VERBAND DER INTERNETWIRTSCHAFT E.V.

POSITION PAPER

eco Position Paper on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts 2021/0106(COD)

Berlin, 07.07.2023

With the AI Act, the European Union wants to create the world's first comprehensive legal framework for the regulation of AI systems. The Commission is following a risk-based approach in its draft published in 2021. This means that the requirements for AI systems should be proportionate to the risk in the respective areas of application. For this purpose, the Commission's proposal defines various use cases that are considered high-risk. In addition, the regulation also bans certain practices altogether.

eco supports the Commission's risk-based approach. AI systems hold great potential for economic contributions, science and society, which is why it is important, also in terms of Europe's innovative capacity, to support the development of such systems and to accompany them from a regulatory perspective in order to create legal certainty. At the same time, it is also necessary to address the potential risks in order to create confidence in the technology. The right balance between justified regulations and the promotion of innovation is important. We have already made this clear in our position paper on the Commission's draft.

Both the European Parliament and the Council of the European Union have now set their negotiating mandates for the trilogue negotiations. eco would like to take this opportunity to point out relevant points which, from the point of view of the Internet industry, should be further considered in the negotiations.

1. On the scope of application

The scope of the regulation is largely determined by the definition of the term "AI". Both the Council and the Parliament have now made changes to this definition. In its report, the Parliament proposes to align the definition with the OECD's short definition. We welcome this step, as we believe it is important to find a definition that is internationally compatible. It remains to be noted that this is currently being renewed and may have to be adapted in the trilogue negotiations.

In addition, the scope of the regulation will be extended by the Council and Parliament. General-purpose AI systems and foundation models are now also to be covered by some of the provisions of the AI Act. Under certain conditions, these systems can also fall into the high-risk category. From the perspective of the Internet industry, an expansion to include general-purpose AI in the scope of the AI

Act can make sense if the additional bureaucracy is kept at a low level. However, we do not support the position that foundational models and general purpose AI (GPAI) are generally high-risk, as this would call the risk-based approach into question. GPAI and foundational models can be used for a broad range of use cases and can be deployed in vastly different contexts. The specific risk relating to a use case will have to be evaluated in the context of that application and the context in which it will be deployed.

2. On the definition of high-risk AI systems

Due to the risk-based approach, the definition of high-risk AI is particularly relevant, as most requirements apply to such systems. In the Commission's draft, the definition of such systems was still very broad, also with regard to the areas of application in Annex III. The Council and Parliament are adapting the corresponding Article 6 and are also making changes to Annex III. In its report, the Parliament proposes an additional level for the classification of AI systems as high-risk. With the additions to Article 6 (2) and 2a, the complexity of the various conceivable use cases can be better taken into account. eco supports the path envisaged by the Parliament in principle but points out that some of the concepts provided for in Article 2 (1), such as "environment" or "health", are very abstract concepts that should be more clearly defined in order to have the desired effect of relieving the burden on AI developers and create a manageable and comprehensive regulatory framework for AI.

The sensitive areas listed in Annex III in the Commission's draft include systems that are used for biometric identification, the categorisation of people or in certain areas of law enforcement. The Parliament is expanding the areas mentioned here, in some cases significantly. eco has already noted in its position paper on the Commission's draft that the use cases in Annex III are defined too broadly and that especially providers of AI systems are confronted with an unnecessarily high bureaucratic burden, along with the associated costs.

The extension may also be problematic in part because, according to Article 4a of the parliamentary report, general-purpose AI systems that could be used in one of the use cases listed in Annex III also fall under the high-risk category. However, this may often be difficult to assess, since such general-purpose systems are – in principle – suitable for a variety of scenarios. In addition to the expected legal uncertainty for the providers of such systems, it is to be feared that the highly restrictive requirements of the AI Act would extend to a large number of such systems as a result of the amendments made. eco fears that the intended regulations will have a negative effect on Europe as an AI location. The association proposes that the obligations for high-risk AI systems only apply to those for which it can be reasonably assumed that they will be used in such an area and that the affected system poses a high risk for the specified protection targets.

The AI Act also affects the so-called "Very Large Online Platforms" (VLOPs), according to the Digital Services Act (DSA). In the parliamentary report, the newly inserted point 8 (a b) in Annex III also includes AI systems that are used on social

media platforms classified as “Very Large Online Platforms” (VLOPs) in the high-risk category. This would result in significant overlaps, as e.g. the use of recommender systems by VLOPs is already extensively covered by the DSA. Providers of VLOPs are required under Article 34 of the DSA to carry out risk assessments to identify systematic risks, like negative effects on fundamental rights and physical and mental well-being or gender-based violence stemming, among others, from the design or functioning of algorithmic systems. Article 35 of the DSA, VLOPs are also obligated to undertake risk mitigation measures and under Article 27 of the DSA providers of VLOPs are also required to publish the main parameters used in those recommender systems, the reasons for the relative importance of those parameters and any options users have to influence those parameters. For these reasons, and to ensure legal clarity, we believe that double regulation must be avoided.

3. On the obligations for providers and users of high-risk AI systems

In particular, in the area of high-risk AI systems, the AI Act includes comprehensive requirements for commissioning or importing that providers, importers or users must fulfil. Some of these were already very difficult to fulfil in the original draft and could mean a lot of bureaucracy for AI companies in Europe and hamper innovation. These include the very comprehensive risk assessment, which can be a hurdle for SMEs in particular. On the one hand, the effort is very high due to the required scope, on the other hand, not all risks can be clearly operationalised. The Parliament and the Council go even further in their positions. Article 13 lays down information and transparency obligations vis-à-vis the user. AI Systems are to ensure full explainability of their decisions for the users. In addition, the Parliament also extends the scope of Article 13 (3). Providers of AI systems are now also supposed to explain which dangers for the environment could arise from the use of an AI system and for which scenarios users should not use it. From the point of view of the Internet industry, it is unclear whether this is possible in all cases. It also remains to be clarified under which conditions complete explainability can be assumed and how trade secrets are protected in this context.

Article 9 creates the framework for the obligations of the providers of high-risk AI systems. These have also been partially expanded compared to the Commission’s proposal. On the one hand, we welcome some additions that should simplify the establishment of a compliant risk management system, such as a restriction to the reasonably foreseeable risks. On the other hand, Article 9 has also been expanded, as the risk management system is extended to include protection goals that are vague and difficult to define, such as equal opportunities, health and the rule of law. Here, the impact on providers can be difficult to assess.

Deployers of high-risk AI systems are also supposed to carry out a detailed fundamental rights impact assessment according to the new Article 29a. There is an urgent need to ensure that the necessary assessments can be operationalised in order to enable the implementation of the provisions.

4. On prohibited practices

In Article 5, the AI Act defines practices for which the use of AI systems is prohibited. Artificial intelligence has the potential to change our society and economy enormously, which is why, from the point of view of the Internet industry, it is imperative to ban some application scenarios for ethical reasons and to protect fundamental rights. eco is critical of the use of AI systems for real-time biometric monitoring in public spaces and continues to reject them. In its approach, the Council creates some exceptions in this regard. On the other hand, the Parliament has tightened up the ban in its report, which we welcome. At the very least, biometric recognition needs strong safeguards. It should only be used in public spaces, if at all, in individual cases and subject to a judge's approval. We also reject the storing of the recordings. However, we believe that exemptions for private authentication purposes (e.g. a facial recognition lock for accessing one's home or an office building) or child safety measures should be provided to safeguard innovation and users' security.

The government's ban on "social scoring" is also appropriate from our point of view, as this can endanger fundamental rights. Nevertheless, from the point of view of the Internet industry, it must be made clear that this ban is limited to those areas where fundamental rights are affected, and no legitimate business models of private companies are affected. The current wording of the Council and Parliament does not make it clear beyond doubt whether, for example, use cases such as the categorisation of customers for personalised offers or measures to assess creditworthiness are affected. Here, a restriction to banning the use of such techniques by state actors would be desirable.

5. On regulatory sandboxes

Promoting innovation is an explicit goal of the AI Act and, in our opinion, should also be a central part of this legislation. The envisaged regulatory sandboxes are an important component for testing AI systems in a protected environment, from which SMEs, in particular, will benefit. We explicitly support this. Access to these sandboxes must be as simple as possible and available to as many businesses as possible. This is particularly necessary in view of the complexity of the AI Act. In addition, we have explicitly positively assessed the possibilities provided for in Article 54 of the Commission draft to "process personal data lawfully collected for other purposes in the AI real laboratory for the purposes of developing, testing and training innovative AI systems in the real laboratory". We believe there is a need to expand the cases in which these regulations apply. In principle, all products that are created in a protected environment of the sandbox should be given this possibility in order to improve the quality of their products. However, the Parliament restricts this in its report. The Council's approach also refrains from extending Article 54 to at least additional use cases Improvements should be made here in order to increase the innovative capacity of the European AI economy and, above all, to support SMEs in complying with the rules of the AI Act. The presumption of conformity provided for in Article 53a (de) is also helpful, as it removes the burden

of proof from SMEs and, therefore, reduces hurdles and bureaucracy for the testing of AI systems.

6. On copyright

The inclusion of generative foundation models, as called for by the Parliament in particular, also moves copyright issues more into focus in the AI Act. Among the obligations included in the parliamentary report for generative AI are disclosure obligations regarding the data used for training. This is intended to allow copyright holders to withhold permission to use material covered by copyright or to charge fees for its use. It is important to emphasise that the files referred to are only used for training and are not copied. Nevertheless, fair compensation that takes into account the value of the data for the finished AI system is important in our view. Overall, however, the existing copyright law must also be more strongly adapted to the digital realities of the 21st century. In contrast, we consider the disclosure obligations created here to be impracticable and support the position of the European Commission, in particular with regard to Article 4 of the EUCD, which allows right holders such as publishers to opt-out of text and data mining remains fit for the purpose.

7. Conclusion

Overall, improvements could be achieved in some areas by Parliament and Council compared to the Commission's draft. Nevertheless, from the perspective of the Internet economy, the balance between bureaucracy and innovation support can still be improved. Furthermore, in our assessment, some of the envisaged obligations are difficult to comply with, which could put an additional burden on the European AI economy, especially in view of the high penalties envisaged. The Parliament is even calling for the penalties outlined in the initial draft to be increased. In order to promote the growth of the AI industry, we propose the following points, which, from the point of view of the Internet industry, should be taken into account in the trilogue negotiations:

- Create a clear scope of application
  In order to avoid undesirable developments and to promote innovation in the field, it is important that the scope of application in the AI Act is clearly defined. In particular, the definition of AI must be internationally compatible and precise so that the regulation can set international standards and European providers are not discriminated against. High-risk AI systems must also be precisely defined so as not to unnecessarily hinder innovation. Here, the exceptions proposed by the Parliament are a good approach that must be continued. There must be no double regulation in interaction with other regulations, such as the DSA.

- Creating realistic requirements for providers and users of AI systems
  In order to create trust in the technology, transparency and monitoring of possible risks, in principle, make a contribution. However, the obligations

provided for in the AI Act, especially for providers of high-risk AI systems, go too far in the view of the Internet industry. In particular, the inclusion of abstract and sometimes difficult-to-define and difficult-to-operationalise terms such as “health” or “environment” in the assessments to be carried out is challenging to implement in practice. Moreover, it is not clear what is meant by “explainable” AI. Clarifications and restrictions to well foreseeable problems and risks are needed here.

- Strengthening trust in artificial intelligence
  The use of artificial intelligence offers many opportunities for business, science and society. However, as with any technology, there are also risks. To address these and create trust in the technology, we advocate a complete ban on biometric surveillance in public spaces and social scoring by the government. At the same time, however, it is important that non-critical and legitimate business models continue to be allowed in order to prevent excessive regulation.

- Promoting innovation and SMEs
  In our view, regulatory sandboxes are an important tool for promoting innovation and supporting SMEs in particular in the development of AI applications. Therefore, access should be as simple and open as possible. The presumption of conformity can also reduce the bureaucratic burden for companies that will arise in the implementation of the Ai Act, which we support.

- Copyright for the 21st century
  The technical developments in the field of AI highlight the need to adapt copyright legislation to the digital age. We believe a full disclosure requirement for generative foundation models is neither practicable, necessary, nor appropriate.

About eco
With more than 1,000 member companies, eco is the largest Internet industry association in Europe. Since 1995 eco has been highly instrumental in shaping the Internet, fostering new technologies, forming framework conditions, and representing the interests of members in politics and international committees. The focal points of the association are the reliability and strengthening of digital infrastructure, IT security, trust and ethically oriented digitalisation. That is why eco advocates for a free, technology-neutral and high-performance Internet.