Feedback to the European Commission's regulation proposal on the Artificial Intelligence Act

Brussels, August 6, 2021

General

National AI associations that have gathered around the European AI Forum have put forward the following feedback to be considered by the European Commission (Commission) in regard to the Artificial Intelligence Act. The below listed feedback concludes that the current proposal lacks clear definitions and operationalization. In addition, a harmonized European approach is missing. This is a joint statement by **KI Bundesverband (Germany), Hub France IA, AI Austria, AI Cluster Bulgaria, Fundacja Digital Poland, AI4SI (Slovenia) and CroAI (Croatia).**

1. **Definition**

   We perceive the definition of AI in the proposal as too broad. Almost any existing and future software could be classified as AI under that definition. We urge the Commission to revise its definition of AI so that only real AI applications will be considered. However, in the sense of a level playing field where the same regulations apply to techniques having the same risk implication, we believe that the prohibitions and obligations of the Artificial Intelligence Act should **not only be triggered by any tailored and specific technology defined as AI, but also consider measures having equivalent effect**. Currently, use cases identified as prohibited or high risk may be realized without applying the technologies specifically defined as AI, allowing circumvention of framework of trust to be created by the Artificial Intelligence Act.

2. **Risk-based approach**

   We welcome the risk-based approach and that not every AI-system is banned without a closer examination. Still, the risk categories lack clear definition and operationalization. Especially for SME, it will be hard to assess AI products without guidelines. We believe compliance standards on a more granular level should be provided to ensure clarity of the obligations and requirements.

3. **Guidelines**

   We found several unclear operationalization of definitions, criteria and requirements. These lead to uncertainties on the side of businesses in general and among SMEs in particular.

We underline the importance of application- and industry-specific guidelines for the implementation of the act in the industry. These guidelines should already be developed jointly with AI developers.

4. **Harmonized European framework**

It will be crucial for the European AI ecosystem to create a level-playing field in all Member States of the EU. No country should be able to take advantage of lower sanctions or easier audit processes. Unfortunately, the current proposal is not clear enough on how a harmonized framework can be established and ensured.

5. **Data and Bias**

We welcome the goal of the Commission to create better data sets. However, we evaluate Article 10.3 as unrealistic, as even representative data sets can be misleading, and a bias can evolve out of every data set. Even though huge amounts of data are created and collected daily, such data and its potential remains untapped in data silos and the Artificial Intelligence Act does not create a basis for data sharing, of course subject to appropriate safeguards. Acknowledging the fundamental importance of data privacy and individuals' rights to data, we believe that data available and gathered already (e.g. by institutions, authorities, etc) should be made available subject to safeguards imposed for the rights of individuals under the GDPR and privacy acts. Moreover, we lack a differentiation in the definition of the term bias between unwanted societal biases and useful technological ones. In the current form, the definition also entails AI applications that do not deal with societal issues. A bias should not directly be disregarded, but assessed on a case-by-case basis.

6. **Recitals**

We believe many of the current recitals are too general and based on assumptions towards AI applications. Therefore, the recitals should be rewritten, ideally jointly with AI developers.

7. **Sandboxes**

The AI regulation shall be an enabler of AI innovation and strongly stand behind start-ups, especially during prototyping and testing. Therefore, start-ups and innovators should be allowed to create their own sandboxes, following a code of conduct. While in the sandbox phase, the involvement of supervisory authorities should not be mandatory. When leaving the sandbox phase, which shall mean that a product-market fit is found, start-ups and SMEs shall be obliged to invest in fully complying with AIA rules and regulations.

The Regulation proposes the creation of “AI regulatory sandboxes,” which are controlled environments intended to encourage developers to test new technologies for a limited period of time, with a view to complying with the Regulation. Among other things, these regulatory sandboxes should allow personal data lawfully collected for a separate purpose to be used to develop or test innovative AI systems. The Regulation would also require Member States to adopt measures benefitting small-scale providers and start-ups, such as priority access to the regulatory sandboxes and support in complying with the Regulation and other EU rules.

In order to guarantee the equality of all member states, a report should be created outlining the status of regulatory sandbox adoption and offering roadmaps for harmonization of the basis set-up of regulatory sandboxes. We believe that from a technology point of view, **developing modern AI techniques require the following three pillars: (i) data access, (ii) heuristic knowledge and (iii) computing power.** Therefore, the framework for the creation of AI sandboxes should provide active support in these three vital areas to foster the development of trustworthy European AI and excellence center.

8. Prohibition of biometric surveillance

The Artificial Intelligence Act prohibits "real time" remote biometric identification systems in public spaces for law enforcement purposes (Article 5) with several worrisome exceptions. We believe the scope of the current provision does not sufficiently prevent the risk of indiscriminate mass surveillance and the full threat such use case poses to fundamental principles of democratic societies. In our view, the prohibition should extend to (i) systems having equivalent effect, irrespective of the technology, (i) public authorities and private actors acting on their behalf, (ii) 'post' biometric identification systems subsequently applied and not provide for any exemptions based on the criminal offence.