

## Feedback Report on the “White Paper on Artificial Intelligence” in the context of the European Commission’s public consultation

by AI4Belgium

### A. Introduction

We welcome the publication of the White Paper on Artificial Intelligence (AI) by the European Commission (EC), and the opportunity to provide our feedback on it. Overall, we believe that the risk-based approach to AI governance is something that could be very beneficial in terms of safeguarding the protection of EU citizens, without overburdening European companies and organizations with heavy requirements. A balance must be found between securing innovation and protecting our European values, which seems to be acknowledged by the European Commission. While this White Paper provides a good start in setting out how this balance should be reached, its publication also raises a lot of questions around the concrete implementation of this approach, around the terminology and scope of the measures, and about some of the propositions made.

This Feedback Report is the product of a workshop held by AI4Belgium. 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 manner. AI4Belgium has the ambition to position Belgium firmly within 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.

During the workshop, a delegate from the European Commission explained the context and purpose of the White Paper, and engaged into fruitful discussions with members of the AI4Belgian initiative. A lot of questions were directly answered during the workshop, yet further questions and remarks were also raised which we believe could help in contributing to the improvement of the Commission’s approach to AI regulation. These questions and remarks were collected during the workshop, and subsequently circulated within the AI4Belgium community, allowing all members an opportunity to consult the feedback document and provide their further input. The end result comprises the consolidated feedback of the AI4Belgium members.

This report first provides general points of feedback raised by the community (B). Thereafter, comments are provided more specifically concerning the eco-system of excellence (C) and the eco-system of trust (D) that the Commission intends to establish. Finally, some concluding remarks are offered (E).

### B. General comments

- Several concerns were raised regarding the scope of the White Paper. On the one hand, it is appropriate to delineate which technology is being assessed, and to propose a working definition of Artificial Intelligence. On the other hand, such definition would need to reflect the state of the technology in adequate manner, providing legal certainty and not being overly broad. We would suggest the EC to carefully reconsider the scope of its AI-definition, and in particular to clarify to which extent it is meant to cover also traditional software, or whether it is rather only limited to e.g. *machine learning* applications. The currently proposed working definition seems to be

# AI4Belgium

deficient in this regard and is in need of further clarification. Actively involving more (technical) AI-experts would be beneficial. It might also be useful to clarify the link between AI and robotics.

- The main focus of the White Paper lies on AI, and more specifically on AI applications using *deep learning* methods. However, a number of issues directly stem from the data that is being used rather than from the AI-application. We would hence suggest to put more emphasis on the need for adequate data governance processes, as for many AI challenges (such as bias, quality or transparency) this will be key to solving the issues, regardless of whether the underlying application could be strictly categorized as an “AI-system”.
- The document is structured around enhancing consumer trust in AI. However, it fails to focus on the importance of also enhancing companies’ trust in implementing AI. Due to the great ambiguity and uncertainty around the regulations that are currently applicable to the use of AI applications, many companies are reluctant to start using them, precisely because they do not trust that by doing so they do not expose themselves to legal infringements. A specific example here is that, currently, some companies may not be willing to use AI in their HR processes because they fear that they might not be legally compliant, and that thereby the positive effects of using AI (when doing so in an ethical manner), such as the removal of previous human biases, are missed out on. We would therefore suggest the EC to issue specific guidance (potentially also on a sectoral basis) what regulations already apply to AI and in which manner their compliance can be secured by companies.
- While the White Paper recognizes that there are already a lot of regulations in place, there have only been limited studies on the interplay between AI and these existing regulations. We would suggest considering and clarifying to which extent it would be a more suitable approach to try and integrate potential concerns arising from AI as much as possible into these separate existing regulations rather than proposing a new all-encompassing regulation which may raise important overlaps.
- The current crisis around COVID-19 sheds a new light on AI as a supporting instrument in fighting the fallout of the disease. At the same time, the ethical concerns associated with the impact on privacy, autonomy and civil liberties are likewise more prominent. It would be beneficial for these considerations to be taken into account in the Commission’s reviewed approach to AI.
- Better integration between the AI strategy and the Commission’s data strategy could be helpful. More clarity is also needed on the link between AI policy on the one hand, and open data and FAIR access to data on the other.
- It is important that the Commission collaborate with practitioners, businesses, developers etc. in defining the requirements to ensure that it is workable and realistic in practice. A multidisciplinary approach involving experts from other disciplines (ethicists, lawyers, sociologists...) is crucial.

## C. An ecosystem of excellence

- We welcome the acknowledgment of the need to build an ecosystem of excellence around AI, which is a crucial element of the EU approach to AI.
- However, it appears that the actions proposed in this section might be more political than concrete: most of them are rather ‘high level’, and for people who are working with AI on a daily basis it is unclear what direct benefits they will generate. This renders it more complicated for European companies and organizations, especially for SME’s, to see where and how they can actively participate in these actions and how this will create value for them specifically. Moreover, it appears that many of the actions proposed are in fact reiterations from previously made

# AI4Belgium

commitments. We would therefore recommend further stimulus towards the development of an AI ecosystem of excellence in Europe, with actionable plans for achieving this.

- “Excellence” should, furthermore, not be seen as separately from “trust”. We can further enhance European AI excellence by ensuring that the technology is of high quality and trustworthy, and ensuring trust will also contribute to European excellence in AI. It would hence be good to see both ecosystems as one common endeavor rather than as separate issues.

## D. An ecosystem of trust

- While a focus on AI regulation that is centered around risk seems appropriate, the concept of ‘high risk sectors’ raises a number of questions.
  - Some concerns are raised about the cumulative requirement of high-risk sector and high-risk application, which could leave out some important high-risk applications in sectors that were not marked as such.
  - It is unclear what happens to applications that can be used across different sectors, which can often be the case when it comes to AI. How would a delineation and evaluation take place of whether an application that is working in a certain sector cannot also be used in another sector? Are multiple certifications/ex ante assessments needed for this? On paper this distinction may sound straightforward, but in practice many applications are designed for horizontal rather than vertical usage.
  - Moreover, this may incentivize companies to try to classify their applications in a vertical setting which has not been categorized as “high-risk” to avoid strict requirements, potentially leading to situations where applications that can nevertheless cause a significant risk are classified as non-high risk.
- How and where to draw the line between high and non-high risk will be key, and we advise that this classification be made as clear as possible so as to not create unclarity about which AI systems have to comply and which do not. Risk can be defined in many different ways, and the White Paper has not yet defined those different ways and the consequences thereof. For instance, even if “risk” is defined as “a breach of fundamental rights”, it is far from straightforward for a company to assess whether or not their AI application may breach a fundamental right, without first knowing what those rights entail, how they apply in a certain setting, and engaging into a fundamental rights impact assessment. This would, however, not only be time-consuming but also prohibitive for many smaller productions, especially if the legal expertise is lacking.
- Consideration must be given to risks that may arise from the development and use of AI applications, but which are not specific thereto and could also arise from other technologies. Although currently a regulation is envisaged that only deals with AI, this would leave out the exact same risks created by non-AI technologies which would nevertheless also negatively impact citizens.
- Risks involving the dual use of AI is also something that should be taken into account and reflected into the Commission’s approach.
- We suggest further consideration on the extent to which the importance of these requirements – and their concrete implementation – may differ across sectors, even across sectors that are “high-risk”.
- We understand that the future regulatory framework would need to be applied to operators that are not established in the EU. However, considering the importance of correctly allocating responsibilities between operators, we wonder how this will be enforced and controlled in

# AI4Belgium

practice. More clarity is needed on the governance of this controlling and enforcing structure, both for actors within the EU and those outside the EU. Clarity is also needed on whether there will be a specific / new authority enforcing this.

- Regarding the question of “subsequent use”, the extension to which AI can be used is less definable and trickier than it is for a classic product. Behind a lawful use can lie an unlawful or discriminant one in a way that is more subtle than it is for a classic product. The same goes for other terms such as “safe”. It might therefore be interesting to define those kinds of terms.
- A clear distribution is needed of the requirements in terms of who is ultimately accountable for compliance (and potential damages) in case of breach. For example, the collection of data for a final application can be done by one operator, the development by another. There should be a clear procedure of how the requirements – and consequences of breaching those requirements – would be applied. For instance, if responsibility for these requirements ultimately rests with only to the final operator, then legislation should mention this in clearest terms possible.
- More clarity is needed regarding the temporal application and implementation of the regulatory framework. Will it work retroactively? Will the regulation regularly be updated in light of new technological developments? Will all products and services which are already in the market also be subjected to these requirements, or will this only apply to applications and services that are put on the market after the regulation comes into force? For AI-users, developers and providers it is important to have such information as soon as possible, in order to have a reasonable time frame to modify their products, services and processes.
- A number of suggestions in the White Paper indicate a close link to certification, both as concerns the ex-ante scheme for high-risk applications, and as concerns the voluntary labelling scheme for the lower-risk applications. We would suggest the EC to carefully consider the cost of such certification mechanisms versus the potential return. Overly burdensome certification schemes will limit market access for new players and stifle not only innovation but also competition. Time to market will also increase which may put Europe at a disadvantage against international players, and deprive European consumers of the same benefits. While we acknowledge that an enforcement mechanism needs to be put in place to verify that the requirements are met, it would be important that all the modalities of such mechanism are carefully considered. Moreover, it would be essential to consider to which extent a new certification/verification would be needed when the system acquires new features or knowledge, and what the impact of such need would be on the market and on consumers.
- Certain requirements that are suggested, such as the provision of information about the AI-application, could be applicable more broadly for AI-systems in general rather than only for high-risk applications, as there is a substantial benefit to ensure more transparency around this. Any additional information obligation should however be implemented in a consumer-friendly way.
- The voluntary labelling as it is currently suggested in the whitepaper raises a lot of questions. If there are no standards or procedures to solidify this suggestion, we fear this may become a meaningless label, or even a false flag of convenience that non-EU companies could fly under to promote their non-compliant products in the EU. While we appreciate that also producers of applications with lower risk would also like to be able to promote their products as “trustworthy”, a clear mechanism would need to be foreseen if this were to be put in place, to ensure that such labels could be verified and thus be meaningful for consumers.
- More careful analysis of ex-post requirements and/or self-assessment mechanisms should be carried out as a potential additional approach.

## E. Conclusion

The comments formulated above are meant as a helpful addition to the approach set out by the EC, of which our impression and vision is overall very positive. We believe that it is important for the Commission to take ownership of the debate around the usage of Artificial Intelligence, and that a coordinated EU approach is the best way forward.

The organization of the public consultation shows an openness towards the input of all those who ultimately would be affected by the outcomes of the policies and regulations adopted by the EU, and the opportunity to contribute our views is something we greatly appreciate.

We look forward to the Commission's revised approach, and to working together on creating Artificial Intelligence for the benefit of Europe and its citizens.