DIGITALEUROPE

16 OCTOBER 2023

AI Act trilogues: A vision for future-proofing, governance and innovation in Europe

Executive summary

DIGITALEUROPE has been a strong supporter of the overall objectives of the proposed AI Act, and its focus on high-risk uses of artificial intelligence (AI).[1] We welcome the Council's and the European Parliament's efforts to strike a balance between protecting the health, safety and fundamental rights of European citizens and ensuring that Europe's growing AI industry remains competitive and continues to innovate.

When regulating something as dynamic and with such high potential as AI, it is paramount not to fall into the pitfall of regulating out of fear. To avoid this, we need clear goals, agile policymaking processes and multi-stakeholder engagement. DIGITALEUROPE's sandboxing report showed how commitment to regulation alone is not enough, and needs to be complemented with proper dialogue and regulatory prototyping across the AI industry ecosystem to be effective.[2]

At the moment, work is still needed to reach the delicate balance and dual ambition of protecting citizens and driving the AI-fuelled business solutions of tomorrow, especially through deeper consultation with industry experts who can interpret how complex AI rules may impact AI-powered businesses.

This paper compares the Parliament's and the Council's mandates for trilogue negotiations,[3] contributing the following recommendations to improve the AI Act and make it truly future proof:

- **AI definition and scope:** The definition of 'AI' must be focused and should align with international frameworks like OECD and NIST to foster

[1] COM(2021) 206 final.

[2] See DIGITALEUROPE, *Sandboxing the AI Act: testing the AI Act proposal with Europe's future unicorns*, available at https://www.digitaleurope.org/resources/sandboxing-the-ai-act-testing-the-ai-act-proposal-with-europes-future-unicorns/.

[3] As reflected in Council doc. 11320/1/23 REV 1.

international harmonisation and market access in third countries.[4] Research and development (R&D) and open-source exemptions are essential for innovation.

- **Risk categorisation:** The risk-based approach is at the core of the AI Act. It is central to ensure that the risk categorisation framework is technology-neutral and focuses on truly high-risk use cases.

  - **Prohibited practices** need precise definition and clarity to avoid unintended restrictions. Prohibitions of social scoring, biometric identification and emotion recognition should be targeted, to permit controlled high-risk applications.

  - **High-risk systems:** The Parliament's 'significant risk' criterion should be upheld, combined with the Council's condition on human oversight, enhanced. The proposed notification process for providers, however, will generate uncertainty and delays, and should be replaced with a documentation-based approach.

- **Alignment with existing legislation:** The AI Act must align with Europe's existing comprehensive legislation, avoiding disruptions to well-established sectoral frameworks such as product legislation, from healthcare to machinery, and finance. The final text should explicitly provide that existing governance and enforcement frameworks, including automatic recognition of notified bodies and market surveillance authorities, can be used when assessing and applying the AI Act's requirements.

- **Requirements for high-risk AI:** Requirements must be technically feasible, avoid double regulation and align with existing legislation. The Parliament's expansion beyond health, safety and fundamental rights, covering rule of law and environment, muddles the AI Act's scope and will only make compliance more problematic.

- **Allocation of responsibilities:** Flexibility in allocating responsibilities to the actors that can most appropriately ensure compliance is crucial. The Parliament's proposed fundamental rights impact assessment for deployers, whilst well-intentioned, is merely duplicative and should be rejected.

- **General-purpose AI (GPAI):** Regulating GPAI requires a light-touch approach, to avoid treating all systems without an intended purpose as high-risk. Any requirements on GPAI or foundation models should focus on information sharing, cooperation and compliance support across the value chain.

[4] Available at https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449 and https://csrc.nist.gov/Topics/technologies/artificial-intelligence, respectively.

- **Implementation:** The availability of harmonised standards to prove compliance, aligned with international efforts, will be central to the AI Act's success. The AI Act should balance risk prevention with innovation support. Regulatory sandboxes should be mandatory across Europe, encouraging participation and real-world testing. To boost innovation, a robust investment plan, especially for start-ups and SMEs, should accompany the AI Act, ensuring growth and competitiveness.

- **Governance:** The AI Board, or AI Office in the Parliament's mandate, should ensure a centralised approach, with continuous engagement with industry and civil society. Coordination and advisory roles of the AI Board and the Commission are essential to ensure consistent application and avoid inconsistencies.

- **Enforcement:** EU-wide safeguards against disproportionate decisions are necessary. A 48-month transitional period is necessary for overall ecosystem readiness, including the timely availability of harmonised standards.

Table of contents

Scope

AI definition

The definition of ‘AI’ must delineate the AI Act’s precise scope. It should align with well-accepted international frameworks, particularly the OECD and NIST, to promote harmonisation, international standards efforts, and market access in third countries.

Both the Council and the Parliament have endeavoured to achieve this alignment, and the final text should combine their efforts. The Parliament’s wording is more in line with international best practices, whilst the Council’s wording is superior in differentiating AI from merely advanced software systems by explicitly referencing autonomy and system-generated outputs.

Exemptions

R&D

We strongly endorse the vision of both Council and Parliament that the AI Act should not apply to AI systems developed exclusively for R&D purposes.

AI systems used in the R&D phase typically lack operational impact on individuals, and their inclusion would deviate from the AI Act’s primary goal of safeguarding European citizens.

Furthermore, AI outputs utilised in R&D may ultimately contribute to the development of technologies, products or services that will in themselves fall into scope. To prevent the duplication of regulation at different stages of a technology’s lifecycle, risking the relocation of R&D activities outside Europe, we recommend incorporating the Council’s wording from Recital 12b into Art. 2 of the final text: ‘As regards product-oriented research activity by providers, the provisions of this Regulation should also not apply.’

Open source

This innovation-centric approach is further evident in the Parliament’s exemption of free and open-source AI components when not part of prohibited or high-risk AI systems. Such provisions are crucial as they contribute to research and innovation in the market, advancing Europe’s technological leadership.

However, the Parliament’s open-source exemption does not extend to foundation models. These models, due to their substantial development and training costs, remain the domain of a limited number of companies. For European researchers and innovators to compete globally and benefit from the latest AI advances, access is essential. Open-source and similarly permissive licences not only empower developers without typical access to such technology, but also democratise AI innovation. It also contributes to enhancing the safety and security of models and mitigating biases by involving a broader range of stakeholders.

The final text should support this by exempting foundation models provided under free and open-source or similarly permissive licences, whilst applying minimal provisions to those who make their models available to encourage widespread access to these cutting-edge models.

Risk categorisation

Prohibited practices

DIGITALEUROPE fully supports the prohibition of AI practices that are proven to be particularly harmful and run counter to European values.

To avoid the inadvertent restriction of acceptable low or high-risk practices, these prohibited practices should be precisely defined.

Social scoring

For example, in Art. 5, a clear differentiation should be made between social scoring practices deemed of unacceptable risk and high-risk use cases like credit scoring for creditworthiness assessments, as well as lower risk scenarios such as fraud risk scoring.

Biometric identification and categorisation

The current broad prohibition on biometric categorisation and identification proposed by the European Parliament would inadvertently outlaw beneficial and legally mandated use cases, such as the detection of child sexual abuse material and deepfakes under robust safeguards. The original Commission proposal and the Council's position provide a more nuanced delineation of the ban's scope, specifically targeting practices carrying unacceptable risks, thus presenting more proportionate proposals.

Whilst acknowledging the potential risks to fundamental rights, it is crucial to recognise the significant public safety and national security benefits derived from the responsible deployment of AI-powered biometric identification, accompanied by stringent and meaningful safeguards.[5] Concerns over the use of biometric identification for purposes beyond law enforcement are suitably addressed through the classification of such use cases as high-risk under Annex III, expressly exempting them from Art. 5.

Emotion recognition

[5] Managing risks in such operations can be achieved by clearly defined processes and controls such as human review, confidence scoring, judiciary supervision, clear use policies, reasonable boundaries around data retention, and transparency measures.

The Parliament’s proposed ban on emotion recognition is overly broad, and should be more targeted to permit useful applications in controlled settings such as the high-risk framework.

Emotion recognition AI systems have myriad useful, sometimes lifesaving applications. For example, these systems can monitor the fatigue or vital signs of a pilot or driver to ensure passenger safety, identify aggressions in public transport or support responders when handling emergency calls.

Exemptions

The Parliament’s exemption for AI systems intended for therapeutic purposes is appreciated. However, it should align with the scope of the medical devices regulations,[6] whose definition of ‘medical device’ encompasses not only therapeutic but also various other specific medical purposes, such as diagnosis, prevention, monitoring, prediction, prognosis and alleviation of a disease. Such medical purposes should equally be recognised.

Clarifications by the European Parliament, such as the exemption of one-to-one verification systems and the acknowledgment that lawful advertising does not constitute a ‘subliminal technique,’ contribute to legal clarity and should be retained.

High-risk systems

Critical areas and use cases – Annex III

Both the Council and the Parliament introduce additional criteria for classifying an AI system covered in Annex III as high-risk, ensuring that the framework effectively encompasses applications with the potential for serious violations of fundamental rights or other significant risks.

In pursuit of this objective, the Parliament’s concept of ‘significant risk’ emerges as a superior criterion for capturing high-risk applications, compared to the Council’s proposal to exclude AI systems whose output is ‘purely accessory’ to the decision-making process.

We propose to merge the two approaches, combining the ‘significant risk’ criterion with a condition on human oversight in decision-making. Our recommendation is that an AI system should only be deemed high-risk if both of the following conditions are met:

a) It presents a significant risk of harm to the health, safety or fundamental human rights of individuals; and

[6] Regulations (EU) 2017/745 and 2017/746.

b) It autonomously makes decisions or is used to directly inform decision-making, materially influencing decisions and diminishing an individual's decision-making autonomy.

Importantly, the Parliament introduces the possibility for providers to determine that their system does not pose a 'significant risk.' This assessment is important to introduce a qualitative element that will make the AI Act's risk-based approach more granular.

Nevertheless, the Parliament suggests that companies' decisions must be notified to authorities, who can object to the assessment within three months and reclassify an AI system as high-risk. The implementation of this notification process raises doubts about its feasibility, considering the availability of adequate personnel and funding resources from the competent authorities' side.

Back in 2021, the working hypothesis underlying the Commission's impact assessment was that 10 per cent of AI systems entering the EU market would be high-risk.[7] With a growing number of AI solutions being developed and put in service every year, authorities might face handling hundreds of notifications per month. This unintended pre-market approval process, if authorities object to notifications to gain more time for assessment, could lead to delays of up to 12 months, discouraging companies from deploying their AI systems in Europe.[8]

Implementing such a notification process would strain already overloaded national authorities or newly established bodies like the AI Office/Board, creating legal uncertainty for authorities who could be held liable if they fail to properly review a notification.

Instead, providers should be required to document their assessment that their AI system does not pose a significant risk, and make it available to competent authorities upon request.[9]

When it comes to potential Annex III changes under Art. 7, we caution against the Parliament's disproportionate scope expansion to include risks affecting the environment, democracy and the rule of law.

[7] CEPS, ICF, Wavestone, *Study to support an impact assessment of regulatory requirements for artificial intelligence in Europe*, p. 142, available at https://digital-strategy.ec.europa.eu/en/library/study-supporting-impact-assessment-ai-regulation. This assessment did not factor in that, in certain sectors, this number can vary substantially. For instance, in the medical technology field, a vast majority of products would fall into the high-risk category due to Art. 6's formal criteria for high-risk categorisation.

[8] Adding to this, such a de facto pre-market approval process would be particularly problematic for AI systems already on the market but deemed high-risk by authorities after a substantial modification, such as a software update, which would equally have to be notified. Given the regular and necessary updates to such systems, it is essential to more clearly distinguish substantial modifications from continuous maintenance or updates.

[9] This solution is consistent with Clause 14(d) of Commission Implementing Decision (EU) 2021/914.

Union harmonisation legislation – Annex II

In contrast to the Parliament, the Council's position broadens the Commission's initial proposal for AI systems subject to Annex II. Similar to the Annex III assessment, we propose that the output of an AI system, whether as an essential safety component or a standalone product, should directly impact safety, or materially influence decisions regarding safety, for the AI system to be considered high-risk.[10]

Alignment with horizontal and sectoral legislation

Europe possesses a comprehensive framework of horizontal and sectoral legislation addressing aspects covered by the AI Act. It is therefore crucial to ensure coordination with existing and upcoming legislation to prevent excessive burdens on heavily regulated products and sectors.

For example, with respect to horizontal legislation, we note that the inclusion of AI systems intended for 'influencing elections' and recommender systems in Annex III would duplicate due diligence obligations already covered by the Digital Services Act within a broader risk management framework.[11]

Existing sectoral regulations, ranging from product legislation in sectors such as healthcare and machinery, to finance, are often well-developed in addressing AI-related issues and regularly undergo review and updating. Their principles and objectives are aligned with the AI Act's goals, particularly regarding health and safety.

When introducing new safety requirements, the AI Act should not disrupt existing sectoral product frameworks and their supporting infrastructure under the New Legislative Framework (NLF), including notified bodies and market surveillance authorities.[12]

Whilst the AI Act proposal mentions in principle that compliance with its requirements shall be checked within relevant sectoral conformity assessment procedures, Art. 43(3) is insufficient to achieve this in practice. It does not adequately address the potential misalignment with existing sectoral governance and enforcement frameworks.

In terms of governance, companies should be able to maintain their relationships with bodies familiar with sector and industry specificities. It is essential to prevent the need for redesignation under the AI Act of already-designated notified bodies, which would instead be required by Art. 43(3).

[10] In this context, it is crucial to distinguish between safety and security, including cybersecurity. AI-powered cybersecurity tools operating at a distance from operational safety systems should not fall within the same high-risk category as safety components.

[11] Regulation (EU) 2022/2065.

[12] https://single-market-economy.ec.europa.eu/single-market/goods/new-legislative-framework_en.

Some sectors are already facing bottlenecks due to a lack of notified bodies' capacities, which could worsen if redesignation is required.[13]

Regarding enforcement, companies may encounter different market surveillance and post-market monitoring regimes, leading to difficulties in navigating various authorities. This will result in different and overlapping rules related to incident reporting, non-compliance, recalls, penalties, etc.

To address these issues, we appreciate the Parliament's efforts to acknowledge, in Art. 8(2a), that certain requirements of the AI Act may have already been adequately addressed in the legislation listed in Annex II, section A. This recognition is vital to prevent duplicative efforts in parallel conformity assessment procedures and other implementation processes.

However, the proposed solution that requirements not addressed by Annex II legislation should be 'incorporated' into such legislation 'where applicable' is unclear and might imply the need to revise the relevant Annex II legislation, reopening multiple pieces of legislation, including on medical devices, machinery, radio equipment, toy safety, etc.

To ensure the AI Act's compatibility with existing sectoral frameworks and preserve the overall coherence of NLF legislation, we recommend explicitly recognising that the governance and enforcement frameworks of legislation listed in Annex II, section A, are to be used when assessing and applying any AI Act requirements and obligations. This includes following existing conformity assessment procedures mentioned in Art. 43(3) and automatically recognising existing sectoral notified bodies and market surveillance authorities to extend their conformity and compliance activities to the requirements and obligations set in the AI Act.

Requirements for high-risk AI

To enhance compliance, the requirements established for high-risk AI systems must be technically feasible and less burdensome for stakeholders.

Avoiding double regulation and ensuring alignment with existing horizontal and sectoral legislation, which already addresses quality and risk management, post-market surveillance, corrective actions, technical documentation and record-keeping, is crucial. As argued in the previous section,[14] notified bodies and market surveillance authorities under sectoral legislation will be best placed to ensure alignment between sectoral requirements and the AI Act. This is critical for avoiding redundancy and ensuring that the AI Act enhances rather than hinders existing regulatory frameworks.

[13] Recently there has been ample evidence of such challenges with the transition period for the medical device regulations, for which the Commission has had to propose a delay of at least three and a half years to fix ongoing issues with product assessments (Regulation (EU) 2023/607).

[14] See 'Alignment with horizontal and sectoral legislation' section above.

It is essential to reconcile different risk management approaches to prevent conflicts. In line with the NLF, the risks evaluated should primarily pertain to the health and safety of natural persons. This approach allows for measurable and defined product-related safety and health issues, whilst fundamental rights are more subjective and case-specific.

Whilst certain proposals by the Parliament, such as expanding fundamental rights to cover equal access and opportunities, the rule of law and the environment, have commendable aims, their technical enforcement could be challenging and may impede overall compliance.

Before introducing environment-related provisions suggested by the Parliament, like the logging of energy consumption by design under Art. 12(2a) and the eco-efficient design of foundation models in Art. 28b(d), it is crucial to assess how to leverage existing and future standards. This evaluation should aim to minimise the risk of overlapping regulations that could create conflicting demands with the existing sustainability framework (such as the Energy Efficiency Directive, the Ecodesign Regulation, and the EU Corporate Sustainability Reporting Directive) and industry initiatives like the European Green Digital Coalition.[15]

Moreover, certain requirements, such as risk management and record-keeping, should be limited to the relevant moment in the AI system's lifecycle when their implementation is most pertinent.

Allocation of responsibilities

We advocate for flexibility in the allocation of responsibilities along the AI value chain, allowing actors to assign compliance duties to those best suited to ensure adherence, particularly through contractual obligations.

The Parliament's approach in Art. 28, where the entity deciding to modify a non-high-risk AI system in a way that makes it high-risk becomes a provider and assumes responsibilities, is commendable. However, including a related recital to illustrate the assistance that high-risk AI system providers may offer to downstream operators for compliance could enhance clarity.

Nevertheless, obligations should remain proportionate. In this context, we are particularly concerned by the fundamental rights impact assessment for deployers suggested by the Parliament.

Compliance with the AI Act inherently aims to protect fundamental rights and assess potential risks, based on providers' risk assessments. Requiring an additional impact assessment on the part of deployers is unnecessary at best.

[15] Directive (EU) 2023/1791, Directive 2009/125/EC and the proposed new Ecodesign for Sustainable Products Regulation (COM/2022/142 final), and Directive (EU) 2022/2464, respectively. More information on the European Green Digital Coalition is available at https://www.greendigitalcoalition.eu/.

This requirement may not be relevant for many applications, such as industrial and business-to-business (B2B) AI systems. In addition, and importantly, it overlaps with data protection impact assessments already required under the General Data Protection Regulation (GDPR),[16] adding a substantial compliance burden without significantly improving safety. At a minimum, if multiple assessments are mandated in the final text, there should be explicit provisions to allow their combination, streamlining the compliance process.

General-purpose AI

The Council and Parliament hold different perspectives on how to regulate general-purpose AI (GPAI), given the rapid rise and increased public awareness of foundation models and applications like ChatGPT. In is important to consider that these rules were not analysed in the Commission's impact assessment, and that there is limited data available to comprehend the potential economic impact of adding provisions targeting GPAI systems.

It is challenging to predict which institution's position will be most effective in regulating GPAI without stifling innovation. However, it is essential to remain consistent with the AI Act's spirit and its technology-neutral and risk-based approach, to ensure that the regulation is future-proof.

To adhere to the risk-based approach, we should not treat all systems without an intended purpose as high-risk, as suggested in the Council's position in Arts 4b and 4c, which notably allow providers to explicitly exclude high-risk uses.

However, by focusing on GPAI 'which *may* be used as high-risk AI systems,' the Council's approach deviates from the risk-based core of the AI Act by potentially requiring all GPAI systems to conform to strict requirements initially reserved only for high-risk systems, depending on the Commission's future assessment through implementing acts.

Following the framework set out by the initial Commission proposal, only AI systems falling within the high-risk categorisation, as defined by Art. 6, should adhere to requirements proportional to the risk level of the specific use case.

Given that GPAI systems are purpose agnostic, imposing requirements solely at their level will not be sufficient to comprehensively evaluate and mitigate many downstream risks. Deployers of GPAI systems are best positioned to comply with the full requirements of the AI Act, but GPAI providers should support compliance activities through documentation and information sharing.

The AI Act should encourage cooperation and support across the GPAI value chain, including allowing contractual arrangements to elaborate further on relevant compliance activities. This collaborative approach would promote

[16] Regulation (EU) 2016/679.

responsible use and development of GPAI whilst maintaining the flexibility needed for innovation.

Foundation models

The Parliament, through a new Art. 28b, introduces requirements for providers of foundation models, irrespective of their risk level.

Foundation models, particularly in generative AI, are still in the early stages of development. Many companies are exploring the possibilities of these models and potentially designing their own. Imposing challenging requirements unrelated to the risk level may hinder the emergence of innovative AI applications in Europe, especially for B2B and industrial purposes.

As currently written, most proposals in Art. 28b risk being disproportionate. Whilst some level of risk management, due process, data governance and cybersecurity are essential, any such requirements should be high-level, indicative and aligned with the state of the art in their respective areas. If pursued, these requirements should be practical and extend only to what foundation model providers can reasonably address during design and development. Any requirements that are applied at the model level must be calibrated to model-level risks within the control of the model developer, as risks are often context and use-case specific. A model developer cannot mitigate all risks that all AI systems built on top of the model may pose, given the way they are shaped by decisions taken by downstream developers or deployers.

Overall, as for GPAI, there is value in supporting cooperation and compliance activities across the value chain, particularly via documentation and information sharing. Providers should also be encouraged to invest in the research and development of best practices in areas such as cybersecurity and data governance. Facilitating the publication and peer-review of findings and procedures contributes to transparency, fostering an environment where risk management can continually enhance and evolve.

Concerning generative AI in particular:

- The Parliament introduces transparency requirements for the use of copyrighted data to train AI systems, despite the existing comprehensive copyright protection and enforcement framework in the EU. This framework notably contains provisions that can help address AI-related copyright issues such as the text and data mining exemption and corresponding opt-out for rightsholders in Art. 4 of the Copyright Directive.[17] This additional legal complexity is out of place in the AI Act, which is primarily focused on health, safety and fundamental rights.

[17] Directive (EU) 2019/790.

- Transparency and content safety requirements should be use-case dependent and, where relevant, fulfilled by deployers, who have a better understanding of the final use and context of these systems (for example, a customer service chatbot as opposed to a medical diagnosis tool), not foundation model providers.
- Whilst state-of-the-art tools are being developed that allow for digital watermarking of audio-visual and image content, so that people could know when such content is artificially generated, the dynamic interaction between text-based AI generated content and user editing and refinement makes labelling such content more difficult. In this case, the transparency requirements in Arts 52(1) and (3), as proposed by the Parliament, are much less relevant.

Overall, a balanced and context-aware approach is needed to ensure the responsible development and deployment of foundation models and generative AI.

Implementation

Standardisation

The AI Act relies on the use of voluntary harmonised standards to facilitate the conformity assessment process, a stance we strongly support. It is crucial that these standards are ready and available well before the AI Act's requirements come into effect, providing companies with ample time to integrate them into their business development processes. Recognising the diversity of sectoral and organisational approaches to standards, particularly in industrial, financial and healthcare sectors, is equally important.

Alignment with sectoral legislation is paramount, and flexibility to produce standards tailored to sectorial needs or provide derogations should be available when alignment is not feasible. Ideally, AI Act harmonised standards should have a horizontal basis, with additional details accounting for sector-specific nuances when relevant. Leveraging existing sectoral standards and ensuring compatibility with them is crucial for a cohesive regulatory framework.

Harmonised standards should be aligned with international ones to avoid harmful divergence from global taxonomies and approaches. Such divergence could impact European companies' ability to operate beyond the EU market and hinder our capacity to build trust in AI worldwide.

The Commission's power to adopt common specifications as opposed to harmonised standards should be strictly limited, if not excluded. Common specifications reduce industry's capacity to develop practical solutions in line with international standardisation practices, resulting in harder-to-implement and lesser-quality specifications. Their adoption should follow intensive consultation with the AI Board, European standardisation organisations and relevant stakeholders to ensure their practicality, effectiveness and alignment with industry needs and best practices.

Measures in support of innovation

The AI Act has the potential to significantly impact the deployment of AI systems in Europe, and most importantly European companies' ability to develop them here. The AI Act must not only focus on preventing risks, but on fostering innovation.

To achieve well-balanced regulation, a range of regulatory and co-regulatory tools should be developed through collaborative, multi-stakeholder policy prototyping. Stronger sandboxes can contribute to forming better, more future-proof policy recommendations and drive innovation in a protected environment, providing valuable insights for all stakeholders. These processes should explicitly contribute to the evaluation and review process outlined in Art. 84.

Regulatory sandboxes should be systematically established across Europe, with their implementation being compulsory for each Member State. Incentives, such as a presumption of conformity upon successful exit, should be provided to participating businesses, creating a supportive environment for testing and learning. Participants in the sandboxes may be held liable during the process, but no penalties should be imposed on providers who follow the agreed-upon initial plan with competent authorities. Additionally, testing in real world conditions should be possible as an alternative to sandboxes, provided selected conditions are fulfilled.

Whilst supporting these innovation-friendly measures, it is essential to avoid fragmentation in the implementation and operation of sandboxes, considering their national, regional and local competence. Best practices should be shared amongst Member States to ensure consistency and effectiveness, especially concerning participation incentives for companies and expected outcomes.

To offset potential negative impacts on innovation, the AI Act should be accompanied by the rollout of a robust investment plan across Europe, with specific funding dedicated to start-ups and SMEs. This investment plan would help support and stimulate innovation in the AI sector, fostering growth and competitiveness in the European market.

Governance

To monitor technological developments, coordinate enforcement, and achieve the goals of the AI Act and support Member States in its implementation, a centralised European level represented by the AI Board or Office, is crucial. However, for it to be effective, continuous and constructive exchanges with industry stakeholders and civil society must be ensured.

The AI Act proposal grants significant freedom to Member States' market surveillance and other competent authorities, which may lack sufficient supervisory expertise to assess the AI Act's high level of complexity. This could potentially lead to fragmentation of the single market, contrary to the AI Act's objective of enforcing horizontal rules before individual countries legislate. Therefore, the Parliament's approach to enforcement, where Member States designate a single national supervisory authority ensuring coordination, is welcomed. This is in contrast to the Council and Commission proposals, where each Member State can designate multiple national competent authorities.

In addition, the AI Board and the Commission, in close cooperation with industry and civil society, should play a key role in coordinating and advising Member States. They should possess the necessary powers to ensure consistent application of the AI Act throughout the EU. This coordination and advisory role is crucial to avoid inconsistencies and ensure a harmonised approach in enforcing the rules.

Enforcement

It is crucial to establish EU-wide safeguards against disproportionate and unjustified decisions by national authorities. Harmonised best practices should be defined for specific actions, such as requesting corrective measures or the withdrawal of AI systems, even if they are compliant. In this context, we support the Parliament's proposal, which explicitly establishes rights to lodge complaints and receive effective judicial remedies against supervisory authorities.

However, care must be taken to align with what is technically feasible and not infringe on national competences, such as civil law and liability regimes, when considering proposed articles on collective redress and the right to explanation of individual decision-making.

Access to the AI system's proprietary source code and training or trained models should be the last resort, only pursued when all alternative options have been exhausted. All requests for data to providers and deployers should be limited to what is strictly necessary for assessing the perceived risk, and this data should be deleted when no longer needed for its initial purpose.

Penalties and their enforcement should show leniency for formal non-compliance, especially for SMEs and start-ups that may lack sufficient resources to navigate extensive frameworks like the present Regulation. Administrative fines should be contextualised based on aggravating or mitigating factors, and consideration should be given if a similar non-compliance infringement is already subject to relevant product safety legislation.

Both the Parliament and the Council propose that the Commission should adopt guidelines on the practical implementation of the AI Act, a stance we support. However, any guidelines should be co-developed in consultation with the AI Office/Board and industry, amongst other stakeholders, to ensure they are realistic and fit for purpose.

Enforcement should not be retroactive, following the initial Commission proposal, to avoid market confusion and maintain predictability for companies regarding legal impacts on providers and deployers.

Lastly, to provide ample time for the readiness of the entire ecosystem, the necessary infrastructure and the publication of relevant harmonised standards, the transitional period to implement and apply the AI Act should be at least 48 months. This extension would facilitate compliance and support a smooth transition for businesses.[18]

FOR MORE INFORMATION, PLEASE CONTACT:

Julien Chasserieau

Senior Manager for AI & Data Policy

julien.chasserieau@digitaleurope.org / +32 492 27 13 32

Bianca Manelli

Officer for AI & Data Policy

bianca.manelli@digitaleurope.org / +32 499 71 28 89

Alberto Di Felice

Director for Infrastructure, Privacy and Security Policy

alberto.difelice@digitaleurope.org / +32 471 99 34 25

[18] As previously noted, the Commission has had to propose a delay of at least three and a half years to the transition period for the medical device regulations, to fix ongoing issues with product assessments (Regulation (EU) 2023/607).

About DIGITALEUROPE

DIGITALEUROPE is the leading trade association representing digitally transforming industries in Europe. We stand for a regulatory environment that enables European businesses and citizens to prosper from digital technologies. We wish Europe to grow, attract, and sustain the world's best digital talents and technology companies. Together with our members, we shape the industry policy positions on all relevant legislative matters and contribute to the development and implementation of relevant EU policies, as well as international policies that have an impact on Europe's digital economy. Our membership represents over 45,000 businesses who operate and invest in Europe. It includes 105 corporations which are global leaders in their field of activity, as well as 41 national trade associations from across Europe.

DIGITALEUROPE Membership

Corporate Members

Accenture, Airbus, Applied Materials, Amazon, AMD, Apple, Arçelik, Arm, Assent, Autodesk, Avery Dennison, Banco Santander, Bayer, Bosch, Bose, Bristol-Myers Squibb, Brother, Canon, CaixaBank, Cisco, CyberArk, Danfoss, Dassault Systèmes, DATEV, Dell, Eaton, Epson, Ericsson, ESET, EY, Fujitsu, GlaxoSmithKline, Google, Graphcore, Hewlett Packard Enterprise, Hitachi, Honeywell, HP Inc., Huawei, ING, Intel, Johnson & Johnson, Johnson Controls International, Konica Minolta, Kry, Kyocera, Lenovo, Lexmark, LG Electronics, Mastercard, Meta, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe, NEC, Nemetschek, NetApp, Nintendo, Nokia, Nvidia Ltd., Oki, OPPO, Oracle, Palo Alto Networks, Panasonic Europe, Pearson, Philips, Pioneer, Qualcomm, Red Hat, RELX, ResMed, Ricoh, Roche, Rockwell Automation, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Siemens Energy, Siemens Healthineers, Skillsoft, Sky CP, Sony, Sopra Steria, Swatch Group, Technicolor, Tesla, Texas Instruments, TikTok, Toshiba, TP Vision, UnitedHealth Group, Visa, Vivo, VMware, Waymo, Workday, Xerox, Xiaomi, Zoom.

National Trade Associations

Austria: IOÖ
Belgium: AGORIA
Croatia: Croatian Chamber of Economy
Cyprus: CITEA
Czech Republic: AAVIT
Denmark: DI Digital, IT BRANCHEN, Dansk Erhverv
Estonia: ITL
Finland: TIF
France: AFNUM, SECIMAVI, numeum
Germany: bitkom, ZVEI
Greece: SEPE
Hungary: IVSZ
Ireland: Technology Ireland
Italy: Anitec-Assinform
Lithuania: Infobalt
Luxembourg: APSI
Moldova: ATIC
Netherlands: NLdigital, FIAR
Norway: Abelia
Poland: KIGEIT, PIIT, Digital Poland Association
Portugal: AGEFE
Romania: ANIS
Slovakia: ITAS
Slovenia: ICT Association of Slovenia at CCIS
Spain: Adigital, AMETIC
Sweden: TechSverige, Teknikföretagen
Switzerland: SWICO
Turkey: Digital Turkey Platform, ECID
Ukraine: IT Ukraine
United Kingdom: techUK