BCLP. Client Intelligent

Insights

A GDPR FOR AI? POLITICAL AGREEMENT REACHED ON THE EU AI ACT

Dec 12, 2023

WHAT DO WE KNOW NOW?

This directly-applicable regulation takes a risk-based approach and applies across all sectors (i.e. horizontally). Like the original European Commission text from 2021, the agreed AI Act is understood to set out tiers of AI systems, based on risk:

1. Prohibited AI: deemed to be unacceptable and banned outright;
2. High-risk AI: such as systems used to manage or monitor employees, in an educational training setting, in medical devices or critical infrastructure;
3. Minimal risk AI: the majority of current AI systems fall into this category, e.g. AI-enabled spam filters or recommender systems;
4. Specific transparency risk: e.g. chatbots or deep fake generated content, where users need to be aware that they are interacting with a machine or artificially-generated content.

Prohibited applications include:

- Biometric categorisation systems that use sensitive characterisations, e.g. political, religious, philosophical beliefs, sexual orientation, race
- Untargeted scraping of facial images from the internet or CCTV footage to create facial recognition databases
- Emotion recognition in the workplace or educational institutions
- Social scoring based on social behaviour or personal characteristics
- All systems that manipulate human behaviour to circumvent their free will
- AI used to exploit vulnerabilities of people (due to their age, disability, social or economic situation)

A wide range of high-risk systems may be authorised, if they meet a set of requirements and obligations in order to access to the EU market. These requirements include risk-mitigation systems, high quality data sets, logging of activity and documentation, human oversight and clear user information. In this area, the requirements have reportedly been clarified and adjusted during the recent trilogue negotiations and they are reported to be *"more technically feasible and less burdensome"*, e.g. in terms of the technical documentation to be drawn up by SMEs to demonstrate that their high-risk AI systems comply with the requirements. One additional requirement which MEPs successfully negotiated for inclusion was the requirement for a fundamental rights impact assessment to be conducted for high-risk systems.

In a significant change, real time biometric identification by law enforcement in publicly accessible spaces will now be permitted in exceptional circumstances. This will be subject to judicial authorisation, be limited in time and location and only for specific conditions, such as prevention of a specific and present terrorism threat.

NEW PROVISIONS AND DEFINITIONS

- The definition of AI has been aligned with the widely-used OECD definition. This is likely to help, in terms of conformity with other developing guidelines and frameworks.
- New provisions have been added to take into account situations where AI systems can be used for many different purposes (**General Purpose AI**) and situations where General Purpose AI is subsequently integrated into another high-risk system.
- Specific rules have also been agreed for **Foundation Models**, described as large systems capable of competently performing a wide range of distinctive tasks, such as generating video, text, images or computer code. Foundation models must meet specific transparency obligations before they are placed on the market. These will be required to adhere to transparency requirements, such as drawing up technical documentation, complying with EU copyright law and issuing detailed summaries about the content used for training.
- **High-impact Foundation Models**are called out for a stricter regime – these are Foundation Models trained with large amounts of data which have advanced complexity, capability and performance meaning they can disseminate systemic risks along the value chain. If these models meet certain criteria they will have to conduct model evaluations, assess and mitigate systemic risks, conduct adversarial testing, report serious incidents to the Commission, ensure cyber security and report on their energy efficiency.
- It's reported that changes have been made to clarify the allocation of responsibilities and roles of the various actors in the value chain, in particular, "providers "and "users" of AI systems . Also, we can expect increased clarity over the relationship with other legislation, e.g., data protection.

REGULATION AND ENFORCEMENT

- There will be a dual regulatory approach, with new EU institutions created, as well as enforcement by market surveillance regulators at member state level.
- An **AI Office** in the Commission will be set up to oversee the most advanced AI model standards and testing. The Office will have a **scientific panel of independent experts**. There will also be a **European AI Board** comprising member states' representatives to coordinate between the Commission and the member states. An **advisory forum** for stakeholders such as industry representatives, SMEs, civil society and academia will provide technical expertise to the AI Board.
- Maximum fines will be set at €35 million or 7% of global annual turnover, with a lower level for less serious infractions, such as the supply of incorrect information. The size of the company will also be a factor in determining the level of fine, with proportionate caps being proposed for SMEs and startups.
- Individuals (as well as legal persons) are entitled to make complaints and receive meaningful explanations about the use of AI systems.

PRO-INNOVATION

- A number of measures have been agreed, directed at supporting innovation, to encourage AI development by SMEs in the EU. MEPs wanted to ensure that businesses, especially SMEs, can develop AI solutions without undue pressure from industry giants controlling the value chain. It has been clarified that AI regulatory sandboxes (to establish a controlled environment for developing, testing and validating innovative AI systems) shall also allow for testing in real world conditions, under specific safeguards. Administrative burdens for smaller companies will also be reduced, through some clearly defined exceptions.
- The AI Act will not apply to AI systems used for the sole purpose of research and innovation (another potentially pro-innovation position), or for people using AI for non-professional reasons.

NEXT STEPS

The political agreement is now subject to formal approval by the European Parliament and the Council and will entry into force 20 days after publication in the Official Journal. The AI Act would then become applicable two years after its entry into force, except for some specific provisions (prohibitions will apply after 6 months and the rules on General Purpose AI will apply after 12 months).

The Commission has announced it will be launching an AI Pact to bridge the period before the AI Act becomes applicable. It will convene AI developers from Europe and around the world who commit on a voluntary basis to implement key obligations of the AI Act ahead of the legal deadlines. The Commission proposes bringing interested parties together in the first half of 2024.

COMMENT

The detail of the final agreed text will be important for its impact. The regulation seeks to strike a balance between protecting fundamental rights without stifling the ability of EU organisations, especially SMEs and startups, to innovate and create an EU-based AI sector capable of competing with world leaders, such as the U.S. In particular, stakeholders will want certainty when they are assessing which tier their AI deployment falls within (and therefore the obligations to bring it to market) and when assessing the scope of their responsibilities and liabilities relative to other players, e.g. as providers versus users.

The inherently adaptable nature of this powerful technology, as well as the pace of development, means that legislators are aiming at a target that is not only moving, but accelerating into the future. Time will tell whether the EU can remain at the regulatory vanguard or falls behind through adopting an insufficiently agile instrument.

Political agreement was reached on 9 December in the negotiations on the EU AI Act, arguably the world's most comprehensive and ambitious AI law to date.

Some further steps must take place, including confirmation by the EU Parliament and Council, before the text is adopted and becomes law, but this ambitious legislation is expected to apply throughout the 27 member states of the EU. The AI Act would apply 24 months following its entry into force (with some exceptions for specific provisions), i.e., from 2026. It does not apply to areas outside the scope of EU law and should not affect member states' competences in national security. It will not apply to systems used exclusively for military or defence purposes.

RELATED PRACTICE AREAS

- Data Privacy & Security

MEET THE TEAM

Kate Brimsted

London

kate.brimsted@bclplaw.com
+44 (0) 20 3400 3207
