## AI4Belgium Feedback Note on the European Commission’s Proposal for an ‘Artificial Intelligence Act’ (proposed AI Regulation)

## **Key feedback points**

1. Overall, the proposed regulatory framework is much appreciated and welcomed.
2. The “list-based” approach risks being incomplete, and requires periodic assessments.
3. The Scope of the Regulation requires further refinement.
4. Further clarifications are needed as regards certain terms.
5. The requirement of *ex ante* third party conformity assessment could be extended.
6. Some open questions remain around the value of the proposed CE label.
7. Concerns about the regulation’s enforcement mechanism should be addressed.
8. Additional efforts are needed to stimulate innovation.
9. More attention should be given to the impact of AI on societal interests.

## **Introduction**

AI4Belgium is a community-led initiative, enabling Belgian individuals and organisations to capture the opportunities of AI while facilitating the ongoing transition towards the technology’s increased adoption in a responsible and trustworthy manner. AI4Belgium has the ambition to position Belgium on the European AI landscape, drawing on the many assets vested in the Belgian AI ecosystem, from high quality researchers, excellent entrepreneurs and companies, to innovative public entities, all the while being mindful of the ethical, legal and social challenges that this technology brings forth.

AI4Belgium welcomes the opportunity to provide feedback on the European Commission’s proposed ‘Artificial Intelligence Act’ in the form of a new EU regulation (hereinafter referred to as the ‘proposed AI Regulation’), which was published on 21 April 2021.

The Commission’s proposal was overall well-received by the AI4Belgium community, and is considered to be a strong starting point to ensure that AI systems are deployed in a manner that respects fundamental rights within an environment that is keen on socially beneficial innovation. There is, however, still some scope for clarification and specification throughout the proposed AI Regulation. Without aiming to be exhaustive, this feedback note provides an overview of the main considerations formulated by the AI4Belgium community.

This note was prepared in the context of a virtual workshop organised by AI4Belgium’s Working Group on AI Ethics & Law on 18 May 2021 for the members of the AI4Belgium community, in cooperation with in cooperation with the different regional AI hubs, including Kenniscentrum Data & Maatschappij, CRIDS/NADI and the AI Institute for the Common Good (FARI) During and after the workshop, feedback was gathered on the proposed AI Regulation’s strengths and weaknesses from the perspective of the Belgian AI ecosystem. On this basis, a first draft note was prepared, which was subsequently circulated within the AI4Belgium community in order to provide all members an opportunity to consult the document and provide further input. The end result comprises the consolidated feedback of the AI4Belgium members on the proposed AI Regulation.

In what follows, the key points of feedback that were raised by the AI community are provided, with suggestions on how the proposal could be further improved.

## **Overview of AI4Belgium’s feedback**

1. **Overall, the proposed regulatory framework is much appreciated and welcomed**

AI4Belgium commends the Commission’s overall approach to the regulatory framework for AI that it put forward. The debate on an adequate ethical and legal framework for Artificial Intelligence has been ongoing for several years now, and the time was more than ripe to propose a number of binding rules to ensure that citizens and organizations can trust AI systems that are deployed across the EU through verifiable procedures rather than voluntary guidelines. These procedures to enable trust are not only important to ensure compliance with fundamental rights, but also to stimulate the adoption (and intra-EU trade) of AI to capture the benefits that this technology can generate.

The emphasis on regulating the use of AI rather than the technology itself is welcomed. At the same time, given that AI systems can be repurposed for various uses, the Commission’s proposed design, development and deployment requirements (in terms of risk-management, data governance; technical documentation; transparency; human oversight; and accuracy, robustness and cybersecurity) are essential, and will need to be translated into practice.

1. **The “list-based” approach risks being incomplete, and requires periodic assessments**

AI4Belgium members particularly appreciated the risk-based approach of the proposed AI regulation, and the important signposting of risk levels by way of the chapters’ headings (namely a set of prohibited AI practices, a set of high-risk AI practices, a set of AI practices that require further transparency, and other AI applications). Some members rightfully remarked that a list-based approach risks being incomplete, yet at the same time it is acknowledged that it is difficult to ensure the comprehensiveness of such lists of practices from the outset. It is therefore crucial that the said lists can be updated periodically and in a speedy manner, without the need to revisit the entire regulatory framework.

While such procedure is explicitly foreseen in the context of high-risk AI systems (through delegated powers granted to the European Commission), we note that this procedure is currently lacking as regards the updating of the list of prohibited AI systems. It may be advisable to opt for a similar approach for both types of AI systems. At the same time, whenever these lists are updated, it is essential that the Commission involves a broad set of stakeholders in this process, ensuring that representatives of civil society, industry, academia and the public sector can have their voices heard.

1. **The Scope of the Regulation requires further refinement**

The approach in the proposed AI regulation consists of providing a broad definition of AI, by including both new and old approaches to this technology (e.g. not only machine learning but also symbolic). We believe that this broad approach is helpful to evaluate as many AI innovations as possible, since the focus should lay on the potentially problematic use rather than the underlying technology. If the same harmful conduct can be enabled through a classic type of AI system, this is equally problematic from a fundamental rights point of view.

The broad definition of AI is supplemented with an annexed list of concrete technologies that fall under the scope of AI. One downside to this list concerns the fact that the quality of the scope of this regulation is now largely influenced by the this annex (and the clarity and comprehensiveness of the concepts listed there), which relies on efforts from the Commission who can review this list over time. What is more, the list may ultimately lead to regulation shopping; innovations could defined or framed by AI developers in different way so as to fall inside or outside of the list, hence potentially leading to under-enforcement. The regulation’s scope is, after all, mostly defined by whether or not a given application falls under any of the listed risk-categories (i.e. considered as prohibited, high-risk, or requiring further transparency), and thereby in any case excludes (AI) systems that do not fall under those problematic categories.

Given the focus on the problematic use / consequences of technology rather than on the technology itself, we would suggest to keep a broad definition of ‘AI’, along the lines of the following: each practice or system that relies on automated processes could be considered as an AI system. Hence, for each such practice or system it should be verified whether it falls under the risk categories covered by this regulation or not. Otherwise, the regulation risks having a bias towards problematic uses only by known/hyped AI systems, rather than by systems that potentially cause the same problematic impact but are not listed in Annex.

Finally, the proposed definition seems to focus on AI as a software exclusively. This can cause some interrogations from the scientific community around the exclusion of AI as a hardware (e.g. in robotic devices). If the aim is to secure a broader definition of AI (which includes robotics), or if there is a section that addresses robotics specifically (or a justification of the exclusion), this should ideally be included in the text for clarification purposes.

1. **Further clarifications are needed as regards certain terms**

*Putting on the Market/Into service***:** The proposal specifies that AI systems should comply with the regulation when “placed on the market” or “put into service”. This concept is already well-established and documented in existing legislation relating to physical products, but for digital products this concept is quite new. As digital systems often undergo multiple iterations and developments before they are considered to be fully implemented and ready to release, clarification is needed on when the AI system should be compliant. If, for example, compliance should already be ensured when a proof of concept is delivered to a client, this would significantly increase the costs of developing an AI business case while at that point there is no certainty the application will actually be purchased by the client.

*Citizen Scoring*: Public services already assign scores to citizens in numerous contexts (from verifying eligibility to social benefits to the risk of recidivism, and from the need for intervention to protect / place children to the chances of easily finding a job. Further clarification about the practices that fall under the prohibition on general citizen scoring would hence be welcomed, as the language that is currently used in the proposed regulation, and the examples provided by the European Commission in its presentations are not always clear.

1. **The requirement of *ex ante* third party conformity assessment could be extended**

Currently, the proposal stipulates that only AI systems intended to be used for the ‘real-time’ and ‘post’ remote biometric identification of natural persons will be subject to an *ex ante* third party conformity assessment. Other AI systems classified as high-risk, like recruitment or predictive policing, will be subject to self-assessment by the provider.

However, given the fact that such high-risk systems pose significant risks for citizens in terms of fundamental rights and societal impact, it could be considered to extend the requirement of third party conformity assessments to all high-risk AI systems. Such extension could be beneficial for all parties concerned, as it can enhance trust in the fact that the AI systems meet the required standards. Moreover, this could also improve legal certainty by further reducing the risk of liability claims for unintended consequences of these high-risk AI systems.

1. **Some open questions remain around the value of the proposed CE label**

On the CE-label for AI applications in Europe, the AI4Belgium community is of the opinion that it can help creating trust and assurance in technology that is complex to understand for users. This label could ensure the user that he is working with trustworthy AI. However, with a label certain risks arise such as a potential false flag for unreliable products being marketed in Europe. To achieve such a label, there is a big need to have standards to support organizations to comply with the requirements. As it is, these standards do not yet exist, and it will take a huge effort to ensure that they are published in time before this regulation comes into effect.

In this regard, when setting up these standards or best practices, it is also important to consider the views of various stakeholders, including civil society, so as to ensure that compliance with the requirements is not only claimed but can also be demonstrated and lead to *earned* trust.

1. **Concerns about the regulation’s enforcement mechanism should be addressed**

The proposed regulation sets out various requirements that AI providers and users will need to meet, and establishes an enforcement structure to ensure compliance with those requirements. During the AI4Belgium feedback session, an overwhelming majority of members indicated their preference for a shared governance and enforcement approach, with a good balance between the national and EU level. Currently, the regulation lays more focus on the national supervisory authorities who will be first in line to implement and enforce this regulation. However, lessons should in this regard be learned from the enforcement structure of the GDPR, where the guidance given by national DPA’s was quite limited in the beginning. As an example, the first code of conduct was approved by the Belgian DPA 3 years after the GDPR came into effect. Moreover, enforcement of the GDPR likewise befalls national authorities and – due to unequal investments in the various member states’ authorities – citizen protection is not at the same level in each EU country.

Also in the context of this regulation, it should be considered that too much emphasis on the national level can lead to a risk of unequal implementation in different member states, at different speeds and potentially different interpretations. Belgium has, for instance, been lagging behind with regard to the implementation of the GDPR; this delay may affect innovation and a European level playing field, and the same risks to happen in the field of AI. Strong coordination at the European level will hence be crucial. Moreover, given the importance of the risks attached to the use of AI as set out in this regulation, it will be essential that these authorities receive proper funding (and a sufficiently skilled workforce – which risks being difficult in this field) so that they can provide adequate guidance for organizations and ensure a high level of citizen protection.

The issue of different speeds will also affect the creation of codes of conduct for the voluntary application to AI systems other than high risk. If we assume that the creation of a code of conduct is roughly the same effort and cost for any sector or member state, this absolute cost will mean that there may be more codes of conducts for sectors and member states with a higher turnover. Smaller member states with smaller markets will thus likely have less means to create these codes of conduct.

Furthermore, while currently not foreseen in the proposed regulation, citizens should be provided a right to file a complaint with national authorities, since this will not only help closing the protection gap, but it can also help national authorities to assess and establish potential breaches of the regulation. In this way, public and private enforcement can be more complementary, and citizens will have a more active role in ensuring the protection of their rights.

Finally, the creation of a database for high-risk AI systems deployed in Europe is a welcome development, as it provides for more transparency that can benefit both public and private enforcement of the regulation and of fundamental rights that can potentially be breached by the use of AI. It may however also be considered, given the crucial task of the public sector and the importance to secure trust and transparency, to broaden this database to include all AI systems used by the public sector rather than only those that were explicitly listed as high-risk.

1. **Additional efforts are needed to stimulate innovation**

The abovementioned issue of different member states’ speeds of implementation of the regulation risks being even more prevalent with regard to regulatory sandboxes, as the Commission expects the initiative to be taken by national competent authorities and member states. However, this will be crucial to stimulate innovation in AI and ensure that European citizens can also benefit from the opportunities of this technology. In order to mitigate this issue, additional measures should hence be taken to incentivize the establishment of regulatory sandboxes at member state level.

Indeed, while it is positive that the Commission urges Member States to set up regulatory sandboxes, this process should be further formalized. Regulatory sandboxes can only foster innovation if they are supported by adequate incentives. The relevant national authorities, like the national data protection authorities, need to build competences and experience in this area, and should be supported by the Commission on this. Adequate funding and skilled personnel are also essential. Sandboxes should be closely monitored, and information about regulatory sandboxing initiatives should be shared as openly as possible to provide learning opportunities and best practices for other member states.

Finally, the measures to help small scale AI providers and users may need to be extended. While such providers and users have priority access to regulatory sandboxes, participating in them will require a huge time and resource investment from their side. Hence, they may need to be financially encouraged to participate. While a reduction of the cost of third-party conformity assessment for small scale providers and users is welcome, this should be further extended to specific funding for organizations who undergo a self-assessment procedure. In Belgium, we see that start-ups, scale-ups and SMEs develop many of the most innovative AI applications. Without adequate incentives, this regulation may put them at a competitive disadvantage compared to bigger companies who already have a lot of experience with compliance mechanisms.

1. **More attention should be given to the impact of AI on societal interests**

While the proposed AI regulation certainly advances citizens’ protection against AI’s adverse impact by countering some of the risks posed thereby, the attention to societal interests is fairly limited (as opposed to risks to individual interests). For instance, the adverse effects that the use of AI can have on the rule of Law or on the integrity of the democratic process, does not seem to be tackled through this regulation, nor is the environmental impact of AI systems. There is hence further scope left to provide attention to these aspects, and grant the public a greater role to counter these risks. This can be done, for instance, by allowing individuals to file complaints with supervisory authorities, providing for collective redress mechanisms, and stimulate public interest litigation against uses of AI that may breach public values – for instance through the accumulative effects of the use of AI systems on a wider scale. In addition, stakeholder consultations should be organized at a frequent basis in order to determine the extent to which the regulation needs periodic revision to effectively counter the risks of problematic AI practices.