August 4, 2021

Developers Alliance's position on the European Commission's proposal for a regulation on Artificial Intelligence (AI Act)

{DEVELOPERS ALLIANCE}

Founded in January 2012, the Developers Alliance is a global industry association that supports software developers as entrepreneurs, innovators, and creators.

DevelopersAlliance.org

policy@developersalliance.org

1. General Remarks

We commend the objectives and the risk-based approach of the Commission's proposal. We call on the EU co-legislators, however, to address a series of critical issues so the regulation will be fit for purpose and to reduce the competitive disadvantage for European developers:

- **set legally clear definitions and limit the scope to clearly defined high risk use cases of AI, in line with the declared objectives of the regulation,**
- **provide clear and reasonable rules for high risk use cases of AI, focused on the deployment phase, and less preemptive requirements for the development phase when the intended purposes might not be obvious (as in the case of general-purpose and open-source AI solutions),**
- **ensure reduced regulatory burdens for startups and SMEs and set up a solid framework for regulatory sandboxes as incentives for innovation and entrepreneurship,**
- **remove the proposal's extraterritorial reach to avoid potential barriers to trade on products and services created outside the EU that contain no AI themselves,**
- **recognise that AI systems are by definition modelled on human decision making, with all their weaknesses and strengths. Holding AI to an absolute standard where an equivalent human process is viewed under a reasonableness standard is legally inconsistent.**

The classification of 'high risk systems' in Title III, together with the general architecture of the legal requirements and the enforcement mechanism, set a regulatory regime which covers inception and early development phases of highly innovative technological solutions when use cases are not always obvious. An AI solution could, at the same time, be deployed under 'high risk' circumstances but be a low-risk application. The preemptive effect of such measures will have a negative impact on the ability of European developers to innovate and will drive them outside the EU.

2. Scope and Definitions

Definition Of AI

The AI Act should regulate clearly defined high risk uses of AI, and not software and technology as such. Moreover, the regulation should not focus on regulating AI as such, but on the particular circumstances and use-cases of AI where strict rules should be applied.

The definition of AI should be narrowed to what is generally considered AI within the industry. It should not capture general-purpose software or conventional computational and statistical methods (e.g. basic linear regression).

We understand the EU's intention to regulate AI as an advanced technology which raises risks associated with certain uses, with a focus on significant risks to the health and safety or fundamental rights of persons. Therefore, a legal definition of AI, for the purpose of this regulation, should be strictly limited to the declared policy objectives. Simple algorithms and unsophisticated computational methods, besides falling outside the category of advanced technologies, have been used for a long time and are not suddenly raising concerns that justify special rules.

We find disproportionate the policy option to complement the definition in art. 3.1 with a detailed list of approaches and techniques for the development of AI, particularly if they are to be updated by the Commission without clear criteria. This could be a source of legal uncertainty for AI developers and other industry participants.

AI systems/AI applications

From a semantic and technical perspective, but also for legal clarity and certainty, the term "AI systems" might not clearly reflect the scope, as it seems that the regulation is intended to cover AI applications.

AI capabilities that meet the proposal's definition are already widely - almost universally - deployed. They are often a very small part of a "system" whose purpose is essentially unrelated to the AI component (for instance educational software that suggests new courses based on a student's interests).

AIaaS and OSS

The scope of the obligations should be clear in relation to general-purpose AI solutions (so-called 'off the shelf' AI or AI as a Service - AIaaS) and open-source software (OSS).

It is impossible for the developers of AIaaS to anticipate and monitor all the use cases and therefore to identify and comply with AI Act requirements. Under the proposal, developers that use these services would either need to code their own AI engines for the targeted software they are trying to create (an inefficient market outcome), or AIaaS companies would need entrepreneurs to fully disclose their ideas before using AIaaS toolkits to avoid regulatory liability themselves.

As previously mentioned in our position on the AI White Paper, in the open-source development environment it is also often impossible to identify a single developer or group of developers as the unique creators of an application, as usually, the code is subject to multiple iterations over time by many authors. The developers that wrote the reusable code in an open-source repository cannot be aware of how that piece of code will be further developed or used to build various AI applications. Subsequent users cannot be completely aware of all the details of the open-source code they incorporate.

Finally, for legal certainty, it is imperative to specify when legal requirements are applicable for AI solutions. We suggest a clarification and a better alignment of the definitions "placing on the market", "making available on the market" and "putting into service". In the same vein, the definition of "provider" should also be adjusted, as it is not clear what exactly "developed with a view to placing it on the market" means.

{DEVELOPERS
ALLIANCE}

Founded in January 2012, the Developers Alliance is a global industry association that supports software developers as entrepreneurs, innovators, and creators.

DevelopersAlliance.org

policy@developersalliance.org

Safety Component Of A Product Or System

The definition of the term “safety component”(art. 3.14) should be aligned with the definition proposed for the revision of the Machinery Directive, which refers only to “failure or malfunction which endangers the safety of persons”, but not of property.

Dual-Use AI

The exception from the scope of the regulation provided by art. 1.3 (“AI systems developed or used exclusively for military purposes”) is inadequate. It is not always obvious during the development phase how certain AI capabilities will be deployed. Given the dual-use nature of technology, even if the initial intended purpose is for civil use, later the AI capability could be used and deployed for military purposes. Further, there are areas of military application of AI beyond autonomous weapons, from logistics and transportation and data information processing and predictive analytics to cybersecurity. While we recognize the legislator's intention, we note that from a practical perspective it is impossible to have a clear-cut delineation. The regulation’s impact on the EU’s defence capabilities should be considered.

Problematic Extraterritorial Approach

The extraterritorial approach raises potential trade barriers, because of the expansion of EU requirements not only to AI applications to be imported into the EU but also to products and services created outside the EU using AI (but that contain no AI themselves). Apart from international trade issues, it is unclear how such an extended scope could be enforced, or even how foreign AI could be reviewed and assessed. Moreover, it will deprive European consumers and businesses of the benefits of useful products and services utilizing AI. We strongly recommend the deletion of the provision of art. 3.1 c) “providers and users of AI systems that are located in a third country, where the output produced by the system is used in the Union;”

Correlation With Other Legislation

The regulation should offer more consistency with other applicable legislation, for legal certainty and predictability.

The scope of the regulation clearly overlaps with other legislation (e.g. medical devices, employment), which already provide solid regulatory and compliance frameworks addressing similar risks for health, safety and security of persons. It would have been more appropriate to review those particular sectorial pieces of legislation to address additional risk cases which might not be covered; such an approach would have covered those practices using artificial intelligence listed in Titles II and III of this proposal.

Some measures are meant to ease the overlapping burden - for example, a single declaration of conformity (art. 48.3) for those AI applications subject to other EU harmonisation legislation. Nonetheless, there are areas where the interplay between the current conformity assessments and the additional layer of complexity of the AI Act will prove to be quite challenging in practice, especially with regard to the results of overlapping conformity assessments and the way they should be reflected in the declaration of conformity and the decisions of notified bodies. On top of this, the GDPR’s Data Protection Impact Assessment (DPIA) could be in conflict with some conformity requirements (e.g. art. 12 on record-keeping).

In the case of AIaaS APIs which are designed to be repurposed, changed and configured, the same application might fall under different harmonized legislation, depending on the deployers’ choices. The regulation should provide the necessary legal flexibility in this sense. A solution would be to exclude general purpose and open source solution providers from the obligation of specific “high risk” conformity assessments (as the obligations should fall on deployers), in addition to other requirements of EU harmonization legislation.

Definitions such as “safety component of a product or system” (as mentioned above), “putting into service”, “instruction for use” or “substantial modification” should be correlated with those proposed for the revision of the Machinery Directive.

3. Prohibited AI Practices

Software developers are deeply committed to building trust in the products they develop and therefore we acknowledge the EU lawmakers’ consideration to restrict those AI applications that cause severe harm to fundamental rights of citizens, such as mass surveillance and social monitoring applications.

However, “subliminal techniques” or “materially distorting” a person’s behaviour” should be clearly and narrowly defined. We recommend avoiding beneficial/inoffensive use cases and focus only on clearly harmful practices, with a significant impact on persons’ health and safety. In general, AI techniques are drawn from observations of how humans process and react to information, and as such have no more ability to distort behaviour than a skilled human operator does. Proposals designed to safeguard people’s behaviour should thus apply equally to human and AI operators.

4. ’High Risk AI Systems’

Classification

All the legal obligations relevant for “high risk” use cases should be applicable from a certain point in the development phase or in the deployment phase when the “intended purpose” is obvious. Small scale experimentation and iteration should be excluded.

We are concerned by the unintended impact on AI applications which do not pose any risk of physical or psychological harm at all, but fall into the category of ‘high risk” regardless. There’s no clear mechanism for a developer to determine whether their work might lead to a “high risk” application, as the option to make reference to Annex II and III is not feasible. For example, there is a broad description of the use cases listed in Annex III, points 1, 3 or 4, which could lead to unintended capture of AI solutions which do not pose a “high risk” in accordance with the objectives of the regulation.

We strongly recommend revising the description of “high risk” areas listed in Annex III, taking into consideration the level of human oversight. Those systems where the decisive elements or the final decisions belong to humans should be excluded. For example, simple AI recommendation applications (where the actions are taken by the system’s owners), or those that are only complementary parts of decision-making systems, should not be considered high risk. The “high risk” assessment should be focused on particular use cases, explicitly described, instead of general classifications or even entire sectors. This will provide legal certainty and predictability for AI developers.

Finally, we would observe that in those systems where AI is used to make decisions that mirror those of a smaller scale or more limited human system, a reasonableness standard is more in keeping with the baseline liability of the activity.

Requirements

With regard to the risk assessment system (art. 9), the provisions should clearly specify the risks that need to be considered. In this sense, art. 7 provides the following: “whether an AI system poses a risk of harm to the health and safety or a risk of adverse impact on fundamental rights…”. Similarly, certain recitals reflect the regulatory intention to capture those AI applications with a significant impact on the health and safety or fundamental rights of EU citizens.

Some of the proposed requirements are quite detailed and prescriptive, while some are ambiguous and others even unrealistic. Art. 10.3 contains the best example for the latter: “Training, validation and testing data sets shall be relevant, representative, free of errors and complete.”

The essential requirements should be technically feasible and legally reasonable. Also, they should offer only the principles and related main elements for the conformity assessment, as they are applicable to a large and diverse category of applications. The details should be contained in harmonized standards or common specifications. This will also allow the flexibility to ensure compliance depending on the type of application, the intended purpose and use case, but also the business organisational structure and strategies.

On dataset requirements, clarification is required where third party datasets are used. This is quite common, as developers often use publicly available datasets or datasets provided under different contractual terms. Exemptions or simpler conditions should be specified for these situations.

The interplay with GDPR requirements (art. 10.5) should be further assessed from the perspective of different techniques used by AI developers (e.g benchmarking, differential privacy), usually to test systems performance and to address biases and ensure privacy. A similar observation can be made with regard to record-keeping requirements (art. 12), which could go against data minimisation and other principles imposed by the GDPR.

The requirements proposed in art. 10.2 should make reference to unacceptable or harmful bias. Certain datasets are intentionally ‘biased’, depending on the intended purpose of the AI application (e.g. a medical device for certain category(ies) of patients).

The requirements for technical documentation (art. 11 and Annex IV) are excessive, especially for small developers. The requirement to provide “a description of any change made to the system through its lifecycle” (point 5 of Annex IV) is impossible to meet before actually placing it on the market or putting it into service, and should be removed.

The transparency requirements (art. 13) are impossible to meet in the case of general-purpose AI solutions, which once again demonstrate the need to shift many requirements to the deployment phase for AIaaS, as previously mentioned.

The proposed requirements for human oversight (art. 14) are overly prescriptive and unreasonable (humans to “fully understand” an AI system). Same observation on the relevance of the deployment phase in the case of AIaaS.

Concerning the specifications for accuracy, robustness and cybersecurity (art. 15), these should be circumscribed by a ‘reasonable expectation’, in correlation with the product safety and liability legislation. The deployment phase is more relevant for a large part of these conditions. Also, these obligations are impossible or very difficult to be met in the case of AIaaS.

It is unclear if the quality management system (art. 17) could be covered by current standards (e.g. ISO 9001), which are already applied by companies, including SMEs.

5. Conformity Assessment and Certification

We welcome the application of the principle of self-assessment and declaration of conformity for high risk AI systems but reiterate the need to adapt the conformity assessment obligations for AIaaS and open-source AI solutions.

The obligation to subject AI systems to a new conformity assessment whenever they are ‘substantially modified’ (art. 43.4) should be further clarified, together with the circular definition provided by art. 3.23. AI developers need to know precisely when specific actions or changes would trigger a new conformity assessment.

Regarding harmonized standards (art. 40), we underline that they should be market-driven and voluntary. Their availability when the regulation will come into force is uncertain. Enacting a regulation before standards are agreed by relevant industry sectors is an unwelcome situation. However, harmonized standards represent only one option to benefit from the presumption of conformity.

In the case that the common specifications are envisaged (art.41), the development of such specifications should involve industry stakeholders. We would point out that, in accordance with the New Legislative Framework, specifications are also not mandatory and thus art. 41.4 should properly reflect this.

We note that the presumption of conformity is a 'benefit' and not an obligation for economic operators, as specified by the ECJ ruling in the James Elliott Case C-613/14 (para 38).

Guidelines, best practices and ethical principles, developed and applied by important global companies developing the most advanced AI solutions and investing in AI research are already available. These practices are usually followed by the developer community, including open-source AI developers.

The regulation should specify the necessary flexibility to comply with the essential requirements for 'high risk' use cases of AI, by following other industry best practices, as well international standards (to the extent that these are available).

6. Transparency Obligations

Information and transparency provisions must be balanced against the confidentiality of trade secrets and incentives to innovate new advanced AI solutions.

We note the importance of confidentiality obligations for market surveillance authorities, which will have full access to datasets and source code (art. 64.6 and art. 70).

7. Reducing The Regulatory Burden For Startups and SMEs

We support a harmonized EU framework for regulatory sandboxes in the EU, in support of innovative startups and SMEs. The AI Act should provide the use of experimentation clauses as the legal basis for regulatory sandboxes, as requested by the Member States in *Council Conclusions on Regulatory sandboxes and experimentation clauses as tools for an innovation-friendly, future-proof and resilient regulatory framework that masters disruptive challenges in the digital age*, adopted on November 16, 2020.[1]

The conditions for participation in regulatory sandboxes should encourage greater participation and thus should be specified in a less restrictive way. The regulatory sandboxes should be framed for enhanced collaboration between the participating companies and relevant authorities, with a view to more effective, fit-for-purpose and future-proof regulatory responses.

In addition to the measures listed in art. 55.1, we suggest a specific provision on the consultation of representative organisations of small scale providers and their involvement in the development of relevant standards.

The provision of art. 55.2 should provide a strong legal base and incentive for national competent authorities to apply reduced fees and even exempt small-scale providers from paying certain fees.

8. Governance and Implementation

Legal certainty and predictability are prerequisites for a stable framework which will enable investments and widespread use of advanced AI technology. In this sense, the delegation powers that are specified by art. 73 are inappropriate.

[1] " 9. Understands experimentation clauses as legal provisions which enable the authorities tasked with implementing and enforcing the legislation to exercise on a case-by-case basis a degree of flexibility in relation to testing innovative technologies, products, services or approaches. Notes that experimentation clauses are often the legal basis for regulatory sandboxes, and are already used in EU legislation and in many Member States' legal frameworks."

The governance and effective implementation of the regulation highly depends not only on transparency and due process, but also on adequate expertise and resources of the relevant authorities, both at EU and national levels, considering that the AI applications falling into the scope are highly advanced technologies.

The work of the European AI Board should be supported by continuous industry input, especially on matters related to technical specifications and harmonized standards (art. 57 and 58).

We recommend one-stop-shop access at the Member States level for companies, which will be highly beneficial especially for startups and small scale providers. These should also provide special guidance on compliance.

The obligations for post-marketing monitoring (art. 61) are very burdensome for small scale providers and providers of AIaaS. In any case, these obligations should be reasonable for any type of provider, as in the case of AI-embedded systems in products sold at a large scale it is very difficult or even impossible to monitor and collect the necessary data.

The deployers of AI solutions classified under ‘high risk’ use cases should be the main subjects of the obligation to report serious incidents of malfunctioning. The developers of AIaaS could be informed and involved in further stages of the process.

We welcome the Commission and Member States’ support of codes of conduct, as reliable sources of best practices and effective tools for compliance.

We are concerned about the level of the proposed penalties and administrative fines, which could be disproportionately imposed on startups and SMEs, especially the latter. These will act as a supplementary disincentive for startups and SMEs to develop and utilise advanced AI solutions in the EU.