

The EU AI Act's enforcement provisions — Part 3

In this third instalment in a series of articles on the EU's Artificial Intelligence Act, Tim Hickman, Partner, and Aishwarya Jha, Associate, at White & Case LLP, discuss the timing and nature of enforcement of the upcoming AI legislation in the EU

The EU's Artificial Intelligence Act (the 'AI Act') was approved by European lawmakers in March 2024 and is due to be published imminently in the Official Journal of the EU. In Part 1 in this series (published in Volume 17, Issue 2, pages 4-5), we examined the AI Act's definition of 'AI systems', and noted that the uncertainties arising from that definition are likely to pose a major challenge for organisations seeking to understand whether their data processing activities fall within the scope of the AI Act or not. In Part 2 (published in Volume 17, Issue 3, pages 3-5), we explored the material and territorial scope of the AI Act, and observed its extensive and aggressive extraterritoriality provisions. In this article, we consider the timing and nature of enforcement of the AI Act.

Timing of enforcement

Organisations that are using AI systems or general purpose AI ('GPAI') models to process personal data will potentially face enforcement under the AI Act, but the timeline for the start of enforcement is complex, and depends on the nature of the AI systems or GPAI models in question. In order to plan their compliance programmes, organisations need to carefully consider their use of AI in the context of that timeline, to understand the deadlines by which they need to achieve compliance.

The AI Act will enter into force 20 days after its publication in the Official Journal. Enforcement of Chapters I and II (general provisions, definitions, and rules regarding prohibited uses of AI) starts six months after the AI Act comes into force (i.e., any use of AI that is prohibited under the AI Act needs to cease within six months of the AI Act entering into force, or face enforcement).

Enforcement of certain requirements (including notification obligations, governance, rules on GPAI models, confidentiality, and penalties (other than penalties for providers of GPAI models)) starts 12 months after the AI Act comes into force. However, providers of GPAI models placed on the EU market before this date get a further two years from the start of

enforcement to achieve compliance.

Enforcement of Article 6(1) (and the corresponding obligations regarding high-risk AI systems) starts after three years. However, the AI Act does not generally apply to operators of high-risk AI systems that are put on the EU market or into service before the date two years after the AI Act comes into force (provided that there are no "significant changes in [the] designs [of those AI systems]" after that two-year transitional window).

The Recitals to the AI Act encourage providers of high-risk AI systems to begin their compliance efforts on a voluntary basis during this transitional period, but it appears that there is no penalty for failing to do so.

At the time of writing, all of the time periods described above remain in square brackets in the most recent text of the AI Act, so it remains possible that they could change before the AI Act is published in the Official Journal.

Nature of enforcement

Part 3 (Enforcement) of the AI Act provides for a two-tiered regulatory framework, with enforcement at both the Member State level and EU-wide level. The AI Office was established by the European Commission in January 2024. It is expected to enforce the AI Act's rules regarding the provision of GPAI models and will coordinate enforcement actions across the EU Member States in respect of high-risk and/or prohibited AI systems. Substantive enforcement will be carried out by the national competent authorities of Member States. The AI Board will hold an advisory role, and will issue guidance on the application and enforcement of the AI Act.

Penalties

Infringements of the AI Act's rules on prohibited uses of AI are subject to penalties of up to the greater of €35 million or 7% of an undertaking's total worldwide annual turnover (i.e., the maximum penalties under the AI Act are 1.75 times greater than the

maximum penalties under the GDPR).

Infringements of most other provisions (such as those applicable to the operators of high-risk AI systems or providers of GPAI models) may incur administrative fines of up to the greater of €15 million or 3% of an undertaking's total worldwide annual turnover.

Providing incorrect, incomplete or misleading information to national competent authorities may incur additional administrative fines of up to the greater of €7.5 million or 1% of an undertaking's total worldwide annual turnover.

Much like the enforcement regime under the GDPR, administrative fines under the AI Act will typically be issued by the relevant Member State's competent national authorities and/or courts, in accordance with applicable national laws. However, unlike the position under the GDPR, and in addition to the powers of national competent authorities to issue administrative fines as noted above, the Commission is empowered by the AI Act to impose financial penalties of up to the greater of €15 million or 3% of an undertaking's total worldwide annual turnover for non-compliance concerning the provision of GPAI models. It will be interesting to see how the Commission exercises these enforcement powers, and whether the Commission's approach impacts Member States' own enforcement priorities and strategies.

While the EU legislators have acknowledged the need for harmonising the rules on administrative penalties under the AI Act, the text leaves room for inconsistency in regulatory enforcement across the EU (potentially similar to the inconsistencies that currently impact the enforcement of the GDPR from one Member State to the next). In particular, the methodology for calculating fines under Article 99(7) of the AI Act for specific infringements is somewhat abstract, leaving to the discretion of individual national competent authorities to give meaning to what is "effective, proportionate and dissuasive". While it is hoped that the guidance of the AI Board will lead to some degree of consensus on the issue of enforcement, it remains to be seen how this will play out in practice.

The AI Act makes clear that it does not seek to expropriate or reduce the powers of Supervisory Authorities under the GDPR, which remains an entirely separate regime. For organisations that are subject to both the GDPR and the AI Act, it appears that a single incident (e.g., a data breach due to non-compliant use of an AI system) could potentially trigger investigations, enforcement, and penalties, under both the GDPR and the AI Act.

Extraterritorial enforcement

In Part 2 in this series, we noted that a provider or deployer of AI systems that is based outside the EU (for example, in the UK) will nevertheless be subject to the AI Act if the output of its AI systems — such as recommendations or content — is used in the EU (seemingly regardless of whether this was intended or not). This potentially exposes organisations that are outside the EU (and that may not be trying to do business in the EU at all) to the risk of enforcement under the AI Act.

By way of comparison, while the GDPR also has extraterritorial application, the appetite for out-of-jurisdiction enforcement under the GDPR has been extremely limited, and wherever possible, Supervisory Authorities under the GDPR have tended to take enforcement action against entities that are established in the EU, or have assets in the EU. It remains unclear how much appetite there will be, among the Member State regulators and the Commission, for out-of-jurisdiction enforcement of the AI Act.

Tim Hickman and Aishwarya Jha

White & Case LLP

tim.hickman@whitecase.com

aishwarya.jha@whitecase.com
