Brussels, 4th of October 2021

Joint Letter on the European Commission's Proposal for an AI Act

As organisations developing and deploying artificial intelligence systems, we welcome the opportunity to share our thoughts on the European Commission's proposed AI Regulation. This is a unique opportunity to build together a future-proof, enabling and effective AI governance, with a view to unlocking innovation and increasing the level of trust of European citizens in AI technologies.

To guarantee a vibrant European environment for AI, all AI actors in scope of the regulation need to be given legal certainty, coupled with clear, proportionate, and actionable requirements for the operation of AI systems in diverse settings. This will require a balanced approach, considering the capabilities and specificities of businesses of all sizes, in striving for coherent rules and supervision, and creating avenues for innovation in Europe.

For this reason, we welcome the risk-based approach that the European Commission has taken. To ensure in-scope organizations can feasibly comply with this regulation, we propose the following:

1. Providing a precise definition of "artificial intelligence" and clarifying roles

Currently, the definition of AI is extremely broad, encompassing commonly used tools and processes utilized by most software companies, such as "statistical methods". This, combined with the broad issue areas designated as "high-risk" in later sections, significantly increases the scope of this regulation beyond AI-specific risks, and would ultimately lead to vast legal uncertainty associated with compliance. We recommend revisiting this definition and clarifying the distinctions between AI, deep learning, algorithms, automated processes, and "traditional software". This would provide much-needed clarity, not only for large companies utilizing complex technologies, but for SMEs as well, particularly those that have recently invested in digitalizing operations or have introduced technologies to improve the efficiency of their otherwise non-technological services. More broadly, to achieve effective risk-management, the regulation should ensure that requirements reflect clear outcomes that need to be achieved rather than focusing on how they should be achieved.

In the same vein, there is generalised uncertainty about the roles and responsibilities of the different actors in the AI value chain, namely developers, providers, and users of AI systems. Most of the obligations related to high-risk systems are broadly defined, which does not sufficiently distinguish between the specific roles of these actors and ends up placing the main compliance burden on providers. This is particularly challenging for companies providing general purpose APIs or open-source AI 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 of compliance (e.g., an open deep fake detection API used by law enforcement). In these cases, the AI providers oftentimes do not have knowledge nor means to fulfil the obligations in the AI Act proposal.

The proposed requirements appear, therefore, impracticable and even unrealistic, presenting a real risk for compliance, and we believe they should be refocused to consider technological characteristics.

Clarifying roles and allocation of responsibilities between stakeholders would also be beneficial in addressing people's expectations and the societal context of use of AI

applications, in line with the will of the European Commission to mitigate high-risk and protect fundamental rights.

2. Redefining “high-risk” based on the measurable harm and potential impact

The European Commission utilises the concept of “safety component” in the determination of the level of risk of an AI system, but the proposed definition is open to interpretation and remains a source of uncertainty for the qualification of “high-risk” AI systems. Not only does this potentially conflict with the substantial regulation that already exists in the safety and fundamental rights space, but it would also affect the further development of any AI innovations. To avoid such high cost misinterpretations penalising non-risk AI applications, the AI Act should clarify that the references to "safety components" leverage EU harmonised legislation to ensure alignment with relevant essential requirements. While we agree that safety regulation is critical and a key pillar of consumer protection, we recommend that this Act focus on the specific outcomes that would threaten personal safety, health and fundamental rights and therefore be considered high-risk rather than unilaterally designate safety components as high-risk triggers.

We would also like to request greater clarity in the text regarding the European Commission’s decision to classify the use of AI in employment-related activities, such as “task allocation,” as high-risk. Today’s digital marketplaces rely on the use of algorithms and AI to create vital earnings opportunities and serve consumer needs in real-time. Therefore, we believe the European Commission should evaluate whether the benefits of restricting this use case of AI, and others that are fundamental to online marketplaces, outweigh the costs of restricting access to flexible work.

As drafted, the AI Act’s post-market monitoring obligations appear to fall almost entirely on providers. Although apparently modelled on the EU’s safety framework, this approach is not well suited to AI services, since suppliers of AI services often will have no visibility into how their customers deploy these services into their own systems, and in many cases, would need to work with customers to address any risk that might arise in specific deployments.

3. Ensuring harmonization with existing data, safety, and consumer protection laws

Specifically, the European Commission should identify and build upon existing requirements set by the General Data Protection Regulation (GDPR), the New Legislative Framework (NLF) and other specific sectoral legislation, such as the General Product Safety Regulation (GPSR), with which existing AI systems already need to comply with. Failing to do so would entail a significant risk for operators who will be subject to conflicting obligations. Certain legal discrepancies might create confusion for operators of current systems and will most likely jeopardise enforcement efforts.

By association, we would advocate for the greatest degree of harmonisation possible between the supervisory authorities in charge of AI, which in the current draft, risk fragmenting along national and sectoral lines. AI operators should ultimately benefit from a uniform and consistent legal application throughout the Single Market, enforced by market surveillance authorities whose competence should be strictly limited to verifying compliance and resulting from the typical regulatory process. This point extends to the use of regulatory sandboxes, the inclusion of which is a welcome addition to the proposal, but innovators taking advantage of this legal mechanism must have the certainty that the rules underpinning them are sufficiently clear and applied uniformly across the Union.

4. Ensuring feasibility of legal requirements

Certain requirements for the high-risk AI applications are problematic as currently phrased. For instance, ensuring that training data is “complete” and “free of any errors” is an impossible standard and should be reframed as ensuring “best efforts” or abiding by “industry standards”.

Similarly, a requirement to reveal a source code for market surveillance purposes is not proportional as it is currently phrased. We strongly disagree with this and believe that source code should be protected by the Trade Secrets Directive.

With the enhancement of legal certainty and clear, proportionate and flexible requirements, we are convinced that the AI Regulation has the potential to incentivise further development and innovation in this field in Europe, for the benefit of citizens and AI operators alike.

We therefore look forward to continuing to work with the co-legislators and the European Commission to ensure the right balance is struck on this important and increasingly societal issue.

AFNUM - Alliance Française des Industries du Numérique; CCIA - Computer and Communications Industry Association; CIPL - Centre for Information Policy Leadership; DPE - Delivery Platforms Europe; EEA - European Enterprise Alliance; Free Trade Europa; ITIC - Information Technology Industry Council; Move EU - The European Association of On-Demand Mobility; Plattformsföretagen - Platform Economy; ZPP - Związek Przedsiębiorców i Pracodawców - Union of Entrepreneurs and Employers