SLAUGHTER AND MAY/

CLIENT BRIEFING

5 MAY 2021

EUROPE'S GROUNDBREAKING DRAFT ARTIFICIAL INTELLIGENCE ACT: AN ANALYSIS

The EU broke new ground on 21 April 2021 by issuing the draft of its proposed harmonised legal framework on AI (the "AI Act"), the first attempt worldwide to specifically regulate this rapidly developing and often misunderstood branch of technology.

The proposal follows a wave of previous EU policy documentation addressing AI and directly builds on the Commission's high-level approach to a future EU regulatory framework for AI outlined in its White Paper issued on 19 February 2020 (see our blog on the White Paper here). The lofty ambitions of "excellence" and "trust" in the AI space outlined in the White Paper now form the core principles of the new framework. Another key aim of the EU is one of AI harmonisation. By its nature as a regulation (rather than a directive, for example), the AI Act will become directly applicable in all EU member states, which should help ensure that the national approaches to AI will not fragment across the single market.

The EU has requested feedback on its proposals, and organisations have until 29 June 2021 to respond.

What is AI? (in the EU's opinion)

AI goes beyond (and can be somewhat more mundane than) the humanoid robots portrayed in sci-fi films. In choosing to draft a technology-specific law, the EU was always going to face the challenge of defining AI to be both specific enough to create legal certainty, but broad enough to capture subsequent technological advancements which can occur at a rapid pace. Its proposed definition of an "AI system" aims to achieve this: *"software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with"*. Annex I (which the Commission can update over time) lists (i) machine learning approaches, (ii) logic and knowledge-based approaches, and (iii) statistical approaches. The EU's hope is that this will create current certainty by focusing on existing programming methods whilst also potentially covering a wide array of implementations of those methods and future advances in AI technologies. We will likely see amendments to the definition both as the AI Act progresses and following its implementation.

A risk-based approach

Like the GDPR, the AI Act takes a "risk-based" approach. It requires compliance to be treated differently based on the risks associated with the type of AI in question and identifies four risk categories.

- **Unacceptable risk** – certain types of AI are outright prohibited on the grounds that they violate the rights and freedoms of individuals. These include the use of subliminal techniques to manipulate humans or the exploitation of information about humans to target their vulnerabilities and materially distort their behaviour, each where likely to cause physical and psychological harm; and the use of AI by public authorities to assess trustworthiness. Interestingly, the use of real-time biometric authentication in public spaces for law enforcement purposes (i.e. facial recognition) is also included in this list of prohibited AI systems, but there are carve-outs permitting use for crime prevention and national security. Facial recognition is a key topic of debate in the privacy sphere (the EDPS has issued a statement on the AI Act stating that remote biometric identification in public spaces should be banned entirely) and will likely be a point of contention going forward.
- **High risk** - the other significant grouping is of "high-risk" AI systems which have an adverse impact on safety or fundamental rights. These are defined as (i) AI systems used as safety components of products, or which are products, covered by existing EU safety legislation and listed in Annex II (which include machinery, toys, radio equipment, gas appliances and medical devices); and (ii) certain additional AI systems listed in Annex III (which include those relating to real-time or post-time biometric identification, critical infrastructure, law enforcement and employment, and systems used to evaluate creditworthiness). This list can be added to by the Commission in the future. The bulk of obligations under the AI Act relate to such high-risk AI technologies, and span the categories of data

governance, technical documentation and record-keeping, transparency, human oversight, accuracy, robustness and cybersecurity. A key requirement will be the performance of conformity assessments prior to high-risk AI products reaching the market. The EU will keep a database of high-risk AI systems containing prescribed information which must be input by providers.

- **Limited risk -** there are also transparency obligations in respect of certain types of limited risk AI such as those which interact with natural persons or generate or manipulate content (e.g. chatbots and "deep fakes") in order to ensure individuals are aware they are interacting with machines.
- **Minimal risk -** providers of AI systems which do not fall into the above groupings and are therefore minimal risk are encouraged to nevertheless comply on a voluntary basis, for example via voluntary codes of conduct.

Who needs to comply?

The AI Act imposes obligations on a string of operators along the AI supply chain. The bulk of obligations are on AI providers. They must ensure their high-risk products comply with the regulation, undertake the relevant conformity assessments and monitor their products once on the market. However, distributors, importers and users may also be subject to obligations if they place a high-risk AI system on the market under their name or trademark, modify its intended purpose, or otherwise substantially modify it (upon which the provider's responsibilities will cease). Users will need to ensure compliance with instructions for any high-risk systems, and monitor the operation of and maintain logs for such systems going forward.

For providers in particular, these new obligations will be significant (particularly as their AI systems may also need to comply with other "technology neutral" laws such as the GDPR). Pushback from the tech sector can therefore be expected. The EU has acknowledged the particular challenge posed for SMEs and has proposed a network of "Digital Innovation Hubs" by way of support.

GDPR-level sanctions

The AI Act envisages a governance framework akin to the existing data protection governance framework, with a "European Artificial Intelligence Board" overseeing enforcement and the establishment of national supervisory authorities to apply the AI Act in their own jurisdictions. Crucially for businesses, these bodies will be able to enforce sanctions up to (and even above) GDPR-level. Breaches of the prohibition on AI technologies posing an unacceptable risk – which is a broad category, and encompasses technologies which are by no means unprecedented - could elicit fines of **the higher of EUR 30 million or 6% worldwide annual turnover**, which exceeds the maximum fines under the GDPR. Fines for any other breaches could be **the higher of EUR 20 million or 4% worldwide annual turnover** (GDPR-level), whilst the supply of incorrect, incomplete or misleading information to relevant bodies could result in fines of **the higher of EUR 10 million or 2% worldwide annual turnover**. Affected organisations will therefore need to take the AI Act seriously.

UK implications

Whilst the AI Act will not form part of UK law directly, it does have **extra-territorial effect**. It applies to AI providers offering AI systems within the EU (wherever those providers are located), and to AI providers and users outside the EU if the output produced by the system is used within the EU. UK businesses will therefore need to check whether they are caught by these provisions.

In addition, as well as the extra-territorial reach of the AI Act, those involved in AI supply chains could additionally find themselves subject to new UK legislation on AI in the near future. Digital Secretary Oliver Dowden recently announced that a new "National AI Strategy" for the UK will be published later this year which could outline the UK's own plans for legislative changes, and the Government recently listed "Unleashing the transformational power of tech and AI" as one of its "10 Tech Priorities."

The wider picture

The AI Act marks a bold statement by the EU on the world stage. Although the US and others are taking some steps to legislate AI (for example, by restricting the use of facial recognition technology), the level of obligations proposed by the AI Act is unparalleled in its scope and ambition. The EU has therefore further cemented its digital strategy as one which prioritises comprehensive regulatory frameworks aimed at preserving fundamental rights and ethical values, with the intention that trust in new technologies and innovation will flourish as a result.

Time will tell whether the EU's strategy will succeed. In the meantime, the AI Act will have its own legislative hurdles to overcome within the EU political process. It takes time to agree new law at EU level, and once agreed there will be a two year implementation period. It is therefore **unlikely we will see the AI Act implemented until 2024** at the earliest – but both the tech sector and broader sectors which use AI technologies should keep careful watch.

CONTACTS

Heather Catchpole
ASSOCIATE
T:+44 (0)20 7090 3177
E: heather.catchpole@slaughterandmay.com

Natalie Donovan
COUNSEL PSL
T:+44 (0) 20 7090 4783
E: natalie.donovan@Slaughterandmay.com

Rob Sumroy
PARTNER
T:+44 (0)20 7090 4032
E: rob.sumroy@slaughterandmay.com

Our emerging tech practice supports a wide range of clients, from established international financial institutions and global technology and telecoms providers, to investors, entrepreneurs and high-growth start-ups and market disruptors. We advise on the full spectrum of emerging technologies (AI, blockchain/DLT, fintech, data analytics, quantum etc.) and on the critical interplay between the different laws and regulations affecting specific sectors and technologies, data, privacy, IP, and competition.

London
T +44 (0)20 7600 1200
F +44 (0)20 7090 5000

Brussels
T +32 (0)2 737 94 00
F +32 (0)2 737 94 01

Hong Kong
T +852 2521 0551
F +852 2845 2125

Beijing
T +86 10 5965 0600
F +86 10 5965 0650