July 2025

Implementing the EU digital rulebook: Recommendations for simplification

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

DPE recognises the critical need for an effective roll-out of the European digital legislation, and we therefore welcome the efforts to address misalignments between key digital regulations to guarantee their successful implementation and enforcement, notably as part of the upcoming Digital Omnibus (expected in November 2025). Within this context, ensuring legal clarity and harmonisation of digital legislation is paramount to attain compliance and enforcement.

This misalignment creates real-world impacts on entities subject to digital legislation, in particular on local delivery platforms which sit at the crossroads of various pieces of legislation. The consequences of this misalignment for DPE members ranges from legal uncertainty, disproportionate reporting requirements, and contradictory enforcement. In particular, the local delivery platform sector is subject to issues primarily arising from inconsistencies between three pieces of legislation:

- The **General Data Protection Regulation** (GPDR, 2016), which establishes a comprehensive framework for the collection and processing of personal data of individuals;
- The **AI Act** (2024), which introduces a risk-based approach to regulating the development and use of AI systems and models;
- The **Platform Work Directive** (PWD, 2024), which imposes specific obligations on algorithmic management and the processing of personal data in platform work contexts.

These issues become particularly evident around **three issues**:

1. Inconsistent definitions of 'automated decision/monitoring systems' across three pieces of legislation
2. Misalignment of reporting obligations
3. Fragmentation and dispersion of enforcement powers

Therefore, DPE takes the opportunity to shed light on these issues and propose viable solutions to ensure the existing legal framework is implemented effectively and preserves the protections it guarantees.

1. Inconsistent definitions of automated systems

The misalignment between GDPR, AI Act and PWD on the definition of what entails ”automated decision/monitoring” systems jeopardises the coherent implementation of these pieces of legislation. This leads to a twofold problem: on one side, subjects struggle with duly implementing requirements related to these systems, while on the other side, inconsistent definitions may result in inconsistent enforcement by national authorities.

The **misalignment of the definition of automated systems** across the GDPR, the AI Act, and the PWD raises questions about legal certainty and the coherent application of Union law:

- The **GDPR** (Art. 22) refers to *"automated individual decision-making"* in the context of automated data processing, including profiling, which produces decisions having “legal or similarly significant effects” on a data subject;
- The **AI Act** (Art. 3) defines an *"AI system"* more broadly as a machine-based system that, for a given set of human-defined objectives, generates outputs such as predictions, recommendations, or decisions influencing real or virtual environments. Therefore, an AI system could potentially encompass a wide range of algorithms, automated decision-making and rule-based systems which may or may not be captured by the GDPR and the PWD;
- The **PWD** (Art. 2 and 9) defines *“automated monitoring systems and automated decision-making systems*” in the context of platform work even more broadly, as *“systems which are used to take or support, through electronic means, decisions that significantly affect persons”*.

This fragmented and overlapping landscape generates significant legal uncertainty, duplicative compliance burdens, conflicting obligations, and adds significant complexity. Addressing these issues would help futureproof the overall digital rulebook, as emerging new technologies will require future legislative action built on these foundations.

Clarifying definitions now is critical in order to pave the way towards a legally sound and successful EU digital rulebook.

Our recommendation

Better alignment of these definitions to ensure Article 22 of the GDPR remains the reference for all digital regulations and guarantee regulatory consistency. This would provide for a general and flexible definition capable of ensuring the future-proofness of the overall digital *acquis*.

2. Misalignment of reporting obligations

The GDPR, the AI Act, and the PWD require digital delivery platforms to conduct assessments related to the types of automated systems they use. In particular, attention should be drawn to the multiple procedures provided by the three pieces of legislation for the reporting on data processing. More specifically:

- The **GDPR** (Art. 35) provides that where a type of processing of personal data (considering the nature, scope, context, and purposes of the processing) is likely to result in a high risk to the rights and freedoms of natural persons, the controller must, prior to the processing, carry out a Data Protection Impact Assessment (DPIA);
- The **AI Act**, while not mandating a general obligation to carry out a DPIA for deployers, foresees the obligation (Art. 26), in cases of high-risk AI systems that process personal data, to carry out a DPIA and to draw up detailed technical documentation for high-risk AI systems;
- The **PWD** (Art. 8) mandates digital labor platforms to conduct DPIAs and seems to go beyond that, by mandating the proactive disclosure of full DPIAs to platform workers and their representatives.

These issues regarding reporting obligations translate into difficulties for entities in terms of implementation, as they create legal uncertainty around the processes and scope of the reporting. In turn, the full disclosure of DPIAs mandated by the PWD creates concrete risks to trade secrecy, when the obligation under GDPR would suffice to meet the safeguards requested by both texts. This misalignment not only undermines competitive advantage but also discourages innovation by creating concrete legal and commercial risks.

At the same time, numerous and inconsistent obligations create an uncertain and burdensome environment for businesses, and especially SMEs, who want to invest in AI and digital solutions. In order to foster the roll out of digital solutions and uptake by businesses and consumers alike, Europe needs a clear and solid legal framework.

Our recommendation

The reporting requirements should be better aligned and rely on the baseline procedure provided by the GDPR, as it is the most suitable legal basis for mandating such Data Protection Impact Assessments (DPIA). As the GDPR already implements guardrails in the way digital platforms deal with AI systems, it should remain the reference across all digital regulations.

3. Fragmentation of enforcement powers

Lastly, considering the issues mentioned in the aforementioned points, it is worth noting the fragmentation in the enforcement of the GDPR, the AI Act and the PWD (Chapter 3). In case of misalignment of definitions and reporting obligation, consistent enforcement and interpretation can be powerful tools to ensure compliance. However, the fragmentation of competent authorities responsible for different pieces of legislation and the lack of a coherent cooperation framework amongst them creates an extra layer of misalignment and complexity for businesses. In this respect:

- The **GDPR** is enforced by data protection authorities;
- The **AI Act** compliance will be overseen by data protection authorities national AI offices;
- The **PWD** will be mostly monitored by national labor authorities.

Better coordination and cooperation among these authorities would not only improve the implementation of current rules, but also create a strong enforcement framework able to guide the Commission and Member States in the development of future initiatives, ensuring legal certainty and consistency.

Our recommendation

A collaboration framework based on guidelines from the Commission between all relevant authorities overseeing the enforcement of digital rules is required to ensure EU regulations are successfully implemented and effective.