

DPE position on the Digital Omnibus on AI

Delivery Platforms Europe (DPE) represents the leading local commerce platforms in Europe, providing digital services connecting consumers with local merchants through couriers.

DPE urges the EU institutions to conclude negotiations and adopt the Digital Omnibus on AI as swiftly as possible, before the August 2026 entry into force of high-risk obligations, to enable businesses to plan and implement compliance with the AI Act in a timely manner.

Indeed, while the Digital Omnibus on AI introduces some targeted clarifications, it falls short of resolving fundamental structural issues. Significant uncertainty persists regarding the timeline for the application of high-risk AI obligations, the overly broad scope of high-risk classifications, and the lack of practical implementation guidance. As a result, many of the core ambiguities faced by companies deploying AI systems remain unresolved.

I. Lack of clarity around AI Act timelines and obligations

Support AI uptake by clarifying compliance timelines

Local delivery platforms benefit significantly from the deployment of AI tools, which in turn accelerate the adoption of digital solutions across the local economy.

Clear and predictable compliance timelines are essential to support further AI uptake. DPE welcomes the recognition of the need to better define these timelines in light of the current state of preparedness of guidelines and standards. However, the proposal's continued linkage of compliance deadlines to the availability of standards and guidance risks perpetuating legal uncertainty for businesses, undermining their ability to plan investments and deploy AI solutions with confidence.

Recommendation n°1

DPE recommends maintaining a compliance timeline linked to the publication of the relevant guidelines, with obligations applying 12 months after their adoption. However, as a fallback option to ensure legal certainty, we would support introducing a clear and unambiguous deadline for compliance with the high-risk obligations under Annex III, set at 2 December 2027.

Clarification of roles and obligations within the supply chain

The AI Act framework does not provide sufficient clarity around the roles and who qualifies as a “provider”, “deployer”, “importer”, or “distributor” within the complex AI supply chains. When companies integrate third-party, open-source or embedded models, it becomes difficult to determine who bears which compliance obligations, what documentation is required, and where liability sits, slowing down responsible adoption.

Similar concerns arise in relation to the concept of **“substantial modification” of high-risk AI systems** and the legal consequences that flow from it. While DPE welcomes the proposal’s efforts to better define what constitutes a substantial modification, the framework remains insufficiently clear regarding the resulting obligations and liability shifts across the AI value chain. In particular, greater legal certainty is needed on how substantial modifications affect the roles and responsibilities of providers, deployers and other actors, and on when such changes may trigger a requalification of entities or renewed compliance requirements.

Clarifying these impacts is essential to ensure predictable accountability, avoid unintended disruptions in contractual relationships, and support the safe and effective deployment of AI systems across complex supply chains.

Recommendation n°2

Provide detailed guidance on the definitions of roles and responsibilities among providers, deployers, importers, and distributors including where AI systems are integrated, fine-tuned, or combined with third-party or open-source components.

II. Simplifying compliance to high-risk obligations

Streamlining compliance processes

In its current form, the AI Act **risks classifying low-impact AI systems as high-risk on the basis of formal criteria rather than their actual risk or real-world impact**. For example, Annex III states that “AI systems intended to be used for the recruitment or selection of natural persons, in particular to place targeted job advertisements, to analyse and filter job applications, and to evaluate candidates” qualify as high-risk. However, it does not distinguish between AI systems that materially influence hiring decisions and tools that merely support ancillary HR tasks, meaning a tool used to draft job descriptions could be treated in the same way as an automated candidate-screening system. The Digital Omnibus on AI does little to address this issue. For DPE, Commission guidance is essential to ensure legal uncertainty and proper compliance.

As a result, companies may be required to comply with obligations that are often impractical to operationalise, applying a one-size-fits-all approach that imposes disproportionate burdens on low-impact systems without delivering commensurate benefits for individuals.

At the same time, DPE strongly supports maintaining the registration exemption for non-high-risk AI systems. This exemption plays a critical role in preventing unnecessary and disproportionate administrative burdens that offer limited regulatory value and risk diverting resources away from genuinely high-risk use cases. In addition, the Digital Omnibus on AI should clearly and explicitly confirm that, when national competent authorities request documentation related to an AI system’s risk assessment, they must fully respect the confidentiality of the information and data obtained in accordance with Article 78 of the AI Act. Such a clarification is essential to ensure legal certainty, enable effective cooperation with authorities, and safeguard sensitive business information.

Recommendation n°3

The classification of high-risk AI systems should be based on real-world risk and impact, taking into account contextual factors such as use, safeguards, scale, and system maturity. Classification should be supported by clear, practical Commission guidance and proportionate obligations limited to genuinely high-risk use cases.

Strengthening coordination between Market Surveillance Authorities

In the absence of clear coordination mechanisms, there is a tangible risk of divergent interpretations, parallel investigations, or conflicting corrective measures across Member States. This is particularly the case for cross-border AI systems operating through complex value chains. Such fragmentation would undermine legal certainty for operators, create duplicative compliance burdens, and ultimately weaken trust in the regulatory framework.

Therefore, DPE supports the inclusion of a structured framework for mutual recognition and mutual assistance between Market Surveillance Authorities (MSAs), supported by a clear lead-authority model for cross-border cases and a strengthened coordinating role for the AI Office.

Recommendation n°4

We recommend establishing an EU-wide mutual recognition and mutual assistance framework among MSAs to ensure harmonised enforcement, avoid conflicting decisions, and provide consistent guidance across Member States.