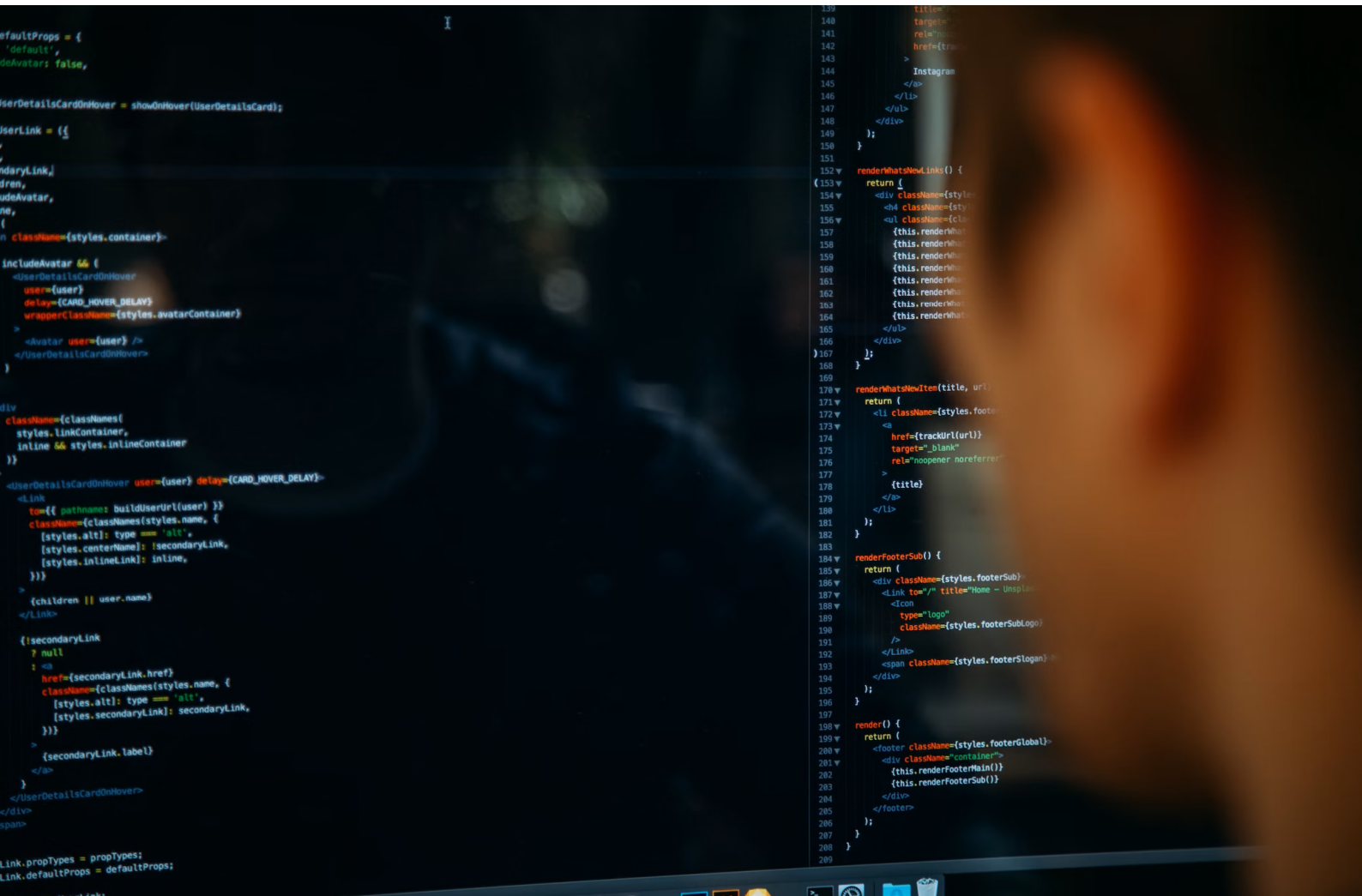
TÜV VERBAND

July 2023

Position Paper

Recommendations for the AI Act trilogue negotiations



Position Paper

Recommendations for the AI Act trilogue negotiations

Introduction

With the Artificial Intelligence Act (AI Act), the European Union aims to become a pioneer in the regulation of AI. The aim is to enable the trustworthy and safe use of AI systems and to ensure the competitiveness of European AI development. The EU Commission published its proposal in April 2021. After intensive negotiations, the Council has agreed its position in December 2022 and the EU Parliament (EP) in June 2023. The joint trilogue negotiations have started and are to be concluded as far as possible under the Spanish Council Presidency.

The TÜV Association has already comprehensively positioned itself on the AI Act during the legislative process. This position paper provides concrete recommendations in order to achieve a robust and effective regulatory framework. In our view, the priority objective of the EU legislator should be to ensure that only safe AI systems are placed on the market, thus strengthening the necessary level of trust of people in AI-based products and systems. Only in this way can a rapid market penetration of high-quality AI systems be enabled, and "AI Made in Europe" become a genuine quality standard and competitive advantage for European companies.

1. Policy objective (Article 1)

- The goal of the AI Act - the introduction of human-centred and trustworthy AI - should be explicitly stated as an overarching objective in Article 1, as proposed by the EP.

  The EP's proposed expansion of the protection goals to democracy, fundamental rights, and the environment is also to be welcomed. The AI Act must consider all risks posed by AI systems and provide for corresponding requirements for providers and users of AI systems to reduce the risks.

2. High-risk classification (Article 6)

- The classification rules proposed by the Council and EP for hig#h-risk AI systems are insufficient, with regard to both physical products in which AI systems are integrated (Annex II) and AI systems which are placed on the market as stand-alone software (Annex III).
- As for physical products, the EU legislators envisage a high-risk classification only if the AI system is used as a safety component of the product and the product is already subject to mandatory third-party assessment. From our point of view, this approach is not sufficient, as new risks may arise from the integration of an AI system into a product. Rather, it is necessary to subject the sectoral harmonization legislation listed in Annex II to a reassessment with regard to the risk potential. A corresponding legal obligation should be anchored in the AI Act.
- In the case of stand-alone AI systems, the EP has added the specific use case as additional qualification criterion for being high-risk. While this addition appears to make sense in principle, the opt-out option for providers envisaged by the EP by means of a notification to the national supervisory authority or the AI Office is to be clearly rejected. There is a risk that AI providers will use this provision as a backdoor to circumvent the mandatory requirements. In addition, the envisaged three-month period for issuing reasoned decisions is expected to pose major challenges for national authorities. In our view, an opt-out option is not necessary if the Commission sufficiently specifies the relevant use cases of areas listed in Annex III via delegated acts.

3. Conformity assessment (Article 43, Annex VII)

- The use of a manufacturer's self-declaration for high-risk stand-alone AI systems (Annex III), as maintained by the Council and EP, should be rejected. If an AI system is classified as high-risk, it should be subject to mandatory certification by notified bodies. Only an independent assessment can rule out potential conflicts of interest on the part of the provider. At the same time, it ensures that the AI system complies with all mandatory requirements of the regulation. The mandatory involvement of a notified body in the case of high-risk products is a core pillar of European product legislation and the New Legislative Framework.
- In order to properly conduct a conformity assessment, notified bodies need comprehensive access to all necessary data (e.g. source code, training and/or validation data). This is indispensable to verify that AI systems meet the requirements of the AI Act. However, both the Council and EP positions severely restrict this access for notified bodies. In our view, this restriction does not seem justified, also because there are already strict requirements in place for conformity assessment bodies as regards the protection of intellectual property and the protection of trade secrets.
- To reduce compliance costs, especially for SMEs and start-ups, the EU legislator should consider appropriate financial support instruments.

4. Alignment with sectoral legislation (Article 8)

- Given that individual sectoral EU legislation already contains AI-specific requirements, it must be ensured that there are no overlapping or conflicting requirements (for example, with the Medical Devices Regulation). The collision rule added by the EP is therefore to be welcomed in principle. The aim must be to create legal certainty for manufacturers and notified bodies.

5. Requirements for high-risk AI systems (Article 9, 12)

- The use of already existing quality management systems in the context of conformity assessment should be made possible, as proposed by the EP. This applies in particular to AI systems that are integrated into products, where the AI Act requirements can be integrated into existing quality management systems. This helps to avoid unnecessary extra work. The objective must be that European legislation is harmonized in such a way that one quality management system is sufficient for one product.

- The mandatory measurement and recording of the energy and resource consumption of AI systems as proposed by the EP is also to be welcomed. In a next step, mandatory energy saving targets should be formulated at EU level.

6. Requirements for notified bodies and designating authorities (Article 30, 38, 44)

- Regarding the designation of conformity assessment bodies by the competent national authorities, uniform specifications and assessment procedures are required to ensure a consistently high level of competence of notified bodies. This is the only way to achieve a uniform level playing field between notified bodies. The cooperation and exchange formats between the designating authorities envisaged by the EP must be supported, as well as qualification standards prescribed for auditors of authorities.

- Due to the continuing development of AI systems, the validity period of certificates issued by notified bodies should be limited. A validity period of four years as proposed by the EP is reasonable in the light of shorter product life cycles and continuous changes in AI systems (learning).

7. AI regulatory sandboxes (Article 53)

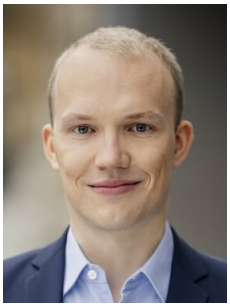
- The establishment of AI regulatory sandboxes is a good way to facilitate the development and assessment of AI systems. Independent assessment organizations should also be included as an important partner in the development and use of regulatory sandboxes. In addition, as envisaged by the EP, their establishment should be made mandatory for individual member states or between several member states.

- However, the successful use of regulatory sandboxes for an AI system alone can and should not lead to a presumption of conformity. Before an AI system is placed on the market, it must still undergo a complete conformity assessment process, if required with a notified body. While the notified body can, for example, draw on certain collected data from the regulatory sandbox as part of the certification process, it must nevertheless always take a holistic view of whether all legal and normative requirements have been fulfilled. For the sake of legal clarity, the term "presumption of conformity" should therefore be deleted from the EP position.

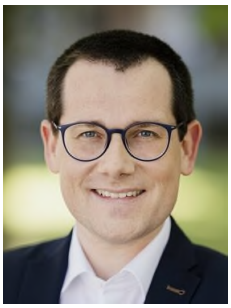
8. Generative AI/foundation models (Recital 60h, Article 28b)

- The last few months have made it clear how quickly foundation models and generative AI systems are developing and what risks they can pose. It is therefore necessary to regulate the use of this technology directly in the AI Act in order to make the legal framework future-proof. The EP approach is therefore preferable to the Council approach.
- Due to the wide range of use cases of foundation models, it also appears suitable to take a risk-based approach to classification. Nevertheless, it must be ensured that all risks emanating from the respective areas of application are fully considered. In a first step, certain basic requirements should be defined for all providers of a foundation model or a generative AI model in accordance with the EP position. In a second step, it should then be ensured that foundation models or generative AI systems that are particularly risky are also classified as high-risk systems and are thus subject to all the requirements of the AI Act.
- Regarding the assessment of foundation models, the EP position foresees an internal assessment on the part of the provider. This is justified by the statement that conformity assessment bodies currently lack the necessary expertise in assessing foundation models. Given the absence of concrete legal and normative requirements, there are of course no comprehensive testing tools for foundation models yet available. This, however, poses a challenge to any kind of assessments of foundational models, regardless of whether conducted internally or externally. In other words, the absence of legal and normative requirements does not give a sufficient justification for limiting the assessment to a purely internal evaluation by the provider itself. Rather, the corresponding assessment procedures for foundation models should be based exclusively on their risk potential. If the EU legislator comes to the conclusion that certain foundation models are to be classified as highly critical, they should also be subject to an independent third-party assessment by notified bodies. Corresponding transitional periods allow European standardization organizations and conformity assessment bodies to develop appropriate standards and assessment procedures for this purpose.

Authors and contact



Johannes Kröhnert
Head of Brussels Office
Email: johannes.kroehnert@tuev-verband.de
Tel.: +49 30 760095 500
www.tuev-verband.de/en



Dr Patrick Gilroy
Head of Artificial Intelligence & Education
Email: patrick.gilroy@tuev-verband.de
Tel.: +49 30 760095 360
www.tuev-verband.de/en

The TÜV Association represents the political and professional interests of its members vis-à-vis politics, administration, business and the public. The association is committed to technical and digital safety for products, systems and services through independent testing and qualified further training. With its members, the TÜV Association pursues the goal of maintaining the high level of technical safety in our society and creating trust for the digital world.

Publisher
TÜV-Verband e. V.
Friedrichstraße 136
10117 Berlin

Tel.: +49 30 760095-400
Email: berlin@tuev-verband.de
www.tuev-verband.de/en