WE ARE SHAPING THE INTERNET.
YESTERDAY.TODAY.BEYOND TOMORROW.

eco

**POSITION PAPER**

# On the Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulations (EU) 2024/1689 and (EU) 2018/1139 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI)

Berlin, 2 March 2026

## I. Summary

The Digital Omnibus on artificial intelligence (AI) represents an important opportunity to recalibrate the implementation of the AI Act in a way that strengthens innovation, legal certainty, and Europe's international competitiveness while preserving high standards of protection. From the perspective of the German digital and internet industry, the proposed extensions of compliance deadlines are a positive step, yet they remain insufficient in scope and duration. Transitional periods must apply consistently to high-risk AI systems and General Purpose AI Models in order to avoid legal fragmentation, investment uncertainty, and market distortions. At the same time, supervisory structures must be strengthened in a way that ensures coherent enforcement across the Single Market, with a clear allocation of responsibilities between EU-level and national authorities and a strong coordinating role for the AI Office.

Beyond enforcement, regulatory policy must actively support innovation. A legally anchored innovation mandate for supervisory authorities, combined with effective regulatory sandboxes, can foster trust, accelerate responsible experimentation, and enable evidence-based regulation. The Digital Omnibus also takes important steps in reforming AI literacy obligations by shifting the focus from rigid company-level duties toward coordinated education and capacity-building measures.

Legal clarity on the use of personal data for AI training is essential for Europe's ability to develop competitive AI models. Confirming legitimate interest as a viable legal basis is therefore strategically important. At the same time, effective bias mitigation requires controlled access to sensitive data under strict safeguards. Further priorities include a risk-based and technologically realistic approach to text watermarking, the reduction of duplicative compliance obligations between the AI Act and the GDPR, the strengthening of regulatory sandboxes at Union level, and proportional relief for small mid-cap companies. Together, these measures can create a regulatory framework that is predictable, innovation-friendly, and globally competitive.

## II. Detailed Assessment

- **On Transitional Periods**

The proposed extensions of transitional periods within the Digital Omnibus represent an important step toward granting companies realistic implementation timelines for the complex requirements of the AI Act. However, these extensions currently remain insufficient. From the perspective of the internet industry, it is essential that the stop-the-clock mechanisms are not limited solely to high-risk AI systems but are explicitly extended to General Purpose AI Models. The current separation creates significant legal uncertainty, as many GPAI models can be deployed both independently and as components of high-risk applications. Divergent timelines for comparable regulatory obligations discourage investment, delay product development, and weaken the international competitiveness of European AI providers. A consistent and technology-neutral design of transitional periods across all relevant AI categories is therefore required.

eco broadly welcomes the approach set out in the Digital Omnibus to link the applicability of obligations for high-risk AI systems to the actual availability of harmonised standards, common specifications, and supporting guidance. This mechanism acknowledges that key prerequisites for legally secure implementation of the AI Act are not yet fully in place. Nevertheless, from the perspective of the internet industry, the proposal does not go far enough. Transitional periods of six or twelve months are insufficient given the complexity of the technical, organisational, and legal adjustments required for high-risk AI systems. In particular, data- and model-driven systems with iterative development cycles require significantly longer lead times for the establishment of governance structures, documentation processes, risk management frameworks, and conformity assessments. eco therefore considers transitional periods of up to 24 months as necessary to ensure high-quality, legally compliant, and innovation-friendly implementation. These extended timelines must also apply to AI models, as substantial adjustments are likewise required at model level in terms of transparency, traceability, risk assessment, and technical safeguards.

- **Governance and Consistent Enforcement of the AI Act within the Single Market**

Coherent and predictable enforcement of the AI Act within the Single Market is a key prerequisite for companies to scale AI solutions, operate across borders, and make long-term investment decisions. From the perspective of the internet industry, any measure that contributes to stronger harmonisation of supervisory practices and reduces regulatory fragmentation among Member States should be welcomed. The envisaged strengthening of the AI Office as a central enforcement authority for AI systems provided by model developers as well as for very large online platforms and search engines under the Digital Services Act can make an important contribution in this regard.

At the same time, it is crucial that the allocation of responsibilities between European and national levels is clear, legally secure, and free of contradictions. Companies must be able to rely on comparable AI systems being assessed and supervised according to uniform standards throughout the Union and on divergent interpretations by individual authorities not creating de facto market barriers or competitive distortions. Centralised EU-level enforcement must therefore not result in parallel or competing competences but must be closely integrated with national supervisory structures. The mandate of the AI Office should also explicitly include the enforcement of transparency and information obligations for low-risk AI systems under Article 50. This is appropriate given the AI Office's central role in developing the relevant Code of Practice and its corresponding expertise in ensuring consistent application.

The obligation introduced by the Digital Omnibus for national market surveillance authorities and public bodies to cooperate more closely and provide mutual assistance is an important step toward more consistent enforcement across the European Union. In addition, the European coordination framework should enable rapid alignment in response to new technological developments, innovative business models, and cross-border cases, requiring clear communication channels, binding timelines, and transparent decision-making procedures.

eco also welcomes the clarification that AI systems used in high-risk areas, but for which providers have determined that they do not qualify as high-risk because they are limited to narrow or purely procedural tasks, will be exempted from registration requirements. This clarification would reduce administrative burden for providers while also limiting potential security risks associated with the disclosure of sensitive system information.

- **Strengthening Innovation-Friendly Supervision within the AI Act Framework**

The AI Act aims to minimise risks and protect fundamental rights. This objective is both legitimate and necessary. However, it must not lead to regulatory authorities acting solely as risk managers. A legally anchored innovation mandate for supervisory authorities at both EU and national level is therefore essential. Such a mandate should clarify that authorities are not only responsible for control and enforcement but also for actively supporting innovation, for example through regulatory sandboxes, authoritative interpretative guidance, and dialogue-oriented supervision. An innovation mandate of this kind would strengthen trust between regulators and industry and help ensure that Europe remains not only a safe but also an attractive location for AI development.

- **On AI Literacy**

Within the AI Omnibus, the Commission proposes amendments to Article 4 of the AI Act, which addresses the necessary AI competencies of workers. eco explicitly supports the approach of replacing the previously envisaged blanket obligation for providers and users of AI systems to ensure AI literacy with a more coordinating

role for the European Commission and the Member States. Promoting AI skills is a key prerequisite for the responsible use of artificial intelligence across business, public administration, and society. At the same time, experience within the internet industry shows that undifferentiated company-level obligations fail to reflect the diversity of use cases, company sizes, and maturity levels of AI deployment and disproportionately burden smaller enterprises.

From the perspective of eco, AI literacy should be understood as a strategic cross-cutting task that is best advanced through coordinated education, training, and information initiatives rather than through rigid regulatory obligations imposed on individual companies. The association therefore welcomes the Digital Omnibus's focus on incentives, voluntary measures, the exchange of best practices, and the provision of centralised information and support services. It is essential that these measures are designed in a practical manner and aligned with the real needs of companies, particularly SMEs and small mid-cap companies. The promotion of AI literacy should be closely linked to existing initiatives, innovation ecosystems, and training structures. The current situation still generates uncertainty for companies and therefore remains counterproductive for the effective implementation of AI systems.

- **On the use of personal Data for AI training**

Explicit confirmation of legitimate interest as a viable legal basis for the training of AI models under the proposed Article 88c is of strategic importance for Europe's innovation capacity and competitiveness. Without a practical, scalable, and uniformly interpreted legal basis for data-driven learning, European companies will be unable to develop and operate competitive AI models in a highly dynamic global environment.

In current practice, substantial legal uncertainty persists as to whether and to what extent personal data may be processed for training purposes on the basis of legitimate interest. This uncertainty leads to restrained investment, fragmented national interpretations, and structural competitive disadvantages compared with third countries where legal clarity is greater or regulatory flexibility broader.

An approach based exclusively or predominantly on consent is neither realistic nor proportionate for modern AI training. Training datasets typically involve very large volumes of data, historical datasets, or publicly available content for which individual consent cannot be practically obtained. There is also a risk of systematic bias if only data covered by explicit consent may be used, which can negatively affect the quality, fairness, and representativeness of AI models.

Legitimate interest offers a well-established risk-based balancing mechanism that appropriately reconciles innovation needs with the fundamental rights of affected individuals. This requires clear legal confirmation that AI training can generally constitute a legitimate economic and societal interest, provided that appropriate safeguards such as data minimisation, purpose limitation, technical and organisational security measures, and transparency are implemented. eco

therefore explicitly welcomes the clarification introduced by the Digital Omnibus, which significantly strengthens legal certainty.

- **Ensuring Effective Bias Mitigation**

Discrimination risks arise not only in systems formally classified as high-risk but also in widely deployed general or supportive applications whose scale can have significant societal impact. Effective detection, measurement, and mitigation of bias in AI systems requires that distortions can be empirically assessed. In practice, this is often not possible without the controlled use of sensitive data such as gender, age, ethnic background, or disability. Paradoxically, current regulatory constraints limit precisely those data that are necessary to ensure fairness and identify structural disadvantages.

From the perspective of the internet industry, the use of sensitive data for bias analysis and mitigation should therefore be permitted for all AI systems rather than being restricted to high-risk applications. At the same time, such use must be strictly limited to what is necessary and accompanied by strong safeguards, including pseudonymisation, access controls, short retention periods, and transparent documentation of purposes. Bias mitigation must not be hindered by legal uncertainty but should be recognised as a core element of future-oriented AI regulation. Europe has the opportunity to assume a leading role in trustworthy and fair AI.

- **On Text Watermarking**

The obligation under the AI Act to label AI-generated content through text watermarking raises substantial technical and practical challenges. At present, no mature, industry-wide solutions exist that are simultaneously reliable, tamper-resistant, interoperable, and scalable across the diverse use cases of generative AI. Premature regulatory requirements risk forcing companies into transitional solutions that quickly prove technically inadequate or economically inefficient, thereby generating additional costs and legal uncertainty.

From the perspective of the internet industry, binding text watermarking obligations should therefore be deferred until robust technological standards and proven solutions are available. Such a temporal decoupling would create planning certainty and prevent regulatory requirements from outpacing technological development. It must also be clarified that AI-generated code should be explicitly exempted, as marking or modifying source code can compromise software integrity, functionality, security, and maintainability, creating new risks for cybersecurity, product liability, and operational stability.

Furthermore, watermarking regulation should follow a risk-based approach and focus on demonstrable benefits for transparency, consumer protection, and abuse prevention. Not all AI-generated text carries the same risk of deception or manipulation, and blanket obligations may inhibit innovation without delivering proportional benefits. The objective should be a technology-neutral and internationally compatible framework that enables effective transparency while

avoiding functional limitations, security risks, or competitive disadvantages for European providers.

- **On the Interaction between the AI Act and the GDPR**

The parallel obligation to conduct a data protection impact assessment (DPIA) under the GDPR and a fundamental rights assessment (FRA) under the AI Act creates significant duplicative burdens for companies without generating proportional additional protection for individuals. Both instruments pursue similar objectives, rely on comparable risk assessments, and require largely overlapping organisational, technical, and documentation processes. This increases the risk that resources are consumed by formal duplication rather than by substantive improvements in safety, data protection, and fundamental rights protection.

Although Article 27(4) of the AI Act allows for coordination between DPIAs and FRAs, this provision is not binding and is likely to be applied inconsistently across Member States. This perpetuates legal uncertainty as to whether an existing DPIA will be recognised as sufficient or whether separate assessments will be required. From the perspective of the German digital and internet industry, it should therefore be clearly established that providers may determine whether a DPIA sufficiently fulfils the requirements of an FRA, provided that all relevant fundamental rights risks are appropriately assessed and addressed. Such clarification would significantly reduce administrative burden without lowering protection standards.

- **On Regulatory Sandboxes**

Regulatory sandboxes are a central instrument for combining innovation, legal clarity, and effective supervision. They enable companies to test new AI applications under realistic conditions while allowing authorities to gain early insight into technological developments, risk profiles, and practical implementation challenges. The Omnibus further specifies the sandbox framework through the proposed amendment to Article 57, introducing a new paragraph 3a. This enables the AI Office to establish a regulatory sandbox at Union level for AI systems covered by Article 75(1), which is fundamentally welcome from the perspective of eco. A centrally organised EU-level sandbox under the responsibility of the AI Office can significantly contribute to harmonising supervisory practice and preventing divergent national sandbox approaches with inconsistent requirements and evaluation criteria. Additional capacity for small and medium-sized enterprises is also explicitly welcomed. At the same time, it should be examined whether participation could be extended to AI models as well. This would be appropriate given that the AI Office is also responsible for overseeing AI models and would ensure that the benefits of sandboxes, including early regulatory clarity, constructive dialogue with authorities, and accelerated innovation cycles, are equally available to model developers.

- **On Exemptions for Small Mid-Cap Companies**

eco explicitly welcomes the extension of AI Act relief measures for small and medium-sized enterprises to small mid-cap companies, reflecting the particular innovation and growth profile of this group. Digital companies often operate in a transitional phase between SME status and large enterprise status and face significant regulatory adjustment costs. Simplifications relating to technical documentation, quality management systems, and sanction regimes therefore represent an important step toward avoiding disproportionate burdens and enabling scaling within the European Single Market. At the same time, the association notes that the need for numerous exemptions indicates the underlying complexity of the regulatory framework. In the long term, the objective should be to create a regulatory regime that is understandable, manageable, and proportionate for companies of all sizes without extensive reliance on exceptions. The current relief measures should therefore be regarded as an interim step toward a simpler, more coherent, and more innovation-friendly AI regulatory framework.

_____

**About eco:** With approximately 1,000 member companies, eco (international.eco.de) is the leading Association of the Internet Industry in Europe. Since 1995, eco has been highly instrumental in shaping the Internet, fostering new technologies, forming framework conditions, and representing the interests of its members in politics and international forums. eco has offices based in Cologne, Berlin and Brussels. In its work, eco primarily advocates for a high-performance, reliable and trustworthy ecosystem of digital infrastructures and services.