Two Years of EU AI Act: What Can We Expect Moving Forward?

31 December 2023

Following the European Commission's ("EC") political approval of the European Union ("EU") artificial intelligence ("AI") Act (the "EU AI Act", "Act" or "Regulation")[1] after more than two years since the initial proposal in April 2021[2], AI & Partners provides input on the central elements of the EU AI Act[3] that can be a success alongside recommendations for how the EU AI Act can be triumphant. **These are based on an certain aspects of the ex-post exercise conducted by DIGITALEUROPE with regards to the General Data Protection Regulation ("GDPR")**[4].

Executive Summary

The EU AI Act's potential impact cannot be underestimated as its adoption represents a clear global milestone for AI rules. It not only stands to provide upgraded rights to consumers, but aims to harmonise the rules across Europe.

However, in light of Member States' stated attempts to ensure a consistent application of the law, fragmentation may arise, ultimately contradicting the harmonisation aim of the Regulation. The following report goes into detail on key elements of the EU AI Act, coming to the main following conclusions:

- Coordinated implementation across Member States is needed in order to create a truly harmonised legal framework.

- The AI Office ("AIO") (or suitable equivalent) should collaborate with industry and other stakeholders in producing essential guidance.

- For the EU AI ACT to be successful, it must be interpreted to suit modern-day developments, most notably the complexities brought about by emerging developments in AI and related technologies, such as blockchain and cloud computing.

[1] https://ec.europa.eu/commission/presscorner/detail/en/ip_23_6473
[2] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206
[3] European Parliament compromise text as adopted on 14 June 2023
[4] https://www.digitaleurope.org/resources/two-years-of-gdpr-a-report-from-the-digital-industry/

Consistency and Harmonisation

Differing Interpretations by Supervisory Authorities

Harmonisation of the EU AI Act across all Member States can be achieved through cooperation between the NSAs, mutual assistances or joint operations. Where these mechanisms are insufficient to reach a consistent implementation of the EU AI Act across Europe, we urge for robust enforcement of the consistency mechanism.

At the moment, enforcement of the EU AI Act is not in force. For example, it remains unknown if the AIO can start a procedure even if the matter is of general importance or has implications in more than one Member State. For matters of general importance with implications across several Member States, we would recommend that the AIO be consulted.

It is possible that NSAs, within their respective areas of competence, start to take decisions on the enforcement of the EU AI Act that differ from decisions taken in other Member States on similar issues. For example, fines issued by NSAs may not rely on common EU adopted criteria. In case of a breach, it is unclear whether any individual suffered pecuniary loss or other distress as a direct result of the breach. This may affect in particular companies from the same industry active in different Member States (e.g. AI system deployer X is treated differently in country A than AI system deployer Y in country B). There may be a lack of consistency in fine calculation, with no common criteria across the EU.

Contrary to the myriad national approaches that exist at present, fine calculation methodology ought to be the result of a European consensus. Otherwise, there is a risk of jeopardising the harmonisation objective of the EU AI Act and creating considerable legal uncertainty for businesses and citizens. Different decisions have the potential for considerable influence on the profitability of business models and thus also jeopardise the desired 'level playing field.'

In addition, where accountability is clearly promoted by NSAs and understood by organisations as a factor in mitigating liability, this can generate a greater focus on accountability beyond a minimum standard, and this should also be taken into consideration when calculating fines.

There must be recognition of the added value of organisations being subject to an independent evaluation of their compliance with applicable AI laws, by way of independent certifications in particular. This non-legalistic and value-driven approach to regulating organisations promotes the value of trustworthy AI and of being accountable to both organisations and individuals.

We encourage independent attestation engagements to provide the highest possible level of assurance with regard to the design, implementation and operating effectiveness of internal controls.

Uncertainties on Applicability of Member State Law and/or the EU AI Act

For companies that operate in more than one Member State, the most challenging circumstance occurs when the laws of several Member States may apply to the same deployer or developer. For example, if the AI system deployment takes place in the context of more than one establishment or takes place in the context of one establishment but involves offering goods and services to individuals in another.

The most obvious example of a potential conflict here is the vulnerability of the individual, but also the exemptions for individuals' fundamental rights and other issues. It is also unclear how the provisions of local law will operate in conjunction with enforcement action taken. Any appeal will be dealt with under the national procedures, leading to a situation where the national courts could render a regulator's decision redundant.

It is unclear how NSAs will deal with situations which require the application of Member State law, where this is not necessarily the national law of their own Member State. For example, where high-risk AI systems are deployed, this could trigger various domestic legal provisions, which would need to be applied by the NSA.

In addition, a deployer may deploy on behalf of firms who are not subject to the EU AI Act. Many deployer obligations only make sense if the deployer is also subject to the EU AI Act, but the obligations exist irrespective of this.

Sectoral Interpretation

Although the EU AI Act stands to improve AI system accountability and awareness, it may not address specific sectoral concerns. This can lead to areas where the application of the EU AI Act provisions is unclear. In this section, we identify potential challenges and barriers faced by specific sectors, namely healthcare and finance, and propose possible ways to mitigate these.

Clear guidance by the AIO and increased use of codes of conduct are among possible solutions which could bring more clarity to the applicability of the EU AI Act. It would also strengthen the overarching framework for the governance of AI system deployment, development and use in the EU that would boost growth and create value.

The EU 2030 Digital Decade Strategy[5] includes AI as a key driver for digital transformation of Europe in 2022. However, this driver and associated AI deployment across the EU can only happen once the EU AI Act's implementation and interpretation challenges are resolved.

Legal Fragmentation: Local Laws and Regulations

One key objective of the EU AI Act was to reduce fragmentation amongst EU Member States and provide legal certainty for individuals and businesses across the EU[6]. While the EU AI Act has the potential to contribute to this objective, it can have a margin for national legislators to maintain or introduce more specific provisions or further conditions to adapt the application of certain rules of the EU AI Act.

Consequently, these national margins may contribute to an even more fragmented legal landscape. For instance, Member States may maintain or introduce further conditions, including limitations, regarding:

- The EU AI Act allows Member States to maintain stricter rules with regard to the development, deployment and use of AI systems. This means that there may be no unified applicability of the EU AI Act across the EU. Foreseeably, it is not the EU AI Act that may restrict the deployment of AI systems in the healthcare sector, but rather the stricter Member State rules that deviate from the EU AI Act. This has can result in Member States adopting different approaches to deployment of AI systems in the healthcare sector, making it difficult to use AI systems with healthcare use cases, locally and in a cross-border context. The fragmentation of rules across the EU's internal borders makes it a complex challenge for organisations to pool AI systems from multiple Member States for a single project, especially in health-related scientific research.

[5] https://digital-strategy.ec.europa.eu/en
[6] https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence

- Use of AI systems in biometric identification contexts. Member States may implement more specific national rules to use high-risk AI systems where it is necessary for a legal obligation in the field of employment law. Divergence of national legal frameworks may create considerable hurdles for companies operating cross-border. For instance, some Member States may allow technical and organisational measures that are indispensable to comply with security and breach notification requirements but undermine the protection of individuals' fundamental rights. Some of these measures may not lawfully be implemented in other Member States, as they may violate some national employee data protection laws.

- Similarly to the European Data Protection Board's ("EDPB") guidelines on various aspects of the GDPR[7], guidance from the AIO (or equivalent) can be specifically addressed to AI system deployers that would help deal with the potential fragmented approaches between Member States.

The EU AI Act and national rules complementing are on the precipice of being applicable. However, there remains a possibility for sector-specific legislation being revised in many Member States. Therefore, there is a need for clarity and guidance on Member States' plans for EU AI Act implementation, such as via the use of the AI Pact[8]. **In addition to removing fragmentation, further clarification of the rules will also help to build trust in the AI economy**.

For example, in the financial sector, although the EU AI Act may not be in direct tension with open banking, there is possibility for a lack of public understanding about how the technology behind open banking works, which can lead to fear and uncertainty about the use of AI systems in an open banking context. More general guidance around best practices for trustworthy AI-compliant practices within the financial sector would be welcomed.

Codes of Conduct

Future reports from the EC's evaluation reports (and other assessment mechanisms) can also highlight how codes of conduct could take into account the similarities in AI system deployment processing within and between some sectors as a suitable way to contribute to the proper application of the EU AI Act.

High-Risk AI System Deployment in the healthcare sector

A narrow interpretation of high-risk AI systems creates potential barriers for their deployment in the healthcare sector. Specifically, pre- and post-market deployment obligations must be satisfied in order for AI systems to be used for legitimate, lawful purposes. This is very onerous and often resource intensive, especially where there is an immediate market need.

A broader assessment of high-risk AI system deployment vis-à-vis other legal bases would be useful in this respect. An alternative ground for certain types of high-risk AI system deployment could be public or legitimate interest. The AIO could consider multiple bases that serve as a legal basis for deployment if it is combined with appropriate conditions and safeguards. Further guidance and clarity from the AIO on these would be welcomed.

[7] https://edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_en
[8] https://digital-strategy.ec.europa.eu/en/policies/ai-pact

Codes of Conduct and Certification

Codes of conduct and trustworthy AI certifications, seals and marks are ways for organisations to demonstrate their commitment to, and compliance with, the EU AI Act. They can help deployers and developers demonstrate trustworthy AI in a practical, objective way to all stakeholders including clients, customers, partners, employees and regulators.

Codes of Conduct

Successfully adhering to a code of conduct demonstrates that an organisation has a competent understanding of how to apply the EU AI Act in practice. Codes are rigorous accountability exercises for adherents and serve to increase transparency. Given the value that codes of conduct have to offer, it is critical to improve the current approval process.

To avoid a similar instance where the EDPB's guidelines and accreditation process for monitoring bodies[7] lead to fragmentation and slowed down the whole process, each Member State should not be required to submit its individual accreditation requirements to the AIO for its opinion. This can avoid a situation where, for example, a Member State's requirements do not take into consideration the unique needs of micro, small, and medium-sized enterprises ("SMEs").

A more streamlined approach, in which all accreditation criteria of all Member States would be assessed together, would result in an EU-wide applicable accreditation requirement. This would shorten the overall procedure and greatly improve European harmonisation.

Accreditation requirements for codes of conduct should reflect the needs of different stakeholder groups and take a risk-based approach that considers the type of AI systems deployed, the size of the code members and the governance arrangements. Too stringent accreditation requirements for a monitoring body would make it impossible to elaborate small-scale codes of conduct.

Finally, the EU AI Act may not limit a code's applicability to a specific industrial sector, and consideration should be given to codes of conduct that span multiple industry sectors and relate to similar AI system operations.

Certification

We encourage the efforts of NSA, the AIO, the EC and industry on the issue of certification. However, we are concerned that the flexibility available for the creation of EU AI Act certifications, seals and marks may lead to unnecessary duplication and further fragmentation by Member States.

We urge that European certification mechanisms should replicate already internationally recognised and widely adopted standards. This approach comes with many advantages, such as:

- Improving cooperation amongst European and international DPAs, reducing unintended barriers for companies by proving accountability in home jurisdictions;
- Providing European-certified organisations with an international competitive advantage; and
- Faster adoption as new mechanisms will not need to reinvent the wheel but will build upon already implemented ones.

Implementation must be practical for all organisations, irrespective of size. Whilst many organisations have adopted various accountability mechanisms, these may not adequately address the requirements of companies throughout the supply chain, many of whom are SMEs.

Certification criteria should reflect the needs of different stakeholder groups and risk factors. Consideration should be given to a certification regime to account for organisations of all sizes and the full range of risk factors. This view supports the EU AI Act requirements that the specific needs of SMEs be accounted for.

Conclusion

The importance of the EU AI Act cannot be understated. One of the core purposes of the EU AI Act is to create one harmonised AI landscape across all Member States – a cornerstone for the achievement of Europe's 'Digital Single Market.' Although in many respects the EU AI Act can achieve this goal, there are some gaps that need to be addressed in order to prevent potential fragmentation in the EU.

We believe that the EU AI Act as a legal mechanism is robust and fit for purpose in facing the challenges of the future, such as the widespread roll out of AI. However, it is important that the EU AI Act, as with the GDPR, be fully implemented across the EU and that Member State derogations be minimised, including through NSA cooperation and coordination. **In addition, we welcome the AIO's role in producing reliable EU AI Act guidance and that stakeholders continue to have the opportunity to provide input.**