Opinions on the Proposed European Artificial Intelligence Act

August 6, 2021
AI Utilization Strategy Taskforce
Committee on Digital Economy
Keidanren (Japan Business Federation)

1. General Points

- ✓ The Proposal for an Artificial Intelligence (AI) Act[1] recently published by the European Commission aims to encourage the development and implementation of trusted AI as a way of resolving environmental and social issues. In this, it shares the same general aims as the Keidanren's Trusted Quality AI Ecosystem.
- ✓ At the present stage, however, some ambiguities and room for interpretation remain with regard to the definitions of prohibited and high-risk AI and other terms, and there is a risk that this will hinder the appetite for investment in Europe and the fostering and strengthening of new AI companies, possibly having a negative impact on innovation and national security. Before the Act is passed into law, terms should be clarified and explanations added, along with guidelines and other provisions.
- ✓ Also, given the rapidly increasing speed of technological innovation and social implementation in the AI field, moving discussions forward without regular consideration of the latest conditions may cause confusion. In determining the concrete specifics of the applicability and content of the regulations, an adequate process should be established for dialogue that includes representatives of industries from outside the EU that will be affected by the regulations at forums including the EAIB (European Artificial Intelligence Board) and international standardization bodies (ISO/IEC JTC1 SC42).
- ✓ At the same time, there is a need to establish a transparent framework to review the content of the regulations in an ongoing and flexible manner by continuing close

[1] 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 (published on April 21, 2021)

dialogue even after the regulations have been introduced. In introducing new laws and regulations, these restrictions should be kept to the necessary minimum, in order to maximize the benefits to society accruing from the use and implementation of cutting-edge technology.

- ✓ The imposition of strict regulations on AI providers alone has the potential to obstruct the formation of a trusted AI ecosystem—the opposite effect to that intended. To ensure the appropriate use of AI, rather than placing all the responsibility on AI providers alone, we hope the regulations will make clear the need for efforts across the entire AI ecosystem, and that steps will be taken to encourage users to make efforts to this end as well.

2. Individual points

- Article 2 Scope

(Excerpt from p.39)

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 Union;

(Opinion)

- ✓ There should be clarification of the obligations imposed on providers and users of AI systems where only the output generated by an AI system is used in the EU (for example, video content created by a company outside the EU using an AI system), rather than the provision of the AI system itself.

- Article 3 Definitions

(Excerpt from p.40)

(13)‘reasonably foreseeable misuse’ means the use of an AI system in a way that is not in accordance with its intended purpose, but which may result from reasonably foreseeable human behaviour or interaction with other systems;

(Opinion)

- ✓ Assuming the provider has taken steps to implement appropriate security measures, there should be an exemption in the case of malicious attacks from users or systems.

(Excerpt from p.40)

(14)‘safety component of a product or system’ means a component of a product or of a system which fulfils a safety function for that product or system or the failure or malfunctioning of which endangers the health and safety of persons or property;

(Opinion)

- ✓ The definition of “safety component” should be made clearer and concrete examples provided within each field of technology. For example, it should be made clear to what extent these provisions would apply to AI camera home monitoring systems, such as fire detectors, baby monitors, and security systems.
- ✓ There should be clarification of who is responsible for deciding whether a device constitutes a “safety component.” If the provider is to be responsible for this decision, steps should be taken to provide the necessary information and other support, including the designation of a specialist body that providers can approach for advice with difficult cases.

(Excerpt from p.42)

(36)‘remote biometric identification system’ means an AI system for the purpose of identifying natural persons at a distance through the comparison of a person’s biometric data with the biometric data contained in a reference database, and without prior knowledge of the user of the AI system whether the person will be present and can be identified ;

(Opinion)

- ✓ There should be clarification of the criteria of the terms “at a distance” and “prior knowledge of the user” as well as of a definition of the user.
- ✓ It should be made clear that a system that temporarily detects and categorizes facial

or physical characteristics but does not identify an individual (for example, an AI system that ascertains overall customer flow within a store without focusing on individuals, for use in marketing purposes by a private company) does not count as a "remote biometric identification system" and does not constitute high-risk AI.

- Article 5 The following artificial intelligence practices shall be prohibited
  Article 6 Classification rules for high-risk AI systems
  (Entire text)

  (Opinion)
  - ✓ A risk-based approach that uses excessively broad definitions of prohibited and high-risk AI runs the risk of inhibiting innovation within the EU. Accordingly, the scope of applicability should be made more limited, and the scope of the regulations made clearer, along with the methods for measuring and assessing risk. The applicability of the regulations could be determined based on individual use cases and their associated levels of risk.
  - ✓ One category of prohibited AI is AI that is used to produce subliminal effects. The definition should be limited to AI that makes deliberate use of subliminal techniques. AI systems in which subliminal effects may be produced unintentionally, such as audiovisual contents, gaming, and commercial messaging for marketing, should not be covered by the regulations.
  - ✓ One prohibited example of AI involves the use of a "real-time" remote biometric identification system for the purpose of law enforcement. It should be made clear whether this includes cases in which law enforcement agencies use such a system for security within their own premises, or cases in which a private company sends a report to law enforcement agencies after its AI system detects signs of suspicious activity. The scope of the term "publicly accessible spaces" should be clarified with specific examples, taking into account the risks involved in individual use

cases.

- ✓ Consideration should be given to the cost effectiveness of the responsibilities placed on high-risk AI stakeholders. For example, the introduction and operation of the provisions laid down in Chapter 2 (including risk management systems, data governance, and documentation and record keeping), Chapter 3 (including quality management systems), and Chapter 5 (including conformity assessment) are likely to have a significant impact on stakeholders, as indicated in the impact assessment (SWD (2021) 84 final). There is therefore a need for more detailed discussions on these sections in the future.

- Article 6 Classification rules for high-risk AI systems

  (Excerpt from p.45)

  1. (preceding text omitted)

  (a) the AI system is intended to be used as a safety component of a product, or is itself a product, covered by the Union harmonisation legislation listed in Annex II;

  (b) the product whose safety component is the AI system, or the AI system itself as a product, is required to undergo a third-party conformity assessment with a view to the placing on the market or putting into service of that product pursuant to the Union harmonisation legislation listed in Annex II.

  (Opinion)

  - ✓ In diagnostic AI that supports the maintenance and upkeep of a "safety component," the output of the AI is not used in a compulsory manner, but decisions are made by a human operator using output information produced by the AI. It should therefore be possible to reduce the risk posed by the AI. Consequently, classification rules (a) and (b) should be eased, either in whole or in part.

- Article 7 Amendments to Annex III

  (Excerpt from p.45)

1.The Commission is empowered to adopt delegated acts in accordance with Article 73 to update the list in Annex III by adding high-risk AI systems where both of the following conditions are fulfilled: (following text omitted)

2.(h) the extent to which existing Union legislation provides for:

(i) effective measures of redress in relation to the risks posed by an AI system, with the exclusion of claims for damages;

(ii) effective measures to prevent or substantially minimise those risks.

(Opinion)

- ✓ Article 7 (2) (h) states that the Commission will take into account the scope of existing EU legislation when considering delegated acts to update the list in Annex III. In this case, opportunities should be provided to canvass a wide range of opinions from industry representatives, to avoid introducing excessive regulations that do not match the actual circumstances.
- ✓ The addition of excessive regulations should be avoided in fields where sufficient third-party certification systems are already in place under existing regulations and systems, such as regulations for medical devices.

- Article 9 Risk management system

(Excerpt from pp. 46-47)

2. The risk management system shall consist of a continuous iterative process run throughout the entire lifecycle of a high-risk AI system, requiring regular systematic updating. It shall comprise the following steps:

(a) identification and analysis of the known and foreseeable risks associated with each high-risk AI system;

(b) 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; (text omitted)

(Opinion)

- ✓ This section refers to analysis and evaluation of known and foreseeable risks: the specific scope of these terms and the measures required should be clarified, along with concrete examples.
- ✓ Provided that an AI provider issues a precautionary warning to prevent misuse or malicious use of the AI, bearing in mind the possibility that AI models may change after being placed on the market, AI users should be held responsible for problems arising from malicious use or misuse within the scope covered by the provider's precautionary warning.

(Excerpt from p.47)

4. …In identifying the most appropriate risk management measures, the following shall be ensured:

(a) elimination or reduction of risks as far as possible through adequate design and development; (text omitted)

(c) provision of adequate information pursuant to Article 13, in particular as regards the risks referred to in paragraph 2, point (b) of this Article, and, where appropriate, training to users.

(Opinion)

- ✓ It should be made clear how much information providers need to maintain and share with users in order to provide information conducive to the appropriate use of high-risk AI and information relating to analysis and evaluation of risks.
- ✓ The requirement for "elimination or reduction of risks as far as possible through adequate design and development" should be clarified, and guidelines should be provided that also consider risk trade-offs.

- ➢ Article 10 Data and data governance

（Entire text）

(Opinion)

- ✓ Guidelines consistent with the GDPR should be provided as soon as possible regarding the use of remote biometric identification and high-risk AI for which the pseudonymization and encryption requirements of the GDPR may apply.
- ✓ It would be desirable to consider the use of infrastructure technology[2] for global data free flow, in order to allow smooth analysis and transfer of data across borders, while complying strictly with the data protection laws of individual countries and regions.

(excerpt from p.48)

2. Training, validation and testing data sets shall be subject to appropriate data governance and management practices. Those practices shall concern in particular, (text omitted)

(d) the formulation of relevant assumptions, notably with respect to the information that the data are supposed to measure and represent; (text omitted)

3. Training, validation and testing data sets shall be relevant, representative, free of errors and complete. (Text omitted)

(Opinion)

- ✓ Clarification should be given on the intended meaning of the terms “formulation of assumptions” and “free of errors and complete.” The obligations should be made realistic and verifiable.

(Excerpt from p.48)

4 Training, validation and testing data sets shall take into account, to the extent required by the intended purpose, the characteristics or elements that are particular to the specific

[2] Platform technology that automatically configures and executes programs at data collection sites that perform the necessary processing for data transfer, such as masking of highly confidential and sensitive data as stipulated by the GDPR and other data protection laws, and automatically transfers data to data analysis sites.

geographical, behavioural or functional setting within which the high-risk AI system is intended to be used.

(Opinion)

- ✓ Taking geographic elements into account as requirements for data sets should be avoided, as this would make it difficult to learn from globally uniform data, and because the act of evaluating individual characteristics and elements in itself risks creating bias.

- Article 11 Technical documentation

(Excerpt from p.49)

1. …The technical documentation shall be drawn up in such a way to demonstrate that the high-risk AI system complies with the requirements set out in this Chapter and provide national competent authorities and notified bodies with all the necessary information to assess the compliance of the AI system with those requirements. (Text omitted)

(Opinion)

- ✓ This section requires companies to "provide national competent authorities and notified bodies with all the necessary information to assess the compliance of the AI system with those requirements." However, from the viewpoint of maintaining confidentiality, thorough-going discussions on this point should be held with multi-stakeholders including industry representatives.

- Article 12 Record-keeping

（Entire text）

(Opinion)

- ✓ Guidelines should be published explaining what laws and regulations should be considered in drawing up contracts, and what division of responsibilities should be

decided in contracts. This should include validating contract processes that are in line with relevant existing legislation.

(Excerpt from p.49)

2. The logging capabilities shall ensure a level of traceability of the AI system's functioning throughout its lifecycle that is appropriate to the intended purpose of the system.

3. In particular, logging capabilities shall enable the monitoring of the operation of the high-risk AI system with respect to the occurrence of situations that may result in the AI system presenting a risk within the meaning of Article 65(1) or lead to a substantial modification, and facilitate the post-market monitoring referred to in Article 61.

(Opinion)

- ✓ The definition of "substantial modification" should be clarified.
- ✓ Logging requirements should be restricted to a scope that can be envisaged and verified in advance.
- ✓ In requiring providers to maintain log data and to carry out monitoring based on data after being placed on the market, from the perspective of protecting personal information and business confidentiality, it would be preferable to avoid requiring providers to store more data than is absolutely necessary.

- ➢ Article 13 Transparency and provision of information to users

(Excerpt from p.50)

1. High-risk AI systems shall be designed and developed in such a way to ensure that their operation is sufficiently transparent to enable users to interpret the system's output and use it appropriately. (Text omitted)

(Opinion)

- ✓ Regarding the requirement to ensure transparency and provide information to users, guidelines should be provided with practicable and concrete examples, including

whether XAI[3] is assumed.

(Excerpt from p.50)

3. The information referred to in paragraph 2 shall specify: (text omitted)

(b) the characteristics, capabilities and limitations of performance of the high-risk AI system, including:

(i) its intended purpose;

(ii) the level of accuracy, robustness and cybersecurity referred to in Article 15 against which the high-risk AI system has been tested and validated and which can be expected, and any known and foreseeable circumstances that may have an impact on that expected level of accuracy, robustness and cybersecurity;

(iii) any known or foreseeable circumstance, related to the use of the high-risk AI system in accordance with its intended purpose or under conditions of reasonably foreseeable misuse, which may lead to risks to the health and safety or fundamental rights;

(Opinion)

- ✓ Since it is difficult to list all the factors including external factors that may apply, it should be made clear that "limitations" refers to those limitations that lie within the scope considered by the provider.
- ✓ Since the scope of what can be foreseen will vary from company to company, the wording "can be expected, and any known and foreseeable circumstances" and "any known and foreseeable circumstances" should be amended to require a provider to provide users with explanations within the scope foreseen by the provider.

- Article 14 Human oversight

[3] XAI (explainable artificial intelligence) refers to AI in which the processes leading to the results of predictions or estimates can be explained by a human.

(Excerpt from p.51)

1. High-risk AI systems shall be designed and developed in such a way, including with appropriate human-machine interface tools, that they can be effectively overseen by natural persons during the period in which the AI system is in use. (Text omitted)

(Opinion)

- ✓ In considering specific oversight requirements within each field, steps should be taken to ensure that these are practical for companies, taking into consideration the following three points. (1) Proper consideration should be given to the level of human involvement required, taking into consideration the respective advantages and disadvantages of oversight by human beings and by AI. (2) This requirement should be omitted or relaxed in cases where steps to eliminate risk have been incorporated at the design stage of the system including AI through an independent safety structure, even if the level of human involvement is low. (3) This requirement should be omitted or relaxed in cases where it has been demonstrated that the AI is free from bias or more accurate compared with a verification of operations by a human operator.

(Excerpt from p.51)

4. The measures referred to in paragraph 3 shall enable the individuals to whom human oversight is assigned to do the following, as appropriate to the circumstances: (text omitted)

(b) remain aware of the possible tendency of automatically relying or over-relying on the output produced by a high-risk AI system ('automation bias'), in particular for high-risk AI systems used to provide information or recommendations for decisions to be taken by natural persons;

(Opinion)

- ✓ A clearer explanation should be given of the content of requirements with regard to the obligation to "remain aware of the possible tendency" of "automation bias."

- Article 15 Accuracy, robustness and cybersecurity

  (Excerpt from pp.51-52)

  1. High-risk AI systems shall be designed and developed in such a way that they achieve, in the light of their intended purpose, an appropriate level of accuracy, robustness and cybersecurity, and perform consistently in those respects throughout their lifecycle. (Text omitted)

  (Opinion)

  - ✓ The scope intended by the phrase "appropriate level" is unclear. Since the ability of companies to foresee these factors will vary, this should be amended to apply only within the scope that a company can foresee.

  (Excerpt from p.52)

  3.…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.

  (Opinion)

  - ✓ Responding to this requirement to implement "mitigation measures" in AI systems that continue to learn would only be possible by signing contracts with a wide range of companies throughout the supply chain as contracting parties, and further multi-stakeholder discussion is needed on this point.

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

  (Excerpt from p.52)

  Providers of high-risk AI systems shall:

  1. (a) ensure that their high-risk AI systems are compliant with the requirements set out in Chapter 2 of this Title;

(Opinion)

- ✓ Providers should be able to obtain an exemption from this requirement on the condition that they fulfill a certain level of due diligence on risk-verification. For example, in a case where a user alters a product or service supplied by the provider in order to allow a method of use deemed to be prohibited AI, the provider should be released from responsibility if this is done by a user without the involvement of the provider.
- ✓ In Clause (34) on p. 26, with regard to "AI systems intended to be used as safety components in the management and operation of road traffic and the supply of water, gas, heating and electricity," the risk of system malfunction is generally reduced through multiplexing and redundancy. In cases where such measures are in place, they should be included as factors to be considered when imposing obligations on high-risk AI.

- ➢ Article 19 Conformity assessment

(Excerpt from p.54)

1. Providers of high-risk AI systems shall ensure that their systems undergo the relevant conformity assessment procedure in accordance with Article 43, prior to their placing on the market or putting into service. (Text omitted)

(Opinion)

- ✓ To ensure that conformity assessment does not become a barrier to market participation for companies from outside the EU, a framework should be put in place as soon as possible to allow companies from outside the bloc to get advice in advance from the authorities on the Artificial Intelligence Act and related regulations and to obtain public certification.

- ➢ Article 24 Obligations of product manufacturers

(Excerpt from p.55)

1. Where a high-risk AI system related to products to which the legal acts listed in Annex II, section A, apply, is placed on the market or put into service together with the product manufactured in accordance with those legal acts and under the name of the product manufacturer, the manufacturer of the product shall take the responsibility of the compliance of the AI system with this Regulation and, as far as the AI system is concerned, have the same obligations imposed by the present Regulation on the provider. (Opinion)

- ✓ In light of the content of the GDPR and other existing laws and regulations, consideration should be given to the division of responsibilities between users and providers/manufacturers, taking into account the balance between innovation and regulation.

- Article 29 Obligations of users of high-risk AI systems

  (Excerpt from p.58)

  1. Users of high-risk AI systems shall use such systems in accordance with the instructions of use accompanying the systems, pursuant to paragraphs 2 and 5.

  (Opinion)

  - ✓ Since it is difficult for providers to shoulder all the responsibility for malicious use, the regulations should contain a clearly stated prohibition on using a system except for the intended use.

- Article 43 Conformity assessment

  (Excerpt from p.65)

  4. High-risk AI systems shall undergo a new conformity assessment procedure whenever they are substantially modified, regardless of whether the modified system is intended to be further distributed or continues to be used by the current user. (Text omitted)

  (Opinion)

  - ✓ Because AI systems are improved in an agile manner through software updates and

learning, the requirement to carry out regular conformity assessments would place an excessive burden on the entity carrying out the assessments, and should therefore be avoided.

- ✓ In Article 3, Definitions (23), the term "substantial modification," cited as a condition requiring a new conformity assessment, should be more clearly defined.

Article 52 Transparency obligations for certain AI systems

(Excerpt from p.69)

1. Providers shall ensure that AI systems intended to interact with natural persons are designed and developed in such a way that natural persons are informed that they are interacting with an AI system, unless this is obvious from the circumstances and the context of use.

(Opinion)

- ✓ The scope and requirements of "AI systems intended to interact with natural persons" should be clarified.

(Excerpt from p. 69)

3. Users of an AI system that generates or manipulates image, audio or video content that appreciably resembles existing persons, objects, places or other entities or events and would falsely appear to a person to be authentic or truthful ('deep fake'), shall disclose that the content has been artificially generated or manipulated. (Text omitted)

(Opinion)

- ✓ This section requires an AI system that generates or manipulates image, audio, or video content to disclose that the content has been artificially generated or manipulated, but there should be clarification about the methods by which this disclosure is to be made. Similarly, if CGI (Computer Generated Imagery) is to be covered by this provision, there needs to be a clarification of the method of disclosure.

- Article 57 Structure of the Board

(Excerpt from p.72)

4. The Board may invite external experts and observers to attend its meetings and may hold exchanges with interested third parties to inform its activities to an appropriate extent. To that end the Commission may facilitate exchanges between the Board and other Union bodies, offices, agencies and advisory groups.

(Opinion)

- ✓ Multi-stakeholders including industry representatives and AI specialists should be involved on an ongoing basis in the European Artificial Intelligence Board as committee members and should participate in its discussions and deliberations. Further, the composition and size of the committee board should be continually reviewed in response to the development and progress of the technology.

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

(Excerpt from p.74)

3. Information contained in the EU database shall be accessible to the public.

(Opinion)

- ✓ The purposes of public disclosure should be limited to the purpose of "assisting providers and others in making a decision as to whether a system constitutes high-risk AI." A database and collection of examples should be compiled of cases deemed to represent high-risk AI and cases that are not, and these should be used to guarantee the transparency of decisions on applicability of the regulations. Further, a framework should be put in place to make decisions in response to queries from providers as to whether a given system or application is deemed to constitute high-risk AI, and the results of these decisions should be regularly added to the database and made publicly available.

- Article 61 Post-market monitoring by providers and post-market monitoring plan for high-risk AI systems

  (Excerpt from pp.74-75)

  1.Providers shall establish and document a post-market monitoring system in a manner that is proportionate to the nature of the artificial intelligence technologies and the risks of the high-risk AI system.

  (Opinion)

  - ✓ In carrying out post-market monitoring based on a template for the monitoring plan, room should be left for providers to obtain log data through contracts with users.

- Article 64 Access to data and documentation

  (Excerpt from p.77)

  1. Access to data and documentation in the context of their activities, the market surveillance authorities shall be granted full access to the training, validation and testing datasets used by the provider, including through application programming interfaces ('API') or other appropriate technical means and tools enabling remote access.

  2. Where necessary to assess the conformity of the high-risk AI system with the requirements set out in Title III, Chapter 2 and upon a reasoned request, the market surveillance authorities shall be granted access to the source code of the AI system.

  (Opinion)

  - ✓ For providers, source code is a vital resource that is the source of their competitiveness as a company, and in some cases providers may not be able to disclose the source code for contractual reasons or reasons of security. There is also a risk that user concerns about the possibility that their data might be disclosed to authorities will hinder the introduction of AI, and access to data by authorities should therefore be avoided. If suspicions arise that make an investigation necessary, consideration should be given to appropriate ways of addressing the situation without relying on disclosure of source code, such as requiring companies to be

accountable for providing an explanation in the first instance.

- ✓ Article 73 of the Japan-EU EPA clearly prohibits demands for access to source code between Japan and the EU, and consistency with this article should be made clear.

- Article 69 Codes of conduct

  (Excerpt from p.80)

  1. The Commission and the Member States shall encourage and facilitate the drawing up of codes of conduct intended to foster the voluntary application to AI systems (text omitted)

  (Opinion)

  - ✓ Consideration should be given to awarding incentives to companies that draw up appropriate codes of conduct.

- Article 71 Penalties

  (Excerpt from p.82)

  6. When deciding on the amount of the administrative fine in each individual case, all relevant circumstances of the specific situation shall be taken into account and due regard shall be given to the following: (text omitted)

  (Opinion)

  - ✓ If the scope of penalties is too wide and the size of fines too large, there is a risk of excessively restricting the activities of companies in the European market. Appropriate penalties should therefore be put in place, taking into account the nature and content of the offense, the extent of the benefit gained as a result, and the presence or otherwise of malicious intent.
  - ✓ Materials kept by the authorities regarding legislation based on this Act should kept for a period sufficiently longer than the period for which companies keep logs and similar materials, since these materials may play an important role as evidence in cases where the litigation period becomes prolonged.

- Article 73 Exercise of the delegation

  (Entire text)

  Article 7 Amendments to Annex III

  (Excerpt from p.45)

  1. The Commission is empowered to adopt delegated acts in accordance with Article 73 to update the list in Annex III by adding high-risk AI systems where both of the following conditions are fulfilled:

  (Opinion)

  - ✓ Considering the impact on business, when the Commission is considering updating the list in the Annex, it should listen to the opinions of multi-stakeholders, including industry representatives and AI specialists, and should make decisions carefully and prudently, having ensured transparency of debate.

- Article 84 Evaluation and review

  (Excerpt from p.87)

  1. The Commission shall assess the need for amendment of the list in Annex III once a year following the entry into force of this Regulation.

  (Opinion)

  - ✓ In carrying out evaluations and revisions, the Commission should give due consideration to international best practices, based on discussions with multi-stakeholders including industry representatives and AI specialists.

- Annex III High－Risk AI Systems Referred to in Article 6 (2)

  (Entire text)

  (Opinion)

  - ✓ The definitions of “high-risk AI” and “safety component” should be clarified.
  - ✓ Systems should not be counted as high-risk AI where the risk of human rights

infringements is sufficiently low. In the case of biometrics and categorizations, for example, systems should not be counted as high-risk AI if it has been confirmed that there is no risk of discrimination through the identification of attributes.

- Annex IV Technical Documentation referred to in Article 11(1)

  (Excerpt from p.6)

  2. A detailed description of the elements of the AI system and of the process for its development, including:

  (a) the methods and steps performed for the development of the AI system, including, where relevant, recourse to pre-trained systems or tools provided by third parties and how these have been used, integrated or modified by the provider;

  (Opinion)

  - ✓ Since some of the methods and steps used in development may be confidential, it may be difficult to disclose all this information. This section should be amended to allow non-disclosure of content relating to the confidentiality of company secrets.

  (Excerpt from p.6)

  (b) the design specifications of the system, namely the general logic of the AI system and of the algorithms; the key design choices including the rationale and assumptions made, also with regard to persons or groups of persons on which the system is intended to be used; the main classification choices; what the system is designed to optimise for and the relevance of the different parameters; the decisions about any possible trade-off made regarding the technical solutions adopted to comply with the requirements set out in Title III, Chapter 2;

  (Opinion)

  - ✓ "General logic" should be clearly defined.
  - ✓ Detailed explanations of AI systems are required to include "decisions about trade-offs," but this should be clarified to require only the listing of trade-offs actually

considered.

- ✓ No requirement should be made to list considerations regarding verifications and settings for optimized systems and trade-offs exceeding the scope decided in discussions with users.