Nemko Digital

EU AI Act & Omnibus: Act Now or Wait? Webinar Report

Executive Summary

The webinar hosted by Nemko Digital addressed the growing uncertainty surrounding the European Union's Artificial Intelligence Act (EU AI Act) and the proposed Digital Omnibus package. With the regulatory landscape shifting, many organizations are questioning whether they should proactively comply with the original timelines or wait for further clarity. The session provided a comprehensive overview of the EU AI Act, explained the implications of the Digital Omnibus, and outlined four strategic options for businesses to navigate this complex environment. The overarching message emphasized that while regulatory timelines may shift, the business risks associated with AI remain constant, making a strategic approach to AI trust essential.

The EU AI Act: A Risk-Based Approach

The EU AI Act is the primary regulation governing artificial intelligence systems brought onto the EU market. It is characterized by its risk-based approach, categorizing AI systems into four distinct levels, each with specific obligations:

Nemko Digital

Risk Category	Description and Examples	Key Obligations
Prohibited AI	Systems posing unacceptable risks, such as social scoring or AI manipulating vulnerable groups.	Completely banned from the EU market.
High-Risk AI	Systems with significant potential to cause harm, such as AI used in medical diagnosis, CV screening, or critical infrastructure.	Extensive requirements including risk management systems, human oversight, technical documentation, and registration in the EU database.
Limited-Risk AI	Systems with specific transparency needs, such as customer service chatbots or deepfake marketing avatars.	Must adhere to transparency requirements, ensuring users know they are interacting with AI.
Minimal/Low-Risk AI	Systems with minimal impact, such as spam filters or grammar checkers.	No mandatory obligations, though adherence to codes of conduct is encouraged.

The regulation also distinguishes between different actors in the AI value chain, primarily Providers (creators or owners of the AI system) and Deployers (users or business users of the system). Understanding one's role and the risk category of the AI system is the crucial first step toward compliance. Nemko Digital outlined a three-step roadmap to compliance: risk categorization, gap analysis (identifying existing measures versus requirements), and evidence collection for validation.

Nemko Digital

The Digital Omnibus: Simplifying the Regulatory Burden

The Digital Omnibus is a legislative package designed to simplify and clarify existing digital, data, and cybersecurity laws in the EU, aiming to reduce the burden on businesses. The AI Act is a significant focus of this package due to the complexities and challenges associated with its implementation.

Currently in the trilogue negotiation phase (involving the European Parliament, the Council, and the Commission), the Digital Omnibus proposes several key changes to the AI Act:

1. Timeline Adjustments: The most significant proposed change is the delay of compliance deadlines. Originally, most high-risk AI obligations were set to take effect in August 2026. The Omnibus proposes splitting this into two dates: December 2027 for Annex III systems and August 2028 for Annex I systems.
2. Data Use and Registration: Discussions are ongoing regarding the limits on using sensitive data for AI bias checks and the rules for registering high-risk systems in the EU database. While some easing of registration rules was considered, the core requirement for full tracking remains.
3. AI Literacy and Deepfakes: The Omnibus debates whether AI literacy training for staff will be a mandatory responsibility for companies or merely an encouraged practice. Additionally, stricter bans on non-consensual and abusive AI content (explicit deepfakes) are proposed.
4. Enforcement Roles: There is ongoing debate over the division of responsibilities between the EU AI Office and national authorities, which could lead to potential fragmentation in guidance.

Nemko Digital

Strategic Options for Businesses

Given the uncertainty introduced by the Digital Omnibus, Bas Overtoom outlined four strategic responses for organizations:

1. Proactive Compliance: This approach involves continuing with compliance efforts as if the original deadlines remain unchanged. It is suited for companies that want to avoid risks early and ensure full alignment with the rules, preventing potential fines or issues down the line.
2. No-Regret Moves: This strategy focuses on taking partial, low-risk actions that are beneficial regardless of regulatory changes. It aims to reduce major risks efficiently without overcommitting resources prematurely.
3. Wait-and-See: Organizations adopting this approach choose to take minimal action until there is absolute clarity on the regulations and deadlines. This strategy avoids premature investment and offers short-term savings but may lead to a rushed compliance effort later.
4. Strategic Differentiation: This forward-looking approach views AI trust as a competitive advantage. Companies choosing this path go beyond mere compliance to drive trust and conversion, using their commitment to responsible AI to stand out in the market.

During a live poll, 40% of the audience indicated a preference for proactive compliance, 30% favored a wait-and-see approach, 22% opted for no-regret moves, and 10% chose strategic differentiation.

Nemko Digital

Focusing on No-Regret Moves

For organizations opting for the "No-Regret Moves" strategy, several key actions were recommended:

- AI Inventory: Identify and map all AI systems and their data dependencies across the organization.
- Risk Classification: Categorize each AI use case by risk level according to the EU AI Act framework.
- Accountability & Oversight: Assign clear ownership and responsibility for AI systems within the organization.
- Transparency & Awareness: Inform users and stakeholders about AI use and provide basic AI literacy training.
- Business Risk Lens: Assess AI not only for regulatory compliance but also for broader business risks (legal, reputational, operational, financial).
- Incident Management: Establish processes to monitor and respond to AI-related incidents.
- AI Procurement & Supply Chain: Implement governance over AI vendors and third-party dependencies.

A critical point emphasized during the webinar was the distinction between regulatory risk and business risk. An AI system might be classified as low-risk under the EU AI Act (e.g., supply chain optimization) but carry a high business risk if a failure could result in significant financial loss or operational disruption. Therefore, a holistic approach to AI governance is necessary.

Nemko Digital

Strategic Differentiation and the AI Trust Mark

For companies looking to leverage AI trust as a competitive advantage, Nemko Digital introduced the concept of the AI Trust Mark. This mark, aligned with the EU AI Act and built on the ISO/IEC 42001 framework, validates that an organization's AI management processes are effectively applied to specific products.

The AI Trust Mark offers several benefits, including enhanced brand reputation, premium pricing opportunities, risk mitigation, and international market access. A notable example shared was Samsung Electronics, which utilized the AI Trust Mark to signal its commitment to trustworthy AI, reinforcing its position as a global leader and building consumer and business trust.

Key Takeaways from the Q&A Session

The webinar concluded with an engaging Q&A session that clarified several important points:

- Applicability: The EU AI Act applies to any AI system sold or deployed on the EU market, regardless of where the company is headquartered.
- Providers vs. Deployers: A provider is the creator or owner who brands the AI system as their product, while a deployer is the business user of that system. The distinction is crucial for determining specific obligations.
- CE Marking and Conformity: High-risk AI systems require a conformity assessment to obtain a CE marking. In some cases, this assessment must be conducted by a third-party notified body. While the Nemko AI Trust Mark aligns with these requirements, it is distinct from an official notified body assessment, though Nemko is in the process of becoming a notified body.
- Determining High-Risk Status: A product is considered high-risk if it falls under Annex I (safety components of regulated products like toys or machinery) or Annex III (specific sensitive use cases like biometrics, employment, or critical

infrastructure) and poses a significant risk of harm to health, safety, or fundamental rights. The context of deployment is often the deciding factor.

Conclusion and Next Steps

The Nemko Digital webinar provided valuable clarity on the evolving landscape of the EU AI Act and the Digital Omnibus. While regulatory timelines may be subject to change, the imperative for organizations to understand and manage their AI risks remains urgent.

Attendees were encouraged to evaluate their current position and choose a strategic path that aligns with their risk appetite and business goals. Whether opting for proactive compliance, focusing on no-regret moves, or pursuing strategic differentiation, the first critical step is to conduct a thorough AI inventory and risk classification. Organizations seeking guidance on navigating these complexities were invited to consult with Nemko Digital's AI Act experts to develop a tailored compliance and trust strategy.

Nemko Digital