TA Tomorrow's Affairs
Analysis of today
Assessment of tomorrow

By: Tomorrow's Affairs Staff

Brussels delays AI law six days before the deadline

From 2 August, every chatbot on the European Union market must inform users when they are interacting with an artificial intelligence system, unless this is already obvious.

Companies that develop AI tools for creating text, images, audio and video must label the content produced by those tools so that it can later be identified as having been created by artificial intelligence.

People exposed to emotion-recognition and biometric-categorisation systems must be informed that such technology is being used. Deepfake content must be flagged, as must text on matters of public interest when it is published without human verification and editorial responsibility.

Violations of these rules are subject to fines of up to 15 million euros or three per cent of the company's global annual turnover. Such penalties give the impression that the European law on artificial intelligence has finally come into full force. Its most important part, however, has been postponed.

Systems that can determine who gets a job, credit, a school placement or welfare benefits, as well as those used in policing and managing critical infrastructure, will not be fully monitored from 2 August 2026 as originally planned.

Just six days before that deadline, the Digital Omnibus came into force, introducing a package of changes that shifted implementation of the strictest obligations for high-risk AI systems to December 2027 and August 2028.

The European Union has therefore begun to apply the simpler part of the law: the obligation to label AI-generated content and warn users that they are interacting with a machine. Oversight of systems that directly affect important decisions in people's lives has been postponed for at least another sixteen months.

What really applies from today

Article 50 does not require all content created with the help of artificial intelligence to carry a visible label. The obligation depends on the type of content, how it was created and the responsibility of the person who publishes it.

Companies developing AI tools to create text, images, audio, and video must ensure that the origin of such content is technically identifiable. This means it should leave a digital trace showing that it was produced or significantly modified by artificial intelligence.

Ordinary language corrections, improvements to image quality, and similar technical interventions are not covered unless they change the essence of the content.

Stricter rules apply to deepfake material. It must be clearly labelled as altered or artificially produced. In satire, works of art and fictional stories, such as films and TV shows, the label can be unobtrusive, but it must remain clear to the audience that the depiction is not real.

> Oversight will mostly be carried out by the national authorities of the member states

A special regime applies to AI-generated texts on matters of public interest. The label is not required when the text has been checked by a human, has passed editorial control, and someone takes responsibility for its publication. The obligation is aimed at content that is produced and published by a machine without genuine human verification.

For systems already on the market before 2 August, an additional deadline of 2 December was introduced for the technical labelling of generated content. Other obligations, including the duty for the user to know when they are interacting with a machine, apply immediately.

Oversight will mostly be carried out by the national authorities of the member states. This means that the same law will enter twenty-seven administrative systems with different

budgets, levels of experience, and technical capacities.

In some countries, oversight will be led by established regulators with expert teams. In others, the same task will fall to authorities that still have to hire people capable of understanding how complex AI systems work.

Six days before the deadline

The Digital Omnibus was published on 24 July and entered into force three days later, just six days before the implementation of the most important part of the Artificial Intelligence Act was due to begin.

The European Parliament had previously approved it on 16 June, the EU Council on 29 June, and the act was signed on 8 July. The final stage of the procedure was accelerated in order to move the deadline forward before it formally took place.

The delay was inevitable because the European Union had not completed the preparations needed to implement the law. Companies did not yet have clear technical rules to demonstrate that their systems were secure and compliant.

The European Commission's directives, the designation of competent authorities in the member states, and the establishment of bodies responsible for checking whether companies comply with the law had also been delayed.

> The postponement of the deadline has a practical justification but political responsibility remains with the EU institutions

Without those rules, companies would not know exactly what regulators expect of them. They might invest a great deal of money in data verification, risk assessment, record-keeping and human oversight, only to be told later by the relevant authority that it had not been done in an acceptable way.

This is precisely why technical standards are crucial for implementing the law. They should clearly define how the company verifies the reliability of the system, how it records its decisions, how it measures errors, and how it demonstrates that a human can intervene when the system goes wrong. At the end of July, many of those rules had still not been finalised.

The postponement of the deadline therefore has a practical justification. However, political responsibility remains with the institutions of the European Union.

They adopted the implementation schedule in 2024 and presented it as proof that Europe can bring order to the field of artificial intelligence. Two years later, they had to admit that they had imposed the strictest obligations before they had prepared the rules, supervisory authorities and experts needed to implement them.

Companies get time, citizens will wait longer for protection

Delaying the strictest rules creates a large gap between the current use of artificial intelligence and the full responsibility of the companies that introduce it.

A bank, employer, school or public service may still use automated assessments, but will not yet have to meet all the obligations relating to data quality, system reliability checks, record-keeping and the genuine possibility of human intervention.

Citizens are not completely without protection. Regulations on data protection, non-discrimination, labour relations, consumer rights, and financial services still apply.

The AI law was intended to strengthen protections, requiring companies to prove a system is sufficiently reliable

The problem is that these regulations are usually triggered only after the damage has already occurred. The candidate can dispute the discriminatory decision, the client can request an explanation for a rejected loan, and the employee can initiate proceedings for unlawful oversight.

The AI law was intended to strengthen protections, requiring companies to prove a system is sufficiently reliable before it can start making decisions about humans. That part has now been postponed until the end of 2027 or 2028.

It is easier to label a chatbot than to control an algorithm

The Digital Omnibus also introduced two new bans. From 2 December 2026, AI systems designed to create fake intimate images without the consent of the person depicted, as well as child sexual abuse material, will be prohibited.

Fines of up to 35 million euros, or seven per cent of a company's global annual turnover, are envisaged for violations of these rules.

Prescribing a ban, however, is easier than enforcing it. With a large platform operating in the European Union, the regulator can request data, order the removal of the system, and impose a fine. It is much more difficult to act against an anonymous service registered outside the EU, especially when the application is distributed across several websites or rapidly changes its address and owner.

Small providers and services operating outside the reach of European institutions will remain significantly more difficult to control

That is why the first actions are likely to target large technology companies and platforms with a clear business presence in Europe. They are visible, have assets and can be compelled to comply with the regulator’s decision. Small providers and services operating outside the reach of European institutions will remain significantly more difficult to control.

With strict penalties, Brussels can quickly demonstrate determination in a few publicly recognisable cases. However, the real success of these bans will depend on whether European authorities can identify those responsible, provide evidence, and enforce decisions even when the provider has no office, account, or property in the European Union.

December 2027 will determine the value of the law

The first months of the application of Article 50 will show how easy it is to adopt a rule and how difficult it is to standardise its implementation.

Checking that the user is warned they are talking to a chatbot is straightforward. It is much more difficult to track AI-generated content that is downloaded, processed and published on multiple platforms, especially when its original digital trail has been removed or lost.

During 2027, the Commission will seek to finalise the technical standards and prepare regulators for the part of the law that is currently delayed

During 2027, the Commission will seek to finalise the technical standards and prepare regulators for the part of the law that is currently delayed. A further postponement of the deadline would be a political defeat, so it is more likely that 2 December 2027 will be formally retained.

Actual implementation will be slower. The initial proceedings will focus on large companies and on cases where violations can be easily proven, while complex systems in health, finance, employment and public administration will, for a long time, depend on the varying capacities of national regulators.

Therefore, the value of this law will not be determined by the date it enters into force, the amount of fines or the number of new guidelines. It will be determined by the first cases in which the regulator forces a large company to change a system, compensate for damages or withdraw it from the market.

If similar cases arise in 2027 and 2028, the current delay can be justified as the price of building serious oversight. If they do not, the European Union will end up with a law that can label content created by artificial intelligence, but cannot control the decisions that the same technology makes about people.