ARTIFICIAL INTELLIGENCE ASSOCIATION OF LITHUANIA

Feedback on public consultation on
“Artificial intelligence – ethical and legal requirements”

Artificial intelligence association of Lithuania supports the European Commission’s proposal for the EU Artificial Intelligence Act (AIA).

Firstly we support the need for transparency for non-high-risk systems, for example chatbots which lead a user to believe they are interacting with a human being. Second, we support the effort to follow the guidelines to ensure AI will be created by ensuring the European Union values, fundamental rights and principles. Having said this, we express a few areas to consider.

- Provide more details on regulators. Since the fines are presented in the AIA. We are concerned that there is missing information about the regulators and guidelines on how and what will be responsible in each country to enforce article 5 and 10. Also, which institutions will be the ones to help for all stakeholders for the consulting on whether the application falls within high-risk or even prohibited applications. Without the self assessment protocols, self standardisation, the current AIA might become an insurmountable obstacle for SME and startups, to follow and ensure all guidelines mentioned in AIA.
- Expand definition of 'internal control'. Common practice is that AI solutions are used not only in border controls, airports, but also by migration departments, foreign offices, criminal law enforcements, shops, self checkout shops and other commercial uses. Current exception for 'internal control' is limiting all other applications, which should fall under the mentioned definition.
- Improve statement (33) "Technical inaccuracies of AI systems intended for the remote biometric identification of natural persons can lead to biased results and entail discriminatory effects. This is particularly relevant when it comes to age, ethnicity, sex or disabilities. Therefore, ‘real-time’ and ‘post’ remote biometric identification systems should be classified as high-risk. In view of the risks that they pose, both types of remote biometric identification systems should be subject to specific requirements on logging capabilities and human oversight."
  Is technically false and should be revised. For example the fingerprint recognition, which can be run by touchless photo scanner, can produce the accuracy significantly higher than any human. However such a system would fall under remote recognition if it is touchless, and biometric since fingerprint is biometric data. We recommend, additional statement "Technical inaccuracies of AI systems intended for the remote biometric identification of natural persons can lead to biased results and entail discriminatory effects, if not certified otherwise (ex. NIST evaluations)".
  https://www.nist.gov/itl/iad/image-group/minutiae-interoperability-exchange-minex-iii

- Ensure that no fragmentation between SME and Large Enterprises will be encouraged. Firstly the responsibilities and infrastructure burden should be proportional. The SME or even a startup, might end up near a steep wall of regulations, before being able to create the solution and attract the funding, if the regulations will involve non-only final product services, but also the process of prototype and research stages. Secondary, the creators of general-use AI systems, have rarely are able to control the usage of technology in final stages of application, for example, the technology of object detection and service to learn to detect objects in images without the programming leads to unlimited number of applications from detection cancer cells in tumor, to detecting guns/war equipment in satellite images. And the creator of object detection technology, can not control on which data the technology will be used in the final application. In such we support the separation of the creator of technology, and the final integrator of application.

- Incorporate the self testing capabilities or general guidelines to follow. We agree, that some guidelines for standardization and testing should come as insurance tool, but Hold providers, deployers and users to feasible standards. As currently phrased, certain mandatory 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). Especially, when for example in the medical diagnosis field, the AI solutions with 80-90% accuracy might be significantly better than expert doctors. We suggest following the widely known independent training/validation/testing pipeline, which should be followed by best practices used in the AI community.

- The clear explanation of definitions “safety components” and “significant changes” and similar should come to place. There may be multiple collisions and fragmentation between the countries implementations of AI systems testing and tracking products, if there are no clear definitions. This is critical when talking about the scope of requirements for high-risk AI systems.