DIGITALEUROPE

6 AUGUST 2021

DIGITALEUROPE's initial findings on the proposed AI Act

Key messages

DIGITALEUROPE welcomes the European Commission's legislative proposal for a Regulation laying down harmonised rules on artificial intelligence ('AI Act'). We have been a key partner to EU institutions on AI topics for years, having notably participated in the work of the Commission's AI High-Level Expert Group. We are committed to keep supporting EU policymakers and to actively participate in the policy and technical discussions surrounding AI.

In this document, we present our initial assessment of the proposed AI Act, which will be complemented by an in-depth analysis with concrete recommendations at a later stage.

Find below an overview of our initial findings:

- The overall objectives and **focus on high-risk cases is appropriate**.
- The **scope needs to be further refined** to ensure legal certainty.
- Some of the **requirements will be difficult to implement**, especially if no harmonised standards are available.
- The **allocation of responsibilities between providers and users should be reassessed** to best reflect the complexity of AI systems and their value chain.
- **Applying the EU product safety approach** (New Legislative Framework) **to AI will be challenging** for most companies, particularly smaller software providers.
- **Effective safeguards and coordination measures would help mitigate fragmentation**, regulatory divergence and differing implementation by national authorities.
- **High compliance costs and paperwork are expected**, which would negatively impact businesses, particularly SMEs and start-ups.

DIGITALEUROPE
Rue de la Science, 14A, B-1040 Brussels
T.+32 (0) 2 609 53 10 / www.digitaleurope.org / @DIGITALEUROPE
EU Transparency Register: 64270747023-20

Definitions, scope & high-risk use cases

Definition of AI

The definition of 'artificial intelligence'[1] set in the AI Act is too wide. The proposed definition encompasses many software technology applications, even when they pose no major concerns around data, opaqueness, safety and reliability. It notably includes within AI techniques "logic-based and statistical approaches, Bayesian estimation, search and optimisation methods".

Considering these rather "basic" algorithms as AI dramatically increases the scope of the legislation. This would create legal uncertainty for companies, requiring them to assess if their software, which conventionally would not be considered an AI system, may still fall within the legislation's scope.

One potential solution could be for the AI Act definition to only refer to those AI algorithms and techniques that may be posing a potential high risk due to their evolving nature or other aspects of their functioning.

Scope

The general scope and focus of the AI Act on high-risk use cases and applications is the right approach. If done right, focusing on actual purpose of the AI system's use will ensure that new obligations are linked to cases where there could indeed be new risks, while avoiding more regulation on low-risk and ancillary or trivial AI systems, beyond the already robust EU safety legislation framework.

The scope[2] of the AI Act should be further improved for legal clarity and to avoid any overlap with the New Legislative Framework (NLF) and other legislation.

Links with existing legislation

The AI Act builds on the New Legislative Framework (NLF), which is the basis for product compliance in the EU. The NLF legislation guarantees the safety of ICT products, correctly implemented through either third-party conformity assessments or self-assessments, with the use of harmonised standards. The AI Act, through its 'AI system' definition, extends this approach to embedded software as well as standalone AI software – this is a novelty for most NLF legislation.

However, while it is sensible to use existing legislation where possible, the exact scope and relation to existing NLF rules should be further detailed (such as how

[1] Article 3(1) and annex 1.

[2] Article 6 and annexes 2 and 3.

to determine whether an AI system is "intended to be used as a safety component of a product, or is itself a product").

It is crucial to align the AI Act with the existing pieces of legislation listed in the Act. For most of the NLF legislation, this means for instance ensuring that new requirements can be integrated into existing conformity assessments.

In the specific case of the Medical Devices Regulation (MDR) and the In-vitro Diagnostics Regulation (IVDR), there is a serious risk of misalignment and duplication. Because the proposed AI Act defines high-risk AI systems broadly, almost all medical device software may fall in its scope and be considered high risk, even though the MDR and IVDR already set extensive and detailed requirements (some going beyond what is proposed in the AI Act). Yet the proposed definitions and requirements are not aligned, or are missing (e.g. definition of 'risk'). For some devices, the proposed requirements may conflict with safety and performance requirements of the MDR and IVDR. This would lead to legal uncertainty for industry and competent bodies. It would also induce higher complexity and implementation costs for all healthcare actors (including hospitals, healthcare professionals and patients) and negatively impact the proper implementation of the MDR and IVDR.

In general, ensuring consistency and synergies with the overall EU legislative framework is key, from the General Data Protection (GDPR) for all the data and record-keeping provisions, to the EU Cybersecurity Act regarding cybersecurity measures and incident notifications from AI systems providers. Such considerations should also take into account future legislation impacting AI, namely the ongoing discussions on the proposed General Product Safety and Machinery regulations, but also the upcoming liability rules on AI.

Evidence-based high-risk use cases

The AI Act, in addition to adapting existing product safety legislation, also sets its own category of high-risk use cases[3]. We support having such a detailed list, as it demonstrates focus and foster legal certainty.

This list could be improved even further by being more concrete and thoroughly defined, to make sure that the AI systems covered do pose a high-risk and to avoid the unintended inclusion of non-critical systems or ancillary or trivial use of AI systems which pose no safety risk[4]. Further clarifying the scope of the list will prevent misinterpretation.

[3] Annex 3.

[4] For instance, annex 3(2) on the "management and operation of critical infrastructure", as written, could unintendedly include non-critical systems such as AI-supported office management solutions. Listing more concrete use-cases could help alleviate this problem.

To ensure legal certainty, the process of expanding the scope of this list should be further clarified. This includes outlining robust assessments showing evidence for any addition to the list, ensuring stakeholder involvement at an early stage, and providing a suitably long transition period.

Clearly defined prohibited practices

We fully recognise and support a ban on AI practices[5] that are proven to be particularly harmful and would go against European values. To ensure legal certainty, such prohibited practices should be clearly defined so that acceptable low or high-risk practices do not risk falling into the scope of the ban.

Requirements, obligations & compliance

Roles & responsibilities of providers & users

Following the principles of the New Legislative Framework (NLF), AI system providers will carry most obligations and requirements set in the AI Act[6].

However, this does not take into account the fact that many obligations and some of the requirements can in practice only be managed by the entity in control of the AI system and its usage in practice, which means the user. For instance, despite taking all necessary precautions by running a risk-management system and following the data governance requirements[7], a provider cannot reasonably foresee all potential uses of the system and what data will be used to (re-)train and feed the AI system. In some cases, joint work from different actors of the AI system value chain will be needed.

The provisions to shift responsibility from provider to user[8], seem insufficient to properly address this issue, especially when the AI system is developed and distributed according to a complex supply chain. We believe that the co-legislators should thus reassess the responsibilities and roles of providers and users to better reflect the reality of designing an AI system, compared to operating it. Ultimately, the AI Act should offer flexibility to allocate responsibilities to the actors that can most appropriately ensure compliance, notably by ensuring the freedom of the parties to allocate responsibilities through contractual obligations.

[5] Article 5.

[6] Chapters 2 and 3.

[7] Articles 9 and 10.

[8] Article 28.

Manageable requirements & obligations

The requirements and obligations should be better tailored to what companies can actually do to reduce risks and make their AI systems safer. As they stand, some of the requirements would be quite challenging to implement, or even impossible in some cases. This could lead to high legal uncertainty, significant costs and increased administrative burden for companies, and have the unintended consequence of hindering European innovation in AI, particularly by smaller and disruptive companies.

For example, the requirements that datasets must be 'relevant, representative, free of errors and complete' and have 'appropriate statistical properties'[9] would be almost impossible to achieve in practice, as:

- These are constantly moving and evolving targets: what is relevant and representative at a given time when developing the AI system will vary based on the use case. The user, rather than the provider, will often be best placed to assess this.
- There is no common understanding about what these requirements entail, and a lack of recognised methods to achieve the intended results. The notions of completeness and ensuring a zero-error rate are also subject to varying interpretations.

Additionally, it is important to note that AI systems may sometimes need to be trained with erroneous or incomplete datasets, to ensure their overall robustness to be deployed in the field – in practice, data used will not be akin to the cleaned and curated datasets from the development and testing phase.

Similar problems arise with other obligations and requirements set in the proposal, on transparency, oversight, accuracy, robustness and cybersecurity, etc.

Compliance

Complex & costly procedures

The proposed compliance framework, while inspired by the existing NLF and EU market access legislation for products, will create complex procedures and bureaucracy, unfamiliar to many businesses, particularly SMEs, start-ups and software developing companies.

Compliance costs would be extremely high. Those would not be one-off costs, due to the important monitoring and reporting obligations, and because of the need for

[9] Article 10(3)

carrying new conformity assessments if the AI systems undergo substantial modifications[10].

Demonstrating compliance

As said before, the AI Act's compliance framework is inspired by the EU's product compliance system, known as the New Legislative Framework (NLF).

With the NLF, the EU legislation sets out essential requirements for product safety, which are then translated into practical technical standards by industry and other stakeholders within standardisation organisations. Companies apply these standards as part of their product design and development processes to be considered in conformity with EU legislation. There is generally no need for third-party conformity assessments to ensure that products being placed on the EU market are safe, except in specific sectors[11]. Market surveillance authorities only have to act in the unlikely event that problems arise (for instance because standards were not correctly implemented).

Applying the NLF approach to AI raises new challenges to address, as the proposed AI Act concerns the protection of fundamental rights as well as product safety. While product-related safety and health issues can usually be measured and defined, risks to fundamental rights are more subjective and use case specific. The provider, subject to the market access obligations, will often not be in a position to even assess these aspects.

In several instances, some features of the product compliance framework are not adapted to AI systems, which are originally software-based, even if they may be integrated into products. The proposal notably expands to all AI systems some "traditional" NLF elements such as the CE marking and the declaration of conformity, intended for physical products rather than for any type of software or service. Using the CE marking for AI software, and other various notification and registration duties, would often make little sense and would place disproportionate administrative burden on the large variety of providers.

Importance of harmonised standards

The proposal relies on the use of harmonised standards to facilitate the conformity assessment process, which we strongly support. To ease the standardisation process, the complex requirements and obligations of the AI Act should be more proportionate and flexible.

[10] The term 'substantial modification' as provided in article 3(23) needs further clarification.

[11] Under the MDR and IVDR, third-party conformity assessments are required.

Several of the requirements may be extremely difficult to turn into concrete technical standards and design instructions for AI system developers. Clearer and more practical requirements would help solve the technical challenge and quicken the overall standardisation process to fit the ambitious application timeline proposed by the Commission (2 years after the entry into force of the AI Act). The standardisation and overall implementation processes would benefit from a longer transition period.

The proposed alternative of using common specifications would not solve the abovementioned issues. On the contrary, it would reduce the industry's capacity to develop practical solutions in line with international standardisation practices, resulting in harder-to-implement and lesser-quality specifications.

Divergence from global standards and norms should be avoided as it would impact the ability of companies to operate beyond the EU market and their capacity to build trust in AI worldwide. The proposed European AI Board should therefore engage with international and European standardisation organisations to leverage existing activities and ensure alignment.

Market surveillance & fragmentation risks

The AI Act gives significant freedom to Member States' market surveillance and other competent authorities. This may create fragmentation of the EU Single Market, contrary to the AI Act's objective of enforcing horizontal rules before countries start legislating individually.

Requirements and obligations set in the Act should be clear enough to avoid creative interpretation by national notified bodies and authorities, and consistent with NLF legislation. To ensure proportionate enforcement, national authorities will need to develop the required AI expertise and allocate sufficient human and financial resources[12]. The European AI Board and the Commission, in close cooperation with the industry, should play a key role in coordinating and advising Member States, and possess the necessary powers to ensure consistent application.

It is particularly important to outline EU safeguards against disproportionate and unjustified decisions by national authorities. Harmonised best practices should be established when it comes to specific actions such as asking for corrective measures or the withdrawal of AI systems, even compliant ones. In addition, any access to AI systems' source code should be an absolute last-case resort, aligned with IPR legislation such as the Trade Secrets Directive, the TRIPS agreement

[12] For instance, notified bodies under the MDR and IVDR lack sufficient resources.

and relevant trade agreements[13]. Finally, rules regarding penalties for infringement should be aligned with existing practices under similar legislation such as the GDPR, and consistent across Member States.

Innovation-friendliness

Impact on smaller businesses

The proposed legislation outlines a complex compliance framework, which will create important administrative burden and costs for all companies. While large companies may be able to withstand the impact, smaller businesses developing AI systems do not necessarily have the capacity to deal with the high compliance costs and paperwork resulting from the provisions of the Regulation.

A simplification and clarification of the overall framework, combined with sufficient support measures, especially for SMEs and start-ups, would ensure that the whole European AI innovation sphere remains competitive and attractive despite the challenges created by the AI Act. The impact could be similar to the costs which resulted from the implementation of the GDPR. The difference being that such costs would remain important due to the AI systems' lifecycle monitoring and reporting, and because each new AI system, or existing system with substantial changes, will need a new conformity assessment.

Sandboxes

DIGITALEUROPE strongly supports the AI Act's provisions[14] for building voluntary regulatory sandboxes for the development, testing and validation of innovative AI systems. However, we believe that the current proposal is not ambitious enough and may lead to potential fragmentation in their implementation and operation.

As set in the proposal, Member States' competent authorities or the European Data Protection Supervisor (EDPS) can develop sandboxes, but they have no obligation to do so. Therefore, it is likely that no such sandboxes will be ready before the entry into force of the Regulation's requirements. Additionally, the AI Board should have extended powers to oversee how sandboxes are managed and avoid national fragmentation.

[13] Such as the EU-UK Trade and Cooperation Agreement (article 207) and EU-Japan Economic Partnership Agreement (article 8.73).

[14] Articles 53 and 54.

DIGITALEUROPE looks forward to working with the European Parliament, the Council and the Commission to discuss and assess how to best improve and implement the proposed AI Act, so that it achieves its ambition of stimulating the development and uptake of trustworthy AI, in line with European values.

FOR MORE INFORMATION, PLEASE CONTACT:

Julien Chasserieau

Policy Manager for Data & Innovation

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

Lara Visser

Director for Digital & Green Transformation

lara.visser@digitaleurope.org / +32 493 89 20 58

About DIGITALEUROPE

DIGITALEUROPE represents the digital technology industry in Europe. Our members include some of the world's largest IT, telecoms and consumer electronics companies and national associations from every part of Europe. DIGITALEUROPE wants European businesses and citizens to benefit fully from digital technologies and for Europe to grow, attract and sustain the world's best digital technology companies. DIGITALEUROPE ensures industry participation in the development and implementation of EU policies.

DIGITALEUROPE Membership

Corporate Members

Accenture, Airbus, Amazon, AMD, Apple, Arçelik, Assent, Atos, Autodesk, Bayer, Bidao, Bosch, Bose, Bristol-Myers Squibb, Brother, Canon, Cisco, DATEV, Dell, Dropbox, Eli Lilly and Company, Epson, Ericsson, ESET, Facebook, Fujitsu, GlaxoSmithKline, Global Knowledge, Google, Graphcore, Hewlett Packard Enterprise, Hitachi, HP Inc., HSBC, Huawei, Intel, Johnson & Johnson, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, Mastercard, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe Inc., NEC, NetApp, Nokia, Nvidia Ltd., Oki, OPPO, Oracle, Palo Alto Networks, Panasonic Europe, Philips, Pioneer, Qualcomm, Red Hat, ResMed, Ricoh, Roche, Rockwell Automation, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Siemens Healthineers, Sky CP, Sony, Swatch Group, Technicolor, Texas Instruments, Toshiba, TP Vision, UnitedHealth Group, Visa, VMware, Waymo, Workday, Xerox, Xiaomi, Zoom.

National Trade Associations

Austria: IOÖ
Belarus: INFOPARK
Belgium: AGORIA
Croatia: Croatian Chamber of Economy
Cyprus: CITEA
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
Netherlands: NLdigital, FIAR
Norway: Abelia
Poland: KIGEIT, PIIT, ZIPSEE
Portugal: AGEFE
Romania: ANIS
Slovakia: ITAS
Slovenia: ICT Association of Slovenia at CCIS
Spain: AMETIC
Sweden: Teknikföretagen, IT&Telekomföretagen
Switzerland: SWICO
Turkey: Digital Turkey Platform, ECID
United Kingdom: techUK