CEE Digital Coalition's call to enable innovation in the EU through sensible AI regulation

Embracing AI technology is key for the European economy and opens up a unique chance for more growth in the rapidly evolving digital landscape of Central and Eastern Europe. However, to make the most of this opportunity, we need to make sure we establish a sensible regulatory framework for AI in the European Union. As members of CEE Digital Coalition, an informal gathering of digital and advanced technologies industry organizations from Central Eastern Europe, we would like to propose our recommendations for the remaining stages of the interinstitutional trilogue negotiations concerning the Regulation of the European Parliament and of the Council laying down harmonized rules on Artificial Intelligence (AI Act).

We want to stress our alignment with the Commission's perspective on advancing AI technology. We fully support the goal of boosting research and industrial capabilities while prioritizing safety and fundamental rights of European citizens. Nevertheless, we would like to propose recommendations to prevent stifling innovation by the regulatory framework. We also advise against introducing abrupt changes to the AI Act at this stage of negotiations without impact assessment and consultation, as this could inadvertently affect AI providers, deployers, and users.

As members of the CEE Digital Coalition, we believe that the emphasis in regulating AI should be put on safeguards that do not hinder its positive applications. Similar to other technologies, the primary risks tied to AI arise from its application, not the technology per se. Consequently,

we endorse AI regulation that is risk-based and neutral towards specific technologies. The aim should be to strike a balance where industries and users can enjoy the socio-economic advantages of AI while safeguarding our citizens. To achieve this, we offer the following recommendations for the remaining parts of the trilogue negotiations.

We urge co-legislators to dismiss the proposed asymmetric obligations, particularly for foundation models, general-purpose AI (GPAI), and generative AI. These categories should not be subjected to intricate, multi-level frameworks lacking clear definitions.

- While we welcome the rejection of the proposed tier for 'general-purpose systems at scale,' we encourage co-legislators to also decline the additional tier for the so-called "high impact" foundation models. Additionally regulating GPAI using foundation models is redundant, considering that existing regulations already cover these models used in high-risk cases.
- Criteria like computing power, training data, or number of users aren't suitable measures of risk. Assessing risk using these criteria creates regulatory gaps, allowing bad actors to exploit the framework by creating smaller but harmful applications. The shortcomings become more apparent with advancements in algorithms, enabling sustained performance with less processing power. Even with regular threshold updates, there's a risk of overlooking models that pose a threat despite being below the threshold.
- The multi-tier approach adds unnecessary complexity, inflates compliance costs, and stifles innovation in the EU without offering additional safeguards. AI risk assessment should be grounded in real-world performance rather than technical specifications.

The AI Act should not mandate pre- and post-marketing external testing and the transparency requirements should be applied with caution.

- Assessing the risk of foundation models is crucial and can be accomplished through various methods, e.g. internal red-teaming. However, a one-size-fits-all approach is impractical and ineffective, especially when demanding external testing before and after marketing, irrespective of the risk level. This requirement also introduces a potential risk to sensitive data, like trade secrets, and should only be considered as a last resort.
- Regarding transparency, it is essential to ensure the effectiveness of technical measures (e.g. watermarks, labels) in building trust in AI before their implementation. As technical solutions for AI transparency are still in the early and experimental stages, enforcing rules should be voluntary for the time being.

Prohibitions should only include specific use cases. Imposing broad bans may inadvertently hinder the beneficial applications of AI technology.

- A broad prohibition on biometric identification (BID) could impede valuable uses, like identifying harmful online content or enhancing product accessibility for users with disabilities.
- The prohibition of BID should include only specific BID applications by public institutions, clarifying that exemptions extend beyond "one-to-many" verification. The Parliament's suggestion to ban all BID in public spaces might inadvertently restrict private entities from using BID for purposes unrelated to mass surveillance. It is also

not clear whether the prohibition applies to private entities and if the exemption for BID used for verification is limited to systems allowing one-to-one verification. These aspects should be clarified to avoid legal ambiguity.

- The proposed ban on inferring emotions is overly broad and lacks evidence or risk analysis. This prohibition could impact safe and beneficial AI applications in the workplace, such as coaching tools and sentiment analysis for enhancing employee and customer satisfaction. The definition of emotion recognition requires clarification, and we endorse the Presidency's proposal to exempt AI used for safety reasons, preserving positive use cases like coaching and efficiency gains. Moreover, the prohibition of positive use cases that boost employee or customer satisfaction should be excluded.
- We urge co-legislators to reject the proposal banning the categorization of persons. While acknowledging the need for precautions to protect citizens from the harmful categorization of individuals, the prohibition proposed by Parliament is excessively broad and it may impede beneficial AI applications, such as enhancing accessibility.

The high-risk classification should only apply to clearly defined use cases presenting real risks. The risk associated with AI systems is contingent on their context and usage, it's not an inherent trait. The EU should uphold its risk-based and technology-neutral approach by designating only clearly defined use cases posing actual risks as high-risk.

- The high-risk classification should only apply to "remotely" applied biometric identification (BID), excluding "one-to-many" verification, biometric-based data, and inferences. The majority of AI in BID serves everyday purposes or entertainment and is not utilized in sensitive areas. It's crucial to differentiate BID involving user interaction from mass surveillance, as verification systems often serve multiple users, such as family members utilizing a voice assistant for personalized features. The Parliament's proposal, however, broadens the high-risk BID category to include "inferences" and "biometric-based data," encompassing a wide array of use cases indirectly linked to biometric data.
- Performance and behavior monitoring based on personal traits should be explicitly excluded from the list of high-risk use cases, as the current wording lacks clarity. The predominant use of AI in the workplace is not harmful and, in many instances, it enhances safety, and efficiency, and focuses on general workplace processes rather than individuals.

We strongly recommend that co-legislators reject the Parliament's proposal to designate AI used in recommender systems by very large platforms as high-risk.

- The Digital Services Act already mandates these platforms to conduct comprehensive risk assessments and mitigation measures, encompassing AI in recommender systems and potential harm to fundamental rights. Introducing additional risk assessments under the AI Act would be inconsistent and impose unnecessary burdens. Moreover, the proposed emphasis on very large social media platforms is misleading and unjustifiable, considering the horizontal nature intended for the AI Act.

As members of the CEE Digital Coalition, we call upon the co-legislators to aim at establishing a cohesive legal structure for artificial intelligence in Europe. This framework is crucial for fostering the continued advancement of innovative AI technology and positioning Europe as a frontrunner in AI research and development. The realization of the full benefits of this

transformative technology is contingent upon having a regulatory environment that is both clear and predictable.

AAVIT - Association for Applied Research in IT (Czechia)

American Chamber of Commerce in Bulgaria (Bulgaria)

ANIS - Employers' Association of the Software and Services Industry (Romania)

Anthill (Bulgaria)

APDETIC - Association of Producers and Dealers of ICT (Romania)

Digital Poland Association (Poland)

DNA - Digital National Alliance (Bulgaria)

F27 (Bulgaria)

INFOBALT (Lithuania)

ICT Association of Slovenia (Slovenia)

ITAS - IT Association of Slovakia (Slovakia)

IVSZ - IT Association of Hungary (Hungary)

SAPIE - Slovak Alliance for Innovation Economy (Slovakia)