FUJITSU

Fujitsu Positioning Paper on Artificial intelligence – ethical and legal requirements

6th August 2021

Fujitsu is one of the world's leading global ICT companies and the largest in Japan. We have around 129,000 Fujitsu colleagues working with customers in over 180 countries. Fujitsu is committed to investing in R&D with Laboratories and Innovation Centers in Japan, Asia, Europe and the US. We use our experience and the power of ICT to shape the future of society with our customers.

Fujitsu's Vision is to enable a **Human Centric Intelligent Society** that creates value by connecting infrastructure, empowering people and creatively defining new forms of intelligence. We are transforming into a strong and reliable **Digital Transformation Company** by investing in our people and new key technologies such as AI, Blockchain and Quantum inspired solutions. Our ambition is to contribute to the benefit of all citizens and society in line with the **UN Sustainable Development Goals** by supporting customers from across the public and private sectors. Investing in AI and Data is critical to achieving this.

Europe is at the heart of our global business. We employ 20,000 people and offer a full portfolio of business-technology products, solutions and services, ranging from workplace systems to data center solutions, managed services, and cloud-based software and solutions. In 2018[1] Fujitsu signed a long-term research and co-creation program with INRIA in Paris-Saclay to develop new AI and machine learning techniques by leveraging advanced mathematics and computing. The **Fujitsu AI Center of Excellence in France** is now operational, employing a growing number of researchers and AI experts developing R&D projects (including Horizon2020) adopting a co-creation approach with our customers. Same applies for Germany having a dedicated Digital Incubation organization staffed with AI experts and Data Scientists, but also for other countries in Europe.

We value the efforts of the European Commission in creating a common approach to AI in Europe and welcome the opportunity to share our thinking on this vital topic. **Fujitsu shares the EU's commitment towards achieving Human Centric trustworthy AI**[2]. Fujitsu strongly supports the European Commission's key objective to foster the development and uptake of safe and lawful AI that respects fundamental rights across the Single Market while ensuring inclusive societal outcomes. Fujitsu, as an AI system and solutions developer and provider, is happy to discuss this further with the Commission.

Fujitsu's response to the European Commission's proposal on AI Act

Introduction

Fujitsu understands the need for European regulation of AI and encourages the European Commission to make all efforts to finalize a framework legislation that can be effective both at European and global level with a strong focus on supporting technology exchange and innovation. In order to do that, this regulation must be as simple as possible

[1] Fujitsu Press Release 2018 - here
[2] Fujitsu Group AI Commitment 2019 - here

with clear definitions and limit the obligations for all stakeholders in the value chain by focusing on essential rules and requirements.

We appreciate the efforts of the European Commission in providing the first horizontal-framework proposal for a regulation of such a complex topic with impact on many technologies and ecosystems-value chains with clear synergies with other regulations at European level.

Artificial Intelligence (AI) must be seen primarily as a great opportunity to improve our society and the life of all citizens rather than a threat. It is important to make sure that this technology does not cause harm to anyone and in particular to the most disadvantaged categories of citizens, ensuring a responsible rollout of the technology with particular focus on privacy, cybersecurity and transparency.

Fujitsu is promoting a Human-Centered development of AI solutions in full respect of human rights, ethics values and in line with the UN SDGs. In 2018 Fujitsu formulated the "Fujitsu Group AI Commitment," demonstrating dedication to Safe and Secure Use of AI. In this statement, we highlighted five main principles:

1 - Provide value to customers and society with AI

2 - Strive for Human Centric AI

3 - Strive for a sustainable society with AI

4 - Strive for AI that respects and supports people's decision making

5 - As corporate social responsibility, emphasize transparency and accountability for AI

Strong emphasis must be placed not only on respecting fundamental human rights but also on sustainability, climate change and green transition in line with the UN SDGs, the recent conclusions of the G20 and the European Commission strategies.

Fujitsu strongly believes in the importance of having a global approach toward AI. An open dialogue about this hugely important technology, allocating strong efforts on Global Standards, R&D investments, shared definitions, rules and principles, will encourage strong cooperation and trade among countries sharing the same principles and fast adoption of AI systems that goes across borders.

Attached a more detailed response to this consultation that incorporates feedbacks and suggestions from Fujitsu experts coming from Europe, Japan, US, Canada and other Countries.

1. Definition of AI (Article 3 and Annex I)

A clear definition of AI represents the basis for a correct and effective interpretation and "use" of this regulation. Fujitsu understands the intention of adopting a broad definition of AI and encourages the continuous work with international organisations such as the OECD to ensure a shared interpretation of what we mean with AI. The final aim must be legal certainty and the possibility to have the same understanding of what is an AI system worldwide. If this won't be the case, there is a risk of having very different rules in different regions.

The actual definition of AI technology in Annex I is very broad and includes any software. The definition should take into account the uniqueness of the AI system that threatens fundamental rights. The inclusion of "(c) Statistical approaches, Bayesian estimation, search and optimization methods" in the definition should be carefully considered.

2. Prohibited AI Systems (Article 5) and High-risk AI systems (Article 6-7 and ANNEX II-III)

Fujitsu supports 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. Dividing some categories as listed in ANNEX II (where sectorial legislation will keep on been applied) and ANNEX III is a good way forward.

On the other side, we encourage the European Commission and co-legislators to better define both how Article 7(2) is going to be applied to the categories listed in ANNEX III and how these categories are going to be periodically reassessed in areas such as education, law enforcement and many others that are going to be defined. 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 provide more clarity to AI providers and allowing open discussion between Institutions and AI stakeholders.

A clear definition of risk is equally important, and some additional work must be done on this point in order to provide stakeholders with a good understanding of how risk is defined. This will be critical to create better understanding on the possible update of the high-risk categories on Annex III.

Banning some AI applications such as the use of 'real-time' remote biometric identification systems in publicly accessible spaces with some exception as stated in article 5 is an approach that must be supported by a precise definition of which AI systems will be banned and which ones will be accepted in order to reduce uncertainty at minimum level.

We also encourage the European Commission to work on a related risk mitigation strategy to be shared with all stakeholders in order to provide clear guidelines. Guidelines should be prepared by involving all actors of the value chain and in particular the industry and the AI providers. This will certainly help in building trust among all stakeholders and will be of help for a correct adoption of the AI ACT.

3. Requirements for High-risk AI systems (Title III, Chapter 2)

i. General view

Fujitsu appreciates the effort of the European Commission described in Chapter 2 to provide a detailed list of requirements for high-risk AI systems. We find there is a good balance between the need of increasing transparency, the ability to explain, fairness and cybersecurity and Fujitsu's approach on AI and engagement with AI4People around the key topic of AI & Ethics. Fujitsu sees these values as key enablers of trust in AI technologies and therefore play an important role in facilitating their adoption.

On the other side, Fujitsu does believe that it is crucial to limit the obligations to what is necessarily needed and to have flexible tools to help companies in easily, effectively and quickly providing the necessary documentation. As instances where one software produced by a company as basic system and in a second phase customized for different needs of different customers but without changing the fundamental architecture and purpose would need to go through the same obligations again should be avoided. In some cases, a "one-size fits all approach" would not be

beneficial for a correct adoption of obligations by different companies working in quite different sectors. It would be then preferable to think about ways to reduce at minimum administrative tasks and to focus on providing the information needed for that sector on article 11 (Technical Documentation) and article 13 (Record Keeping).

Specific guidelines would help in the correct implementation of obligations as well as for the following points related to data governance, transparency and human oversight as it is happening with GDPR.

ii. Standards (Article 40)

Fujitsu strongly believes in the importance of global standards in order to encourage a harmonized adoption of AI systems, interoperability, technology transfer and innovation. Japan is a close partner of the EU and a lot is going on in terms of policy dialogue in the digital sector with significant impact in many applications of new emerging technologies such as AI. There are many standardisation activities taking place outside of European Standardisation Organizations (ESOs) such as ISO/IEC JTC1 SC42 and SC37 that are relevant for the purposes of the AI ACT.

We strongly encourage the European Commission to maintain a strong cooperation with these organisations and provide the necessary working in this AI ACT to allow the work made in these organisations to be reflected in the implementation of this ACT. In this regard we would suggest limiting the use of and implementation of acts by the European Commission that could create unnecessary barriers with third countries such as Japan.

In this context, the role of the European AI Board (Title VI) will be crucial. Fujitsu welcomes the creation of such a body to guarantee a harmonized implementation of the AI ACT and interpretation of its definitions. We do recommend that this body is able to produce guidelines adopted by the national competent authorities for example for the interpretation of some "grey areas-definitions" such as in wording like "significant risk" or "adequate level of protection" or "significant changes" (Art 83). Given the Board's competence to issue opinions on the use of harmonized standards and the definition of technical specifications, it is fundamental that it engages with global standardisation organisations to ensure that global approaches to standardisation remain aligned with the goal of avoiding regulatory divergence. It is also important for AI stakeholders, Trade Associations, Companies, Public Authorities to be allowed to have access to the work of the AI Board in order to provide inputs and ideas for a better implementation of the AI ACT.

iii. Data and data governance (Article 10)

Fujitsu believes that special attention must be given to data governance requirements. Data governance is key for the proper implementation of AI systems based on good quality of data for innovation. We believe that AI quality is highly dependent on training data quality which has been discussed in ISO/IEC JTC1 SC 42 and demographic bias is also discussed in ISO/IEC JTC 1 SC 37. We call on the European Parliament and the Council to amend the text based on the results of the discussions in SC 42 and SC 37. Total coherence with GDPR requirements is equally important.

Article 10 should be better designed to make it possible for companies to test their AI systems and not impose too many ex-ante obligations and restrictions in terms "free of errors, complete" dataset which is an unrealistic requirement but is subject to Article 71 penalties, it unduly increases the risk of developing, providing and using high-risk AI systems in the EU. Therefore, we request that "free of errors, complete" be deleted or modified to a more relaxed form. In addition, "appropriate statistical properties" in paragraph 3 should also be modified so that AI providers make decisions based on customer and market needs. high-risk AI systems because it is too difficult to generally define what is "appropriate". The focus should always be the final AI system that need to be compliant with the main principles adopted in the AI ACT and not the AI system in the testing or training phases. These key phases for innovative AI

systems must be secured and able to work in "safe environments" where mistakes can be made without affecting any fundamental right or principle.

iv. Transparency and provision of information to users (Article 13)

Fujitsu understands and has been strongly involved in the discussions on the importance of ensuring transparency. Interestingly, the case[3] where AI can avoid gender discrimination or creating disadvantages for women, shows that the challenge is actually in the processing and use of the data, and not the classification and identification, (such as 'men and women'). To this end, the purpose of transparency should not be to disclose all technologies and algorisms. Instead, we believe it is important to make the AI system transparent by allowing users to understand it, and third parties to verify the process of the AI systems, such as how to test the fairness of AI, and what standards are used to assess it.

This is a key principle to enhance trust with end-users both on B2C and B2B. We do believe the AI ACT should encourage a proportionate level of transparency in order to ensure the right level of information for the end users and a complete overview of the trade-off between benefits and "risks." Overloading the end user with unnecessary information that could create the opposite effect of discouraging the adoption of the AI System should be avoided.

In this sense, the disclosure of "level of cybersecurity" in Paragraph 3 (b) (ii) is not necessarily required. The existing security certification system represents "level of security management" and no method has been established to prove level of cybersecurity itself. Rather, we believe that disclosing vulnerabilities could potentially put AI systems in use in the EU at risk. Therefore, we think that "Request for disclosure of security level" should be deleted and left to the judgment between the provider and the user.

v. Human oversight (Article 14)

It is important to be flexible when we talk about "oversight by human". While it takes more than a second for a human to react, it is practically impossible for a human to intervene in all of the AI operations that proceed in milliseconds and microseconds. In addition, consideration should be given to cases where it is difficult to visualize data necessary for oversighting performance, such as voice recognition. In some cases, human oversight can lead to long and unnecessary processes that are not adding more value the AI system or compliance with the main principles of the AI ACT. In this sense, paragraph 4 (a) "fully understand the capacities and limitations of the high-risk AI system and be able to duly monitor its operation, so that signs of anomalies, dysfunctions and unexpected performance can be detected and addressed as soon as possible" should take into account the limitations of human supervision. We also request for more clarity on the definition of human oversight such as when, how, at what stage human oversight is required. This must be linked to the risk as the whole AI ACT is adopting a risk-based approach.

We understand "two natural persons" in paragraph 5 includes people from the same organization and requiring third-party intervention should be avoided due to excessive costs.

The overarching issue is the weight of obligation imposed on the provider to conform to a considerable set of provisions, coupled to substantial penalties. In many projects, the performance of a given AI solution is highly dependent on the input data and use case, which are both provided and defined by the end-user. Notably the customer

[3] MIT Tech review There's an easy way to make lending fairer for women. Trouble is, it's illegal.' https://www.technologyreview.jp/s/172585/theres-an-easy-way-to-make-lending-fairer-for-women-trouble-is-its-illegal/

retains ownership of that data which restricts what we as providers could control, in terms of assuring suitability and integrity (free of error). Further, given the investment the client makes in co-creating a given AI solution they then expect some ownership, specifically any trained model. Finally, refinement or retraining may be part of a specific MLOps solution, yet again the new data used and adjustments to historic AI predictions are completely governed by the user and their operational environment.

vi. Accuracy, robustness and cybersecurity (Article 15)

It is a requirement that is deeply related to existing standards, and we understand that the degree of design content conforms to these international standards.

The meaning of "feedback loop" in paragraph 3 is still unclear and the description regarding " feedback loop " is similar with "continuous learning" in an AI system. We request that a more detailed explanation be added by referring to the exiting definition of "continuous learning" to define the term " feedback loop". (See ISO/IEC DIS 22989(en), 3.1.10, https://www.iso.org/obp/ui/#iso:std:iso-iec:22989:dis:ed-1:v1:en) for the definition of continuous learning)

4. Requirements to AI Providers (Title III, Chapter 3)

i. General view

We understand the need for requirements to be imposed on AI operators that are defined as standards by industry. Standardization of AI, ISO/IEC JTC1 SC 42 is already in process, and it is an area that is being actively discussed in various regions including Japan. Therefore, it is very important for Europe does not establish its own standards with European standardization bodies alone and create market rules that are isolated from the rest of the world, but Europe must work closely with international partners to bring together excellence from all over the world, and to take the leadership in global standards.

Depending on the specific content of the requirements, the development and operation costs of AI providers and users may increase unnecessarily, resulting in increased risk in the European market. For example, Article 23 states that "Providers of high-risk AI systems shall, upon request by a national competent authority, provide that authority with all the information and documentation necessary to demonstrate the conformity of the high-risk AI system with the requirements set out in Chapter 2 of this Title, in an official Union language determined by the Member State concerned", but it should be recognized that AI providers will incur significant costs when required to meet standards comparable to ISO 15408 security certifications. The details of the mandatory requirements that determine the extent of the European AI market risk should not be decided in a closed forum in Europe, but rather should be discussed among international stakeholders for the development of AI worldwide, and balanced requirements should be pursued to avoid placing undue burden on only some parts of the AI ecosystem.

The separation of "AI providers" and "AI users" and the strict regulation of the former may hinder the formation of the trustworthy ecosystem. In order to ensure the proper use of AI, it is important to clarify that efforts are required not only for providers but also for the entire ecosystem, and to encourage efforts by users.

ii. Quality Management System (Article 17)

We are aware of the need for a quality management system for AI systems, and are contributing to many domestic and international discussions, including the ISO/IEC JTC1 SC 42, the Japanese Ministry of Economy, Trade and Industry and AIST "machine learning quality management guidelines", and QA4AI (AI Product Quality Assurance Consortium). Because AI quality is highly dependent on training data quality, quality assurance based on AI use cases is more important than a uniform quality management system. We therefore support that this bill should be limited to high-level statements. Requirements should be discussed in ISO/IEC JTC1/SC 42 within the context of "Foundational standards" as well as data quality assurance and lifecycle based on use cases.

iii. Conformity Assessment (Article 43)

The term "substantially modified" in paragraph 4 is unclear and we request to supplement its definition, modify additional contents, or add specific examples.

iv. Automatically generated logs (Article 20) and Post-market monitoring by providers (Article 61)

With DNN (deep neural network) logs, it is not possible"to evaluate the continuous compliance of AI systems with the requirements (Article 61 (2))" due to its non-explanatory nature and this can increase unnecessary loads on AI providers. Therefore, the degree of post-market monitoring should be left to the discretion of providers and users, and we support the content of Article 20 paragraph 1 " to the extent such logs are under their control by virtue of a contractual arrangement with the user or otherwise by law ".

v. Cooperation with competent authorities (Article 23)

We understand that allowing access to information containing trade secrets to a "national competent authority" except law enforcement agencies such as police should be avoided, and that the article "to the extent such logs are under their control by virtue of a contractual arrangement with the user or otherwise by law" guarantees this. We request to add the criteria for "reasonable demand" in order to prevent unreasonable demands from a "national competent authority" except law enforcement agencies.

vi. Reporting of serious incidents and of malfunctioning (Article 62)

As for "the limitation of reporting" not later than 15 days after the providers becomes aware of the serious incident or of the malfunctioning." In paragraph 1, since the distribution of software is widespread unlike hardware, it is practically unrealistic to report to all member countries within 15 days, depending on the criteria of the reporting report that is being done. We request that the deadline be extended to a more realistic one.

vii. Access to data and documentation (Article 64)

Fujitsu requests that the European Commission and co-Legislators review the source code disclosure requirements in Section 64 (2). This is because there is a risk that advanced security technology may be leaked or used for the unintended purpose, and there is a possibility that disclosure may be impossible for reasons such as contracts and security, which may affect the purpose of the realizing trusts and spreading AI.

5. AI ACT Enforcement (Title VIII, Chapter 3)

Fujitsu strongly believes that a harmonized enforcement of the AI ACT will be crucial for a correct adoption of this Regulation. It is key to avoid fragmentation and different levels of enforcement in the Member States that could create uncertainty and discourage innovation and adoption of new AI solutions in the EU market.

6. Support of Innovation (Title V)

Title V of the proposal introduces innovative and flexible regulatory approaches such as regulatory sandboxes to encourage and stimulate AI innovation. Fujitsu is concerned by the adoption of sandboxes as well as the way their implementation is described in the AI ACT. We would rather encourage the adoption of "auditable data access and processes" in the testing and training phases of an AI system. In order to have a good quality of data, it will be essential that the EU will sponsors data programs to encourage citizens to provide their data (data altruism) in a secure, effective and eventually rewarded way. Access to data is essential in the testing phase and this must be allowed in a secured way by the EU so that Innovative solutions can be securely tested in the EU without violating any key principle of the AI ACT.

7. Codes of Conduct (Title IX, Article 69)

Fujitsu appreciates the promotion of Codes of Conduct on the AI ACT. Codes of Conduct should be strongly driven by industry and experts working on AI systems and solutions. Encouraged codes of conduct should be as much align with international standards as possible in order to avoid fragmentation.

8. Penalties (Title X, Article 71)

There is a concern that the wide range of penalties, almost all of the obligations set out in the legislation, and the very high fines may unnecessarily increase the risk of corporate activity in the European market. The article states that when determining the amount of a fine, the nature, gravity and duration of the infringement and its consequences are taken into consideration according to the purpose of the AI. From this sentence, we assume that the amount of a fine may differ depending on whether the person has actually violated human rights, or the person has only committed a formal violation without possibility of violation of human rights. We request more detailed information on the standard and range of fines to help business operators make appropriate risk management decisions.

9. Conclusion

Fujitsu strongly encourages the European Commission and co-Legislators to work together with all stakeholders in order to achieve a common goal: having an effective, flexible and clear horizontal regulation on AI able to "work" at global level.

We appreciate the opportunity to provide our comment to the actual proposal of the European Commission and we are committed to work with the European Parliament and European Council during the legislative process.

The alignment of key principles for AI and new technologies between the Japanese Government and the European Union is an important common ground for further cooperation at an international level. Fujitsu is committed to continue working closely with both the Japanese Government and the Commission by providing advice and contributions from our experts in order to achieve a global view with a strong presence from both regions, with the ultimate intent of delivering benefit for our societies and citizens.