WE ARE SHAPING THE INTERNET.
YESTERDAY.TODAY.BEYOND TOMORROW.

eco

TARGETED STAKEHOLDER CONSULTATION ON CLASSIFICATION OF AI SYSTEMS AS HIGH-RISK

The European Commission is currently conducting a consultation on the development of guidelines for high-risk KI systems. The consultation, in the form of an online survey, is open until 18 July. The full questionnaire can be found here. The feedback received will contribute to the drafting of the upcoming guidelines on the classification of AI systems and related obligations. eco would like to comment on selected questions, which you will find in this document.

Question 35. Beyond the technical standards under preparation by the European Standardisation Organisations, are there further aspects related to the AI Act's requirements for high-risk AI systems in Articles 9-15 for which you would seek clarification, for example through guidelines?

Although the risk management obligations are comprehensive, there is a lack of clarity regarding the proportionate implementation of these processes, particularly for SMEs and start-ups. Guidelines should provide concrete examples of what constitutes an adequate risk management system for different types of high-risk application. The exact expectations for documentation and record-keeping remain unclear across different sectors and AI system types. More detailed templates or best practices would be highly valuable for aligning with future conformity assessments.

Question 36. Are there aspects related to the requirements for high-risk AI systems in Articles 9-15 which require clarification regarding their interplay with other Union legislation? If so, please elaborate which specific aspects require clarification regarding their interplay with other Union legislation and point to concrete provisions of specific other Union law.

The data quality, representativeness and bias requirements in Article 10 intersect with the data processing obligations set out in the GDPR, particularly Articles 5 (data minimisation and accuracy), 9 (special categories of data) and 25 (data protection by design). However, it is unclear how these requirements interact, for example, in situations where AI training requires sensitive data. Furthermore, the Data Act introduces obligations regarding data access and sharing, which could affect the management of training and validation data. Clear guidance is needed on how to reconcile these frameworks, particularly with regard to lawful bases and data portability. The obligations under Articles 9 (risk management) and 15 (accuracy, robustness and cybersecurity) may overlap with the safety requirements set out in the revised Product Liability Directive. Clarification is needed on how AI-specific risk assessments interact with general product safety assessments, and on whether duplication of risk management documentation can be avoided.

Question 37. Are there aspects related to the AI Act's obligations for providers of high-risk AI systems for which you would seek clarification, for example through guidelines?

The definition of 'appropriate human oversight' is somewhat ambiguous. Providing more concrete examples and guidance on how human oversight should be integrated into AI systems, especially in high-risk sectors such as autonomous vehicles, would help to ensure compliance and improve system reliability. The requirements for the continuous monitoring of high-risk AI systems after deployment need to be clarified, particularly with regard to how frequently assessments should be updated, and the role of providers in ensuring ongoing compliance. Guidelines on how to manage this process in the context of evolving technologies and regulatory changes would be helpful.

Question 38. Are there aspects related to the obligations for providers of high-risk AI systems which require clarification regarding their interplay with other Union legislation?

Article 10 of the AI Act requires providers to ensure the quality, representativeness and fairness of data. These requirements overlap with those of the GDPR, particularly Articles 5, 6, 9 and 25, which concern data minimisation, the legal bases for processing and data protection by design. Clear guidance is needed on how to use personal or sensitive data lawfully for training high-risk AI systems and on how to reconcile potentially conflicting obligations (e.g. using more data for bias mitigation versus minimisation principles).

Question 39. Are there aspects related to the AI Act's obligations for deployers of high-risk AI systems listed in Article 26 for which you would seek clarification, for example through guidelines?

From eco's perspective, the obligation to ensure effective human oversight is broadly defined. More detailed guidance on how to implement this in different operational contexts, such as healthcare, employment and finance, would be valuable. This guidance should cover what constitutes 'appropriate' oversight, the required qualifications of human reviewers, and how oversight responsibilities can be documented. The requirement to monitor systems and keep logs raises questions around technical feasibility, proportionality and privacy, especially when the deployers do not control the logging mechanisms. Guidelines should clarify the extent to which deployers must verify logging functionality, retain records and protect logged data in accordance with data protection legislation.

Question 40. Are there aspects related to the obligations for deployers of high-risk AI systems listed in Article 26 which require clarification regarding their interplay with other Union legislation?

Article 26 (2)(b) requires deployers to ensure that the input data is both relevant and sufficiently representative. This obligation may overlap with the data minimisation and purpose limitation principles set out in Articles 5 and 6 of the GDPR. However, it is unclear how deployers should balance these obligations in practice, especially when they are not the original data controllers, but merely users of AI systems. Clear guidance on responsibilities and liabilities in such cases is needed. The duty under Article 26 (1)(c) to inform individuals when they are interacting with a high-risk AI system may overlap with transparency requirements under the Digital Services Act, particularly for very large online platforms and

recommender systems. Further guidance would help to clarify how these transparency regimes align and whether one set of disclosures could satisfy both.

Question 41. Are there aspects related to the AI Act's obligations for deployers of high-risk AI systems for the fundamental rights impact assessment for which you would seek clarification in the template?

The basic concept of fundamental rights remains difficult to operationalise. It is sometimes difficult for deployers to rule out whether fundamental rights could be affected in individual cases, especially as these are not specified further. Standards are needed that make this abstract concept assessable and operationalisable for deployers. The guidelines should also provide clarity regarding the overlaps with the data protection impact assessment that is also required under the GDPR. It should also be clarified what kind of complaint mechanisms are necessary to meet the requirements of the AI Act. The focus must be on an appropriate and practicable solution.

Question 43. Are there aspects related to the AI Act's right to request an explanation in Article 86 for which you would seek clarification, for example through guidelines?

eco believes that Article 86, the right of affected persons to request an explanation regarding decisions taken or supported by high-risk AI systems, raises several important questions that should be clarified. There is overlap with the GDPR, especially Article 15 (right of access) and Article 22 (automated decision-making). It should be clarified how Article 86 complements or differs from existing rights and whether one request could fulfill obligations under multiple legal frameworks. Also, the level of detail and format of the explanation should be clarified. Furthermore, the right to explanation must be balanced against the protection of intellectual property, trade secrets, and security concerns. Clear guidance is needed on how to comply with Article 86 without disclosing sensitive information, and how to handle requests that may go beyond what is legally or commercially appropriate.

Question 44. Do you have any feedback on issues that need clarification as well as practical examples on the application of the concept of 'substantial modification' to a high-risk AI system.

In order to eliminate legal uncertainty, the guidelines should address the issue of substantial modifications. This question is central to determining whether a company is a provider or a deployer, and thus which obligations must be fulfilled. It is important to understand that AI systems can be fine-tuned using in-house training data. This is often an important prerequisite for successful implementation. However, if those responsible for such fine-tuning are treated as operators, this could negatively impact the adoption of AI systems within companies, as the additional obligations could act as a deterrent. It should be emphasised that training using in-house data for internal company purposes does not constitute such a modification.

Question 50. Do you have or know concrete examples of AI systems that in your opinion need to be added to the list of use cases in Annex III, among the existing 8 areas, in the light of the criteria and the conditions in Article 7 (1) and (2) and

should be integrated into the assessment pursuant to Article 112 (1) AI Act? If so, please specify the concrete AI system that fulfils those criteria as well as evidence and justify why you consider that this system should be classified as high-risk.

In eco's opinion, the categories listed in Annex III are already very comprehensive and do not need to be expanded. However, it is necessary to clarify which systems are not considered high-risk in accordance with Annex III, as they fall under the exceptions in Article 6 (3). This clarification is crucial for the precise application of the AI Act, as it is important that only systems that can pose an actual risk due to their intended use in sensitive areas are considered high-risk.

Question 51. Do you consider that some of the use cases listed in Annex III require adaptation in order to fulfil the conditions laid down pursuant to Article 7 (3) AI Act and should therefore be amended and should be integrated into the assessment pursuant to Article 112 (1) AI Act? Please justify why you consider that the use case needs to be adapted in order to fulfil the conditions as per Article 7 (3) AI Act

In principle, as few systems as possible should be affected by Annex III, as intended by the Commission, to avoid stifling innovation. It will become apparent after implementation whether changes need to be made here in order to strike a balance between mitigating risks and enabling innovation.

Question 52. Do you consider that some of the use cases listed in Annex III no longer fulfil the conditions laid down pursuant to Article 7 (3) AI Act and should therefore be removed from the list of use cases in Annex III and should be integrated into the assessment pursuant to Article 112 (1) AI Act?

The design of Annex III must ensure the effective implementation of the AI Act's risk-based approach. Therefore, only systems that pose an actual risk, such as to security, can be categorised as high-risk. For this reason, the interpretation of the exemption rule set out in Article 6 (3) will also be important. This will determine whether the AI Act adheres to its risk-based approach or also regulates low-risk systems. The internet industry believes that it is too soon to decide whether use cases should be removed from Annex III, given that the implementation and interpretation of the provisions are still pending. However, it is essential to ensure that there is no overlap with existing regulations, particularly with regard to the security components of critical infrastructure.

Question 53. Do you have or know concrete examples of AI practices that in your opinion contradict Union values of respect for human dignity, freedom, equality and no discrimination, democracy and the rule of law and fundamental rights enshrined in the Charter and for which there is a regulatory gap because they are not addressed by other Union legislation? If so, please specify the concrete AI system that fulfils those criteria and justify why you consider that this system should be prohibited and why other Union legislation does not address this problem.

The AI Act addresses a large number of potentially risky practices that already overlap with existing regulations, such as anti-discrimination legislation, the GDPR and the DSA. Given this, the list should not be expanded, since all relevant risks are

covered by the AI Act and other existing regulations. Before any new practices are added, it should be checked whether they are already addressed by existing legislation. This is particularly important given the large number of overlaps in digital legislation, which increases the complexity of using digital applications and creates legal uncertainty.

Question 54. Do you consider that some of the prohibitions listed in Article 5 AI Act are already sufficiently addressed by other Union legislation and should therefore be removed from the list of prohibited practices in Article 5 AI Act? Please justify how other Union legislation already sufficiently addresses this AI practice

Trust in AI is fundamental to its acceptance. eco therefore support the prohibitions set out in Article 5, especially those relating to law enforcement. Real-time biometric recognition systems, in particular, should not be used for this purpose. In order to close the existing loopholes, it would be necessary to tighten the ban.

About eco: With approximately 1,000 member companies, eco (international.eco.de) is the leading Association of the Internet Industry in Europe. Since 1995, eco has been highly instrumental in shaping the Internet, fostering new technologies, forming framework conditions, and representing the interests of its members in politics and international forums. eco has offices based in Cologne, Berlin and Brussels. In its work, eco primarily advocates for a high-performance, reliable and trustworthy ecosystem of digital infrastructures and services.