of information to users

- Some of the requirements envisaged in art.13 are unclear. It would be welcome if guidelines were given to providers so that there is more clarity on how to comply with the various obligations under this article. For instance, art.13(3)(b)(ii)/(iii) should be altered to account for the fact that predictable ranges vary per each company regarding 'which can be expected, and any known and foreseeable circumstances'. As such, it should be only necessary to explain to the user the range of assumptions per each company.
- Regarding art.13(3)(b)(v) requirements for the provider of the high-risk AI system to supply information on ‘the specifications for the input data’: it is unclear what this means. Also, art.13(3)(e) requires the provider to give information about the

expected lifetime of the AI system, which is difficult to estimate. These items should be explained fully.

Human oversight

- We would like the European Commission and EAIB to mandate the development standards and common specification by the European Standardisation Organizations in a practical manner by ensuring the appropriate level of human oversight, considering the pros and cons of human oversight and machine control respectively. For example, AI-controlled machines have lower accident rates compared to full human oversight. In addition, if the human is 'out of the control loop', it is extremely difficult to meet the oversight requirement. In cases such as these, it would be beneficial if the requirement on human oversight could be mitigated or exempted (e.g. if the product design incorporates independent safety measures for AI risk prevention).
- JBCE is concerned that human supervision or instruction could hinder output in certain circumstances. Therefore, we would favour some flexibility to allow blocking intervention by a human supervisor if the intervention is likely to lead to misuse.
- Regarding Art.14(4)(b) on automation bias, there is a requirement to "remain aware of the possible tendency". This is important for both providers and users, but non-specific obligations are difficult in practice and as such should be clarified (e.g. providing technical documentation, regularly delivering webinars to users, etc.).
- In the case of RBI classified as high-risk in Annex III, the user may take no action/decision on the basis of an identification done through RBI, unless this has been verified and confirmed by at least two natural persons (art.14(5)). This may be difficult to apply in practice.

Accuracy, robustness and cybersecurity

- When it comes to designing AI for accuracy, robustness and cybersecurity throughout the lifecycle, it is difficult to cover how people and other systems interact with the target AI system. Further, the capacity to manage this per each provider will vary. As such, we feel that the appropriate level for each of the desired outcomes should be clarified, giving a range that can be used to guide companies.
- More specifically, Art.15(3) states that 'high-risk AI systems that continue to learn after being placed on the market or put into service shall be developed in such a way to ensure that possibly biased outputs due to outputs used as an input for future operations ("feedback loops") are duly addressed with appropriate mitigation measures.' Implementing 'mitigation measures' to prevent feedback

loops would be difficult, as this would require cooperation and agreement between provider and user. Additionally, this obligation would result in sizeable costs for providers and would create barriers to entering the market – which in turn would inhibit innovation. We therefore suggest that art.15(3) should be phrased in such a way that the provider is obliged to take mitigation measures to reasonably address feedback loops but is not obliged to ensure that that feedback loops do not occur.

- Under art.15(4), it should be noted that "adversarial examples" (or attacks) are not a realistic threat or issue for some AI systems operating in the physical world. We understand from preceding text that this will be taken into account on a case-by-case basis; however, it would be beneficial to clarify that this requirement is applicable in particular to AI systems operating in cyberspace.

4. Obligations of providers and users of high-risk AI systems and other parties

- The proposed Regulation imposes different obligations on providers and users of AI systems, but in practice it is not always clear who the provider and the user are. For instance, who is the provider if company A provides AI services and company B adapts these services for deployment? Who is the provider if company A is a platform provider and company B uses company A's AI technology to deploy a tool? What if company A helps company B deploy the tool? What if the two companies go into business together and co-brand the tool? It should be noted that if company A buys a general-purpose AI system which is not considered high-risk under the Regulation from company B and then further develops it into a high-risk AI system, company B may not wish to share with company A all the information which company A would need in order to put together all the technical documentation that providers must draw up according to art.11 and Annex IV, as some of this information would constitute trade secrets. A practical consequence of the obligations in the proposal could be that company A would try to produce all components of its high-risk AI system in-house; however, this would mean that small companies would have difficulties producing high-risk AI systems. We would therefore welcome clarification on providers and users to ensure legal certainty across different contexts.

- Manufacturers of products which incorporate AI systems as safety components, and which are subject to NLF product legislation (Annex II-Section A), must ensure the compliance of the AI systems in question (art.24). In situations where a particular product incorporates AI systems developed by third parties, the compliance obligation for manufacturers could be onerous, especially in terms of documentation and logging systems. Once again, the third parties which have contributed the AI systems may not wish to share information which constitutes trade secrets.

- More specifically, regarding Art.16(a) & 17(f), as a prerequisite for the requirements on data management, a clear concept of ownership of data and

accountability between each operator and other third parties in the AI value chain should be clarified, taking the opinion of in the EAIB and the upcoming Data Act into account.

- When considering obligations set out across Chapter 3 (art.16-29), it is crucial that the specific scope of each economic operator's responsibilities (notably in between provider and users) is clearly identified in the forthcoming discussions in the EAIB. We would like the balance of liability between all market participants to be properly considered.
- Art. 29 states that the user will guarantee, and monitor, that the input data is appropriate, but we believe that it is necessary to clarify the procedures to ensure that the criteria, risks, and scope of responsibility for determining "appropriate" are properly shared and agreed upon by the parties concerned.

Standards, conformity assessment, certificates, registration

- Art.19 compels conformity assessments for high-risk AI systems. We believe the European Commission should provide an online scheme which enables interested providers to consult compliance and conformity assessment obligations with the approved authorities prior to placing AI onto the Single Market (e.g. through an online certification scheme). This should reduce barriers for market access and enhance harmonization.
- Art.43(4) provides for a new conformity assessment procedure if an AI system is substantially modified after being placed on the market. The definition of the term 'substantial modification' provided in art.3(23) should be further clarified, because we believe that as a precondition for the establishment of provisions on sanctions, the clarification of cases in which sanctions are imposed, the foreseeability of whether the requirements will be violated, and the possibility of avoiding violations of the requirements, must be ensured.

5. Transparency obligations for certain AI systems

- The transparency obligation in art.52(1) - which states that providers must notify natural persons when interacting with an AI system unless it is obvious from the circumstances and the context of use - should be further fleshed out. For example, it would be helpful if the preamble to the Regulation offered some examples of AI systems that fall under this provision, other than chatbots. Further, we would welcome guidance on how companies should notify natural persons that they are interacting with an AI system. For instance, should there be a banner on the website, or would a pop-up notification suffice?
- We would welcome clarification on whether the transparency obligation in art.52(3) to label deepfakes would apply to computer generated imagery (CGI) in the context of video games. If it does, companies would require guidance as to how

to notify natural persons that an agent appearing in a video game or a player active on a gaming platform are deepfakes.

6. Measures in support of innovation

- The AI regulatory sandbox in Article 53 requires submission of annual reports on the development, testing, and verification of AI systems by the competent authorities. It is important that this does not lead to leakage of corporate secrets or loss of market opportunities due to the passage of approval time.
- Title V of the proposal introduces innovative and flexible regulatory approaches, such as regulatory sandboxes, to encourage and stimulate AI innovation. We are concerned by the adoption of sandboxes and their implementation as described in the Regulation. We would rather encourage the adoption of 'auditable data' processes in the testing and training phases of an AI system. During testing and training, high quality data is vital, and so the EU should sponsor data programmes to encourage citizens to share their data ('data altruism') in a secure, effective, and eventually beneficial way.

7. Governance

- The role of the European AI Board will be crucial for governance. We welcome the creation of such a body in order to guarantee harmonised implementation of the AI Act, and interpretation of its definitions. We recommend this body produces guidelines to be adopted by national Competent Authorities (e.g. for the interpretation of some grey area-definitions, such as 'significant risk', 'significant changes', or 'adequate level of protection' (Art 83)). Given the Board's competence includes issuing opinions on harmonised standards and definitions of technical specifications, it is fundamental that it engages with both European and global standardisation organisations to ensure that global approaches to standardisation avoid regulatory divergence. It is also important for AI stakeholders (trade associations, companies, public authorities) to have access to the work of the AI Board in order to provide inputs on improving implementation of the Regulation.
- According to art.57, the European AI Board will be composed of national supervisory authorities and the EDPS. However, we believe that the Board should also include AI ethics experts and industry representatives amongst its members. This would be particularly important in terms of ensuring that the Board can effectively help the Commission and national supervisory authorities to provide guidance on emerging technology issues, as provided in art.57. In the particular case of members of the Board who represent industry, membership should be reviewed periodically to ensure it reflects AI technological developments in the various industry sectors (including verticals). In addition, we strongly recommend the Commission includes views from Japanese industries in the forthcoming discussions on requirements and common spec. at the EAIB.

- Regarding art. 56-59, it is important that national authorities and notified bodies have adequate knowledge and expertise to conduct efficient and rational investigations and conformity assessments.
- Art.59 should provide more guidance on which type of authority each Member State should designate/establish as the competent authority to ensure the application and implementation of the Regulation. In the absence of such guidance, Member States will likely assign as competent a variety of different national authorities, ranging from new authorities set up specifically for the purposes of the AI Regulation, to DPAs and telecoms regulators. It would be desirable to avoid fragmentation across Member States on this point, to ensure companies have clarity on who their interlocutor in each Member State will be as far as the AI Regulation is concerned.
- Under art. 60(5), any businesses' confidential documentation obtained by the national public authorities or bodies should be treated in compliance with the confidentiality obligations set out in Article 70. We underline that this principle must be properly ensured by all national authorities and notified bodies. It is also essential that these entities offer adequate security for corporate secrets provided by businesses.

8. Enforcement

- Art.64(2) provides that, when assessing the conformity of AI systems with the rules on high-risk systems, market surveillance authorities shall be granted access to the source code of the AI system. We suggest that this provision should be deleted, both because it would endanger the confidentiality of trade secrets and because it would contradict existing trade agreements (including the EU-Japan EPA) which ban disclosure requests for source code.
- We appreciate the promotion of Codes of Conduct in the AI Regulation. Codes of Conduct should be driven by industry and experts working on AI systems and solutions. Codes of Conduct should also take a global perspective in order to avoid fragmentation.

9. Confidentiality and Penalties

- Art.70 allows the Commission and Member States to exchange confidential information with third country regulators who have entered into bilateral or multilateral confidentiality arrangements that guarantee a sufficient level of confidentiality, if necessary. We believe it is important that this should not inhibit companies from entering the market.
- The upper limits of fines for companies which do not comply with the Regulation (envisaged in art.71) are extremely high (reaching up to 6% of a company's total worldwide annual turnover). We question why these upper limits are so much higher than those envisaged in the GDPR (4% of the company's total worldwide

annual turnover). It is also worth pointing out that, in the particular case of high-risk AI systems, providers and product manufacturers will need to comply with the highly complex and at times vague obligations enshrined in articles 8-15, and thus there will certainly be situations where companies acting in good faith would breach some of those provisions unintentionally. Both these considerations point towards the need for more revised upper limits for fines.

- Art.71 should clarify that if a particular incident triggers penalties under both the AI Regulation and the GDPR, only one fine should be imposed. An example of an incident which could trigger double fines would be a provider of an AI system who breaches both art.10(5) of the AI Regulation and art.9(1) of the GDPR in a situation where the provider fails to put in place the appropriate safeguards while processing a special category of personal data in order to ensure that any bias included in the AI system is monitored, detected and corrected. As a reminder, art.9(1) of the GDPR states that the processing of special categories of personal data (data which reveals racial/ethnic origin, genetic data, data on sexual orientation etc.) is prohibited, while art.10(5) of the AI Regulation states that the provider of a high-risk AI system may process such special categories of personal data in order to address bias.

About JBCE

Founded in 1999, the Japan Business Council in Europe (JBCE) is a leading European organization representing the interests of about 90 multinational companies of Japanese parentage active in Europe. Our members operate across a wide range of sectors, including information and communication technology, electronics, chemicals, automotive, machinery, wholesale trade, precision instruments, pharmaceutical, textiles and glass products.

For more information: https://www.jbce.org/ / E-mail: info@jbce.org / EU Transparency Register: 68368571120-55