Contribution to the European Commission consultation on the proposal for a regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)
3 August 2021

ADIGITAL
POSITION PAPER

Proposal for a Regulation Laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts

On April 21th, the European Commission proposed new rules which set the path to build an ecosystem of trust in Artificial Intelligence (IA) in the European Union with the presentation of its proposal for a Regulation laying down harmonised rules on IA (Artificial Intelligence Act) which is the first ever legal framework in this field.

Artificial intelligence (AI) is evolving rapidly and it is a strategic technology which provides enormous opportunities. While most AI systems pose low to no risk, other AI systems may represent undesirable risks which must be addressed.

In this context the proposal seeks to ensure that IA is safe, lawful and goes in line with EU fundamental rights. Thus, its main goal is to stimulate the uptake of a trustworthy artificial intelligence and ensure a well-functioning internal market for AI systems where benefits and risks are adequately addressed.

Adigital would like to take this opportunity to provide its feedback on the proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act).

Hence, Adigital welcomes the regulatory proposal on Artificial Intelligence and is committed to continue supporting the creation of trusted and innovative AI technologies in Europe.

I. General Remarks

The draft Regulation is built on a risk-based approach needed to foster trust in AI without hindering its responsible development. **Adigital has long called for a proportionate approach that would regulate high-risk use cases**, not the AI technology itself.

We support the idea outlined in the proposal that AI applications should be considered high-risk when they meet certain criteria, such as the severity and the probability of occurrence of certain serious harms to persons, for instance, threats to health, life or fundamental rights.

In this context, reflecting the complexity of the AI ecosystem in the balance of obligations for different stakeholders, it's crucial. It will seldom be feasible or effective for providers of general-use AI systems to manage all of the risks associated with potential application in high-risk systems, as is currently envisaged in the AIA. For example, the provider will often not have access to the operational data necessary for post-market monitoring if the AI system has been put into operation by another entity. To address this, we recommend a new class of "deployers" be added to the AIA with responsibility for complying with regulatory requirements associated with deploying general-use AI systems in high-risk applications.

Likewise, **Adigital opposes the use of technologies including facial recognition for mass surveillance, racial profiling and violations of basic human rights and freedoms**. We agree with the European Commission that the use of **AI Systems by law enforcement authorities for biometric identification should be prohibited unless certain safeguards and very limited exceptions apply.**

We commend the European Commission for following the recommendations of the Commission's High Level Expert Group on AI Ethics in drafting some of the legal requirements for high-risk AI systems.

Thus, while Adigital welcomes the principle of the risk-based approach, we believe that some adjustments will be necessary to make sure the new rules are proportionate, legally clear and risk-based all the way through the text.

Hereinafter, we provide some examples:

- **Regarding the definition of artificial intelligence, as well as the list of techniques covered in Annex I seem very broad.** While we understand the European Commission's objective to make this regulation future-proof and technology neutral,

such a broad scope does not seem to align with the risk-based approach. With such a broad definition and set of techniques, a very significant amount of software applications could be covered by the text.

- **It is unclear how and if the rules apply to general purpose AI,** where the provider cannot know if the use will be high risk and cannot dictate the exact use of the system by the user.
- Some of the areas classified as **high-risk applications in Annex III seem very broad** and thus, would include uses which are not high risk at all, for instance. in the area of human resources.
- **Some requirements applying to high-risk systems will need to be revised** to better take into consideration proportionality and feasibility, as they may be difficult to comply with, while some obligations on providers are overreaching.
- To sum up, we recommend clarifying certain provisions to provide legal certainty around scope and protect privacy. The AIA includes a number of terms and provisions that would benefit from further clarification to ensure that providers of AI systems understand how the scope and requirements of the AIA apply to their products. For example, the definitions of "safety components" and "significant changes" could be further clarified to provide legal certainty around when systems come in scope of requirements for high-risk AI systems.

Obligations for providers and users

The proposal as currently drafted does not distinguish between the responsibilities of AI users when in a deployer role, and the responsibilities of providers to the customers. This is challenging for companies providing general purpose APIs and/or open source models that are not specifically intended for high risk AI systems, but are nevertheless subsequently used by third parties in a manner that could be considered high risk and in scope for compliance (e.g. open deep fake detection API that is used by law enforcement, traffic routing model used by municipalities to dispatch first responders).

In such situations, we would recommend for deployers to bear primary responsibility for compliance and conformity assessment, because only they can verify the end-uses to which their systems are put, and any additional data that has been input into training their system. Providers of general purpose APIs should of course provide all information necessary for the deployer to conduct their conformity assessment, but cannot be responsible for something over which they have no control and little to no visibility. A similar logic applies with regards to open source systems, which should be granted exceptions. Obligations to comply with mandatory requirements should lie with the legal or natural person building on the open

source tools, as they control the purpose and use of the AI system, and in most cases the open source tool provider will not even be aware of its use. Imposing the obligations on the providers of open source tools would disincentivize making them available, which would hinder innovation.

Furthermore, it would be beneficial to clarify that the publication of pure research that touches upon prohibited (e.g. subliminal manipulation) or high-risk AI systems (e.g. deepfake detection, medical applications, emotion detection) is permitted without restrictions and does not qualify as "placing on the market" or "putting into service."

Transparency requirements

We support the minimum transparency obligations for lower-risk applications. People have the right to know when they are interacting with an AI system.

Nevertheless, we would welcome additional clarity with regards to the transparency requirement in relation to the use of AI systems with clients. Transparency should only be required where the client is interacting directly with an AI application (as set in article 52), and not be required when there is no direct interaction, such as e.g., to process the client's business or request.

Moreover, regarding transparency requirements on high-risk AI systems as established in article 13 it is important to ensure that the amount of technical information to be provided with regards to capabilities, limitations and performance of the system does not conflict with intellectual property rights and trade secrets.

Standards and conformity assessment

We welcome the process proposed for companies to use harmonised standards and conformity self-assessment on some of their products. These mechanisms for the European market have proved to be successful in driving innovation and developing and making safe and trusted technologies available to the EU market. Also, the infrastructure with conformity assessment bodies is well established and efficient.

Hold providers, deployers and users to feasible standards. As currently phrased, certain requirements of the regulation will be extremely difficult or impossible to meet in practice (e.g., the Art 10(3) requirement that datasets be "free of errors and complete" demands a level of perfection that is not technically feasible).

We do not disagree with the spirit of the requirements, but they should be composed in a fashion that reflects feasible, best practice standards.

Enforcement

Regarding the enforcement of this Regulation, in order to ensure a level playing field, we think it is important to ensure a harmonized application regardless of the type of company providing/using the high-risk AI system and the national authority(ies) supervising its application. For that reason, all companies providing/using a high-risk AI application should be subject to the same requirements and the same supervisory expectations.

For instance, in the proposed AI regulation, firms providing creditworthiness assessment / credit scoring systems would be supervised by financial authorities in case they are credit institutions, other market surveillance authorities if they are not banks or even not supervised if they are considered small-scale providers. Although we understand the rationale behind the designation of financial authorities as the supervisors of financial institutions' credit activities, if credit applications are considered high-risk, there is no reason to apply the requirements that are intended to avoid excessive harm on citizens differently depending on the legal form of the firm providing the system.

Moreover, some concepts ('foreseeable risks', 'reasonable foreseeable misuse', 'generally acknowledged state of the art') are vague and some obligations refer to other Union laws intended to protect fundamental rights. This could create legal uncertainty that should be removed in the final text by avoiding the inclusion of terms and legal references that could be interpreted differently by providers, users and authorities. In those cases where some legal uncertainty cannot be removed in the final text, the European Commission should develop guidance or recommendations to ensure supervisory expectations are aligned and understood by providers and users having to meet the legal requirements.

Finally, art 64.1 establishes that "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". Although APIs are a common and secure standard to access data remotely, we think mandating the development of APIs only for supervisory purposes would require large investments without bringing considerable benefits to market surveillance authorities that can always perform their duties on the providers/users' premises.

Consequently, we think that article 64.1 should be redrafted as follows:

"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.~~"