Position Paper on proposed Artificial Intelligence Act (AIA)

Who we are and why our input matters

We are the Belgian, Dutch, French and German CIO-associations; the communities of Chief Information Officers (CIO's) and other senior leaders that are responsible for digital technologies and digital transformations within private or public organisations. All our members are European business users of digital technologies. We do not represent ICT providers and consultants.

Business users of digital technology are a key link in the digital transformation of society and economy: including the use of AI systems. To reap the benefits of Artificial Intelligence in Europe, the position of *business users* - companies and government organisations - of digital technology must be taken into account. Business users also play an influential role in the development of AI systems that comply with European standards and values through their joint purchasing power in the market for AI systems. Therefore, we are a main stakeholder in the establishment of the AI Act.

Our associations welcome the opportunity to provide feedback on the proposal for the Artificial Intelligence Regulation. We consider the AI proposal a starting point to assess how to honour fundamental rights, health and security, while allowing AI technology to flourish.

Summary

An appropriate framework for the safe, responsible, and sustainable use of AI systems in Europe is essential for the full exploitation of AI technology in the years to come. AI encompasses a very broad range of technologies which develops at a very high rate. Each category of AI has specific opportunities, operational contexts and use cases as well as risks. To achieve an appropriate framework that allows European businesses and government organisations to successfully make use of AI systems, it is necessary to provide guidance and to ensure the governance structure is solid and able to evolve with the developments in technologies. Furthermore, there needs to be a fair balance between the requirements for providers and users. Compliance with requirements, the provision of clear information and comprehensible technologies and products, assurance, and a harmonised approach to oversight are crucial for this AI Act to succeed. In particular, we have identified five points that we believe require additional attention or should be re-evaluated. Taking into account

these aspects would help create an AI-Act that enables business users to effectively contribute to European economy and society by using AI systems.

General overview of AI and the proposed AI Act

Companies and governments use AI systems to an increasing extent in essential business processes. With that, the impact of AI on the daily life, health, mobility, and safety of EU citizens grows. AI systems enrich and expand the possibilities of the digital domain through their ability to process (large amounts of) data in order to gain insights or execute actions (with or without human intervention). By these means, AI systems can improve business processes for both companies and government organisations and create value for organisations, the economy and society.

> *For example, in healthcare AI systems make diagnoses by comparing images of a patient with a gigantic database of images. Another example, AI systems are used to prevent the failure of factory lines by timely signalling the wear off of parts outside their "regular" patterns. Furthermore, AI technology is and will increasingly be a necessary component in cyber security solutions because of its great strength in for instance pattern recognition.*

Consequently, we support:

1. The appropriate framework that the AI Act introduces for the safe, responsible, and sustainable use of AI systems in Europe, essential for the full exploitation of AI systems in the years to come.
2. The risk-based approach of the AI Act by establishing classes of AI systems for which the intensity of requirements increase with the risk that an AI system poses to the health and safety of EU citizens and their fundamental rights. The risk-based approach provides clarity and oversight, without creating unnecessary market entry barriers for low-risk applications of AI systems.
3. The application of the AI Act to all AI systems that are placed on the market or have their output in the European Union.

We would like to express our serious concerns about five aspects of the proposed AI Act:

1. Scope and risk classifications should keep pace with evolution of AI technologies and market situations
2. The need for guidance for developers of AI and users
3. The fairness of the balance in the responsibilities of providers and users
4. The assurance of compliance and harmonised approach to oversight
5. The scope and application of the sandbox environments to stimulate innovations

The aspects mainly concern high-risk AI systems. We elaborate on the five aspects below.

1. Scope and risk classifications should keep pace with evolution of AI technologies and market situations

AI technologies develop at a very high pace and encompass a wide and expanding range of technologies. We welcome article 2(1) of the AI Act, which sets out that the scope of the AI Act includes output produced outside the EU if that output is used within the EU. This provision should remain.

On five specific points the scope of the AI proposal needs specification and clarification:

a) Do AI systems and their output that are strictly used within an organization, also fall within the scope of the AI Act?

b) How will the Commission ensure that certain technologies that may feature within an AI system, such as logical functions or statistics, do not lead to disproportionate complexity and costs when they are included within the scope of AI? Such technologies are also broadly used outside of AI, and would make compliance extremely difficult and costly, without adding a real benefit.

   For example, a switch in railroad tracks use some form of logic to make sure trains do not collide (they provide security). If this would be interpreted as AI, it would be classified as high-risk. This would have a major impact on the operations and costs of railway operators, while not adding any extra benefit.

c) How does the Commission make sure low risk AI systems will not cause major disruptions? Such low-risk AI may carry a substantial risk in disrupting the economy or society.

   For instance, low tech spreadsheets and their formulas and algorithms used by brokers and agents in stock markets. These relatively low tech, yet related to AI, technologies could lead to serious disruptions if they lead by mistake to large scale sale of stocks.

d) Business users are concerned about how self-developing technologies will be classified and kept compliant in case they develop through self-adaptation technology into an AI system of a higher risk category, based for instance on machine learning algorithms. How will this be addressed?

e) Machine learning algorithms are developed based on the data they are ‘fed’. A clear and fair balance in responsibility is crucial for business users. How would certification and re-certification work in cases of AI based on machine-learning? Does every new version

need to be certified in full, or should this be done periodically? And if a periodical recertification is required, what would be a relevant period? Moreover, is every user/data owner responsible for re-certification, or is the primary provider of the technology responsible, or both? To what extent?

f) The definition of AI together with the high risk systems referred to in article 6 (2) can lead to unnecessarily broad scope of AI functioning that could actually not lead to the risks identified. For example the 'employment use case' (annex 3 sub 4) should exclude 'traditional' software that do not have any risky automated machine learning or decision-making in them, to avoid unnecessary complexity and costs to all employers.

2. The need for guidance for developers of AI and users

The proposed AI Act sets out requirements and obligations for AI providers, manufacturers, importers, distributors, and users. It also establishes an enforcement structure including significant fines. In that regard, we would like to point out our experience with the implementation of the GDPR. We considered adequate guidance on the GDPR to be missing for several years. However, the high fines under the GDPR prompted our members to massively seek consent for the processing of data, leading to overflooding citizens with messages. Real constructive guidance for business users did not arrive until three years after the GDPR came into force; a code of conduct approved by the Belgian DPA.

In the case of the AI Act it is imperative that guidance is provided before the AI Act enters into force. Moreover, that guidance should be suitable to i.a. business users and available throughout the EU. Articles 55 (1), 59 (7) and 62 (2) aim at establishing guidance, but only after the Act has come into force, while it also relates to guidance by national authorities. We find it crucial to make it possible for business users to know exactly what is expected of them. The difficulties in interpretation as experienced with the GDPR must be avoided. Our member companies have subsidiaries in multiple EU member states and do business in multiple member states. The European Artificial Intelligence Board, as foreseen in article 56 and 58, should assist in providing guidance on the AI Act. Furthermore, the guidance should be regularly updated to keep up with technological and regulatory developments.

3. The fairness of the balance in the responsibilities of providers and users

Our associations understand the distribution of responsibilities between providers and business users as laid down in the AI proposal. We nevertheless caution against a black and white approach. In daily practice, co-creation, joint efforts and consortia of providers and users occur. It should be transparent in all cases how to determine a fair distribution of responsibilities between stakeholders.

Additionally, we signal the need for compliance by design, third party assurance and an appropriate division of responsibilities between provider and business users of software and digital technology. Our experience with the GDPR supports these vital needs. In practice, it is near impossible for business users to make software fully compliant with the GDPR requirements in a technical sense and to reach the necessary contractual agreements with software providers. Companies and government bodies cannot offer sufficient counterbalance to the much larger software providers. Similarly, the essential conditions for safe, responsible and sustainable use of AI cannot be achieved by simply imposing obligations on business users of AI systems. This would be unfair as providers of AI systems are indispensable to ensure such essential conditions and therefore also have to bear a considerable part of the responsibility in the usage of AI systems.

In light of the above we also want to point out that under article 10 (5) only the provider is allowed to gather and process (demographic) data for the purpose of bias monitoring. In our opinion business users should have the same right as they can apply more effective and meaningful debiasing methods when they can 'de-bias' for their own population of individual end-users using their own data sets. The business user is otherwise in a dependent position and may not be able to adequately perform testing without provider's involvement.

4. The assurance of compliance and harmonised approach to oversight

We emphasise the need for availability of information relating to AI systems to authorities and business users, as well as for expert supervision in each Member State. It should be prevented that Member States impose national requirements on the use of digital products, including AI, or interpret the rules differently. Also, each member state should have sufficient expert staff to adequately supervise the application of the framework. Otherwise, the adoption of AI by EU business users will be severely hampered by decreasing transparency and economies of scale, and consequently increasing costs and risks.

The current implementation of the GDPR shows several lessons to be learned and situations to avoid. For instance, the lack of accurate information available to users and authorities on compliance of software with GDPR, the number of different interpretations of obligations and a growing number of pages in guidance, which continues to increase the complexity and the necessary means companies have to put in. We also notice the very different levels of expertise and capacity of the different data protection authorities, the competent authorities for the GDPR, in the different members states. Below we will go into more detail on specific aspects relating to the supervision of legislation in the digital domain.

A) Provision of information by providers of AI

AI system providers should be required to provide timely, complete and accurate information and evidence on the system's compliance with all relevant laws, norms and

requirements to business users. The information is necessary to assess whether the basic principles of the AI system are in line with laws and requirements. Moreover, that information is essential to perform (possibly mandatory) Data Protection Impact Assessments (DPIAs).

Article 22 of the AI proposal only mentions the supervisor, whereas the business user also has a direct interest in knowing about shortcomings in a high-risk AI system. For example, it is undesirable that the situation arises where the supervisor is informed by a provider of a serious flaw in a healthcare system, while hospitals continue to use the AI system. It should be clear how the business users of high-risk AI system will be informed.

The obligation for providers to share information with business users should be included in the final AI Act. This obligation should also apply if the provider is not the original developer of the technology. The aim of such an obligation is to prevent the original provider, who is responsible for compliance by design, from hiding behind intermediate providers and importers to escape accountability.

Article 28 of the AI proposal states that business users can be designated as providers in certain cases, with the corresponding obligations under the AI Act. Under paragraph 2, the original provider is in such a case no longer a provider. However, that should only be the case if that original provider has provided timely, complete and correct information and remains accountable for compliance by design. In the AI Act it should be clarified how it is ensured the business users are correctly informed, as well as how accountability is divided between the original provider and the user that becomes the provider in the sense of article 28 AI Act.

Article 29(3) states that the user shall ensure that input data is relevant for the intended purpose of the high-risk AI system. It is unclear how it is determined what data is relevant for the intended purpose and by whom. Further clarification on this matter would be helpful to business users of AI systems.

B) Explainability instead of transparency

The proposal regularly focusses on the need for transparency and states that there should be a public list of high-risk AI systems. Our members feel this may be too burdensome and compromise the effective day-to-day operation of business users. Instead, the notion of explainability should be used, as that allows business users, consumers and authorities to know how products of AI systems came to be, without making too high demands on the business users of AI systems. Towards supervisory authorities a higher level of insight into for example audit trails could be made available, in order to let these authorities carry out their mandate. This could for instance be achieved by requiring AI providers and users of AI

to keep an internal list of such systems, that can be made available to the authority, similar to the system of the GDPR.

C) Providers to be represented and held responsible within the EU

We applaud the obligation to appoint an authorised representative established in the European Union in case an importer cannot be identified - recital 56 and Article 25. We find it crucial that all organisations in charge of the implementation and enforcement of the AI Act, be it the National Competent Authority (NCA), competition authorities or other bodies, are able to conduct all necessary steps towards a clearly designated authorised representative, independently of where in the European Union it is established. A precedent of this was also established in relation to the GDPR.[1]

D) Authority of NCAs across Member States

It should be ensured that the different NCAs can investigate authorised representatives. These authorities should be sufficiently mandated, staffed and provided with adequate funds, to ensure knowledge of both technological and market related developments and the ability to timely and adequately execute their roles. In situations where the national competent authority of the member states in which the authorised representative is established, is unable or unwilling to investigate, other NCAs should be able to enforce the AI Act.

As far as the work of conformity bodies and technical services is concerned, we highlight the need to draw lessons from the 'Dieselgate' scandal. The European system of oversight was unable to prevent the putting on the market of cars which largely surpassed the allowed level of NOx-emissions.[2] Our associations ask the European Commission to ensure that

[1] On 15th of June 2021, the Court of Justice of the European Union ruled that the Belgian DPA in its case against Facebook, may, under certain conditions exercise its power to bring an alleged infringement of the GDPR to the attention of the judicial authorities of a Member State, even if this supervisory authority is not the lead authority for that processing. The case has been started in 2015 in Belgium.

[2] While the European Commission seem to have drawn lessons in ensuring market surveillance authorities have access to the source code -article 64 (2) – the lessons on the functioning and the financing of the notified bodies and technical services performing the conformity tests are not taken on board.
The report on the inquiry into emission measurements in the automotive sector of the European Parliament, 2016/2215(INI) lists several short comings:
While in many cases the choice by a car manufacturer of the type-approval authority of a certain Member State is due to geographical or historical reasons, the lack of a harmonised interpretation of the rules can lead to a situation of competition among the type-approval authorities of different Member States, as car manufacturers may choose an authority on the basis of its flexibility in the interpretation of the rules.
It is the car manufacturer that usually chooses the technical service to be used: in principle, the type-approval authority can challenge the choice, but it seldom does so. National authorities have never asked technical services to perform additional tests to ensure the implementation of the requirement to meet the regulatory

different NCAs can oversee the notified bodies and technical services performing the conformity tests. Not only the NCA of the country in which the notified bodies and technical services are established, but also NCAs from other European member states.

5. The scope and application of the sandbox environments to stimulate innovation

We welcome the introduction of regulatory sandboxes where providers can test their AI products and services. The sandboxing mechanism as described in article 53 will likely work well for putting physical products on the market which have AI as a safety feature. However, for digital products, the lifecycle is different. Digital products undergo multiple changes and adaptations before they go live and are put to use by business users. But even after that, the systems are often only used in a limited setting or on a small scale and gradually rolled-out through the whole organization. If an AI system can only benefit from the regulatory sandbox until its first 'go live', we fear the sandbox will simply be too small and have too little impact on the final product. Also, if an AI system is only required to be fully compliant at the proof-of-concept stage, which is a stage without certainty that the system will be sold, the compliance costs of working with the ultimate product are likely to be too high. The initial preconditions set in the sandbox do not correspond and fall short of the large impact/risk AI products can have during a later stage of their lifecycle.

Final remarks

The arguments described above should not be deviated from just because of the potential impact of regulatory pressure on the opportunities for small and new providers of AI system. The small size of an AI provider should not be a reason to lower the requirements for a high-risk system or shift the responsibility to the business user. After all, it would be inexplicable when the 'derailment' of an AI system in for example healthcare or traffic control results in casualties, but the provider cannot be held accountable for supplying an unsafe system because it has only four employees. Or perhaps because the provider in question has only a modest turnover in the EU, but is in fact a sales office for a large tech provider that operates globally. Just as the current proposal for the AI Act sets out, the risk level of the application must be leading.

We would like to emphasize our appreciation for the European Commission's proposal for the AI Act. We trust that our contribution will help to make the AI Act as fit for purpose as possible, offering Europe's businesses and public organizations access to safe, responsible, and sustainable AI systems. The result of the combined work of the Commission and other

---

limit in "normal use" or of the ban on defeat devices. For technical services, running additional tests on their own initiative would entail supplementary costs and might put their commercial relationships with manufacturers at risk.
(EMIS report, CHAPTER 5: TYPE-APPROVAL AND IN-SERVICE CONFORMITY, https://www.europarl.europa.eu/doceo/document/A-8-2017-0049_EN.html#title7)

stakeholders, among them our members, will provide the framework for future development of AI and the good use of these powerful technologies in Europe. Collectively we need to make sure we offer Europe the best possible chance to succeed in regulating and working with AI systems, while keeping in mind European values and business opportunities.

If we can be of further assistance by explaining our position or providing more insights into the business user's perspective on AI, we welcome you to contact **Ronald Verbeek, director of CIO Platform Nederland, via bureau@cio-platform.nl**