

NO BORDERS FOR COMPLIANCE: EU AI ACT OBLIGATIONS FOR NON-EU DIGITAL AGENCIES AND TECH COMPANIES

DOI: 10.5937/EMC26275D

Ivana Denčić

University of Novi Sad, Technical faculty "Mihajlo Pupin", Zrenjanin, Republic of Serbia

E-mail: ivana.savic@tfzr.rs

Sanja Stanisavljev

University of Novi Sad, Technical faculty "Mihajlo Pupin", Zrenjanin, Republic of Serbia

ABSTRACT

This paper addresses the critical problem of non-EU digital agencies and tech companies that service the EU market but remain largely unaware of or unprepared for their compliance obligations. The enforcement of the European Union Artificial Intelligence Act (EU AI Act) on August 2, 2026, introduces a comprehensive regulatory framework with significant extraterritorial reach. Grounded in both legal analysis and operational reality, the primary objective of authors is to map the extraterritorial scope of the AI Act onto this specific category of non-EU digital providers, classify their compliance readiness, and propose an external accountability framework as a systemic response. By drawing parallels with the General Data Protection Regulation (GDPR), this study highlights the structural gaps in awareness and resources among Small and Medium-sized Enterprises (SMEs). We introduce a diagnostic typology of readiness, identify two distinct scenarios of regulatory exposure, and demonstrate why an external accountability architecture is one of the best viable paths forward for these organizations.

Key words: EU AI Act, extraterritoriality, compliance readiness, digital agencies, external accountability

INTRODUCTION

The European Union Artificial Intelligence Act (Regulation (EU) 2024/1689) represents the world's first comprehensive horizontal regulatory framework for artificial intelligence, with its primary enforcement deadline set for August 2, 2026 (European Parliament and Council of the European Union, 2024). While the regulation aims to ensure that AI systems placed on the European market are safe and respect fundamental rights, its jurisdictional scope extends beyond the physical borders of the EU.

The global digital service sector: comprising marketing agencies, web development firms, design studios, and Software-as-a-Service (SaaS) startups, increasingly relies on AI technologies to optimize workflows and enhance deliverables. These non-EU digital providers frequently service EU-based clients, thereby falling directly within the scope of the AI Act. The core problem addressed in this paper is that a significant portion of these non-EU entities remains unaware of their regulatory exposure or lacks the necessary guidance to achieve compliance. The regulatory exposure is structural and immediate. It directly impacts how these organizations operate and survive in the market.

To understand what this means for non-EU digital providers, we need to map the exact reach of the AI Act, diagnose where these companies currently stand, and define the external accountability mechanisms they will need to survive the regulatory transition.

THEORY

We Have Seen This Before: The GDPR as Regulatory Mirror

The implementation of the General Data Protection Regulation (GDPR) serves as a vital precedent for understanding the challenges associated with extraterritorial EU legislation. Similar to the AI Act, the GDPR introduced stringent requirements that applied to any organization processing the data of EU residents, regardless of the organization's physical location. The pattern that emerged was consistent and predictable: initial unawareness, followed by panic compliance, and eventually the emergence of a specialized compliance service industry.

Prior studies on GDPR adoption demonstrate that small and medium-sized enterprises (SMEs) consistently struggle with resource constraints, expertise deficits, and the translation of qualitative regulatory requirements into technical controls (Sirur et al., 2018; Lopes & Oliveira, 2018; Politou et al., 2019; Potter et al., 2023). The key lesson is that non-EU companies frequently operate under the misconception that EU regulations do not apply to them. This vulnerability is currently being replicated with the AI Act. As Wernick and Meding (2025) demonstrate, this misconception extends even to AI researchers outside the EU who fail to realize that publishing models or datasets can trigger compliance obligations. This paper expands that argument to the specific vulnerabilities of non-EU digital agencies.

AI Governance and External Accountability

The regulatory shift marks the end of internal self-assessment as a sufficient proof of compliance. As AI systems integrate into high-risk domains, internal audits are no longer enough to prove safety or fairness. Falco et al. (2021) advocate for governing AI safety through independent audits, a concept further supported by the United Nations University (2024) on the governance of AI. Papagiannidis, Mikalef, and Conboy (2025) propose a comprehensive research framework for responsible AI governance, emphasizing the need for external oversight. Herrera-Poyatos et al. (2025) argue that responsible AI systems require a holistic approach integrating auditability, accountability, and governance across the AI lifecycle.

The missing piece in this literature is operational: who builds the accountability infrastructure for an SME that has no legal team, no compliance officer, and no budget for either? This paper addresses that gap directly.

METHODS

This paper employs a conceptual and analytical research design grounded in a systematic legal analysis of Regulation (EU) 2024/1689 and its technical annexes. We started from our core research question regarding when and how non-EU digital providers fall within the Act. From there, we identified and interpreted the relevant provisions. We verified our reading against official implementation guidance and legal commentary from practitioners.

From this analysis, we develop two scenarios that show how a non-EU agency becomes exposed to the Act depending on where AI sits in its work. We also develop a typology that classifies these providers into three groups by the structural nature of their compliance gap. Building on these findings, we then propose an external accountability model as a systemic response to that gap. The two scenarios and the typology are diagnostic instruments derived from the analysis. They have not yet been validated against empirical data.

FINDINGS

Operational Scenarios of Extraterritorial Exposure

Article 2 establishes output-based jurisdiction, applying the rules to providers placing AI systems on the market or putting them into service in the EU, regardless of their physical location (European Parliament and Council of the European Union, 2024). Article 3 distinguishes between a provider, the entity that develops an AI system or has it developed and places it on the market under its own name. Also a deployer, the entity using the AI system under its authority.

However, the most critical mechanism for non-EU digital agencies is not Article 3, but Article 25. Article 25 creates a transformation mechanism: any agency that rebrands, substantially modifies, or changes the intended purpose of a third-party AI system automatically assumes the full obligations of a provider. An agency that applies its own brand to a third-party AI system and delivers it to an EU client has, under Article 25, assumed full provider obligations. Where the system is high-risk, this includes the requirement to appoint an EU authorized representative under Article 22 (William Fry LLP, 2024; Holland & Knight, 2026). As Fabiano (2025) emphasizes, entities cannot escape provider obligations through outsourcing arrangements. Article 22 therefore functions as a latent obligation, one that is frequently triggered by standard industry practices like white-labeling.

The exposure of non-EU digital providers to the AI Act can be categorized into two primary scenarios with fundamentally different compliance implications. Scenario A covers AI embedded in delivered products: a non-EU agency develops a product, such as a custom SaaS platform or a mobile application—that incorporates an AI system and delivers it to an EU client. If the agency places the system on the market under its own name or substantially modifies an existing high-risk system, it assumes the full obligations of a provider under Article 16.

Scenario B covers AI used in the production process. The critical determinant under Article 2(1)(c) is not the transit of static output into the EU, but whether that output triggers specific obligations. Two channels are relevant: first, when AI-generated content falls under the transparency requirements of Article 50 (e.g., synthetic media delivered to EU audiences); second, when AI-assisted code or systems are integrated into Annex III high-risk categories by the EU client. Standard internal efficiency use does not automatically constitute provider status. The regulatory risk escalates when the agency's output directly shapes the risk profile of a system deployed within the EU. This exposure represents an immediate operational reality across the digital service sector, rather than a distant regulatory horizon.

Regulatory Obligations and Readiness Typology

Non-EU digital providers caught within the scope of the AI Act face a tiered set of obligations based on the risk classification of the AI systems they provide or deploy. Table 1 maps the key articles, their substantive requirements, and their practical implications for non-EU digital agencies.

The compliance infrastructure required by the AI Act remains largely unavailable to SMEs. Harmonized standards are incomplete, regulatory sandboxes are not yet operational in most member states, and national supervisory authorities have not been designated in the majority of EU countries.

From this starting point, we propose a diagnostic typology of compliance readiness categorized into three distinct groups. Table 2 maps the current state, the required state, and the gap between them. Tsakalakis et al. (2025) confirm that while the Act's SME support measures reduce procedural burden, they do not alter the substantive compliance obligations that apply to providers. Accountancy Europe (2025) similarly notes that SMEs must independently assess applicability and take required steps regardless of size.

Table 1: Key EU AI Act Articles and Their Implications for Non-EU Digital Providers

Article	Requirement	Practical Implication for Non-EU Digital Agency
Art. 4	AI Literacy	All staff using AI must demonstrate sufficient understanding of its capabilities and risks. No SME exemption.
Art. 5	Prohibited Practices	Absolute ban on manipulative AI, social scoring, and real-time biometric identification. In force since February 2025.
Art. 16	Provider Obligations (High-Risk)	QMS, technical documentation, human oversight, EU database registration, and conformity assessment required before market placement.
Art. 22	Authorized Representative	Triggered via Article 25 white-labeling. Requires a written-mandate EU authorized representative before market placement.
Art. 50	Transparency	AI systems interacting with humans or generating synthetic content must disclose their AI nature.
Art. 62	SME Support Measures	Priority sandbox access and simplified QMS templates. Does not eliminate substantive obligations (Accountancy Europe, 2025; Tsakalakis et al., 2025).
Art. 99	Penalties	Up to €35M/7% turnover for prohibited practices; €15M/3% for high-risk violations; €7.5M/1% for incorrect information.

Table 2: Compliance Readiness Typology — Current State vs. Required State for Non-EU Digital Providers

Category	Current State	Required State (AI Act)	Key Gap & Risk
Unaware	No knowledge that the AI Act applies extraterritorially. Operates under the assumption that non-EU status provides immunity.	Accurate self-classification as provider or deployer; basic AI literacy; awareness of prohibited practices (Art. 5).	Highest penalty exposure. Sudden market exclusion when EU clients demand compliance verification. No time to remediate.
Aware but lost	Aware of the AI Act's existence but unable to determine how it applies to their specific business model (e.g., confusion between Scenario A and B, or provider vs. deployer classification).	Correct role classification; mapped AI inventory; understanding of which articles apply to which systems.	Misclassification risk: acting as a provider but complying only as a deployer. Resources spent on wrong compliance track.
Aware but stuck	Understands obligations but lacks financial, technical, or legal resources to implement them (e.g., cannot establish a QMS, cannot afford an EU authorized representative).	Operational QMS; appointed EU authorized representative; registered high-risk systems in EU database; technical documentation maintained.	Good faith effort does not protect from enforcement. May be forced to exit the EU market due to prohibitive compliance costs without external support.

DISCUSSION

The compliance gap among non-EU digital providers runs deeper than information. Closing it requires more than awareness campaigns; it requires a redesign of how compliance infrastructure is delivered to entities that lack the scale to build it internally. The complexity of the AI Act, combined with the resource constraints typical of SMEs, creates a market entry barrier that is invisible until it becomes a market exclusion event.

The most significant blind spot is the Article 25 trigger mechanism. Agencies that consider themselves mere deployers can become providers without realizing it through the everyday practice of white-labeling. Once triggered, this activates the Article 22 requirement to appoint an authorized representative within the EU before placing a high-risk AI system on the market. This mandate is creating a nascent market for representation services, analogous to the GDPR DPO market post-2018. However, non-EU SMEs currently lack clear, affordable pathways to access it. While Article 62 introduces proportionality measures for SMEs, these provisions reduce procedural complexity without eliminating substantive obligations (European Parliament, 2025; Walters et al., 2024). An SME that cannot afford a QMS consultant is not protected by the existence of a simplified QMS template.

The institutional framework for this pressure is already in place: the EU Community of Practice on Public Procurement of AI published Model Contractual Clauses for AI (MCC-AI) in March 2025, providing standardized templates through which EU clients can transfer compliance obligations to their suppliers (European Commission Community of Practice on Public Procurement of AI, 2025). Once Article 26 deployer obligations take full effect in August 2026, vendor due diligence will shift from best practice to legal requirement. Failure to provide verifiable compliance documentation results in immediate procurement exclusion by EU enterprise clients. External accountability architecture is the only viable path for SMEs that need to stay in the EU market without building an internal legal department. This architecture operationalizes a Compliance-as-a-Service (CaaS) model based on three integrated elements: pooled technical documentation, fractional authorized representation under Article 22, and automated Annex III inventory mapping. By distributing fixed compliance costs across a portfolio of non-EU providers, the framework renders prohibitive regulatory requirements economically viable at scale.

CONCLUSIONS AND IMPLICATIONS

The EU AI Act establishes a regulatory perimeter that extends globally, capturing non-EU digital agencies and tech companies that service the European market regardless of their physical location. This paper has mapped the extraterritorial mechanisms of the Act, demonstrating that outsourcing does not eliminate provider obligations (Fabiano, 2025), and that Article 25 acts as a hidden trigger transforming deployers into providers through practices like white-labeling. Two primary scenarios of exposure a) AI embedded in delivered products and b) AI used in the production process, carry materially different compliance requirements, with Scenario B representing an underexplored regulatory blind spot.

The proposed typology of compliance readiness diagnoses three structurally distinct failure modes that cannot be resolved by the same intervention. Resource constraints and regulatory complexity drive the gap, and the response must match that reality.

Practical Implications: Non-EU digital agencies must take three concrete steps immediately. First, inventory all AI tools used in the production process and those delivered to clients. Second, verify whether any of these systems, or the agency's modification/rebranding of them, fall into Annex III high-risk categories. Third, if servicing EU clients and delivering AI-embedded products under their own name, consult on Article 22 obligations before August 2026.

The typology proposed here serves a diagnostic purpose. The next step is empirical validation. We need to know how many agencies are unaware, how many are lost, and how many are stuck. That data does not yet exist. Building it is the research agenda.

Limitations: The practical enforcement of the AI Act, particularly concerning Scenario B, remains to be tested in legal precedents and regulatory actions post-August 2026. The compliance window is open now, not at some future enforcement horizon.

REFERENCES

- Accountancy Europe. (2025). The EU AI Act: A guide for SME accountants. https://accountancyeurope.eu/wp-content/uploads/2025/02/250219_SME-AI-Act.pdf
- European Parliament. (2025). Interplay between the AI Act and the EU digital legislative framework (Study PE 778.575). Policy Department for Transformation, Innovation and Health. [https://www.europarl.europa.eu/RegData/etudes/STUD/2025/778575/ECTI_STU\(2025\)778575_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2025/778575/ECTI_STU(2025)778575_EN.pdf)
- European Parliament and Council of the European Union. (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union, L 2024/1689. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689>
- Fabiano, N. (2025). Subject roles in the EU AI Act: Mapping and regulatory implications. arXiv. <https://arxiv.org/html/2510.13591v1>
- Falco, G., et al. (2021). Governing AI safety through independent audits. *Nature Machine Intelligence*, 3, 566–568. <https://www.nature.com/articles/s42256-021-00370-7>
- Herrera-Poyatos, A., Del Ser, J., López de Prado, M., Wang, F.-Y., Herrera-Viedma, E., & Herrera, F. (2025). A framework for responsible AI systems: Building societal trust through domain definition, trustworthy AI design, auditability, accountability, and governance. arXiv. <https://arxiv.org/pdf/2503.04739>
- Holland & Knight. (2026, April 28). U.S. companies face EU AI Act's possible August 2026 compliance deadline. Holland & Knight Cybersecurity and Privacy Blog. <https://www.hklaw.com/en/insights/publications/2026/04/us-companies-face-eu-ai-acts-possible-august-2026-compliance-deadline>
- Lopes, I., & Oliveira, P. (2018). GDPR compliance in SMEs: There is much to be done. In *Proceedings of the International Conference on Information Systems and Technology Management*. https://www.researchgate.net/publication/328862700_GDPR_Compliance_in_SMEs_There_is_much_to_be_done
- Papagiannidis, E., Mikalef, P., & Conboy, K. (2025). Responsible AI governance: A review and research framework. *Journal of Strategic Information Systems*, 34(1), 101835. <https://www.sciencedirect.com/science/article/pii/S0963868724000672>
- Politou, E., Alepis, E., & Patsakis, C. (2019). A framework for GDPR compliance for SMEs. *European Journal for Security Research*, 4(2), 145–173. <https://link.springer.com/article/10.1007/s41125-019-00042-z>
- Potter, Y., Corren, E., Munilla Garrido, G., Hoofnagle, C., & Song, D. (2023). SoK: The gap between data rights ideals and reality. arXiv. <https://arxiv.org/abs/2312.01511>
- Sirur, S., Nurse, J. R. C., & Webb, H. (2018). Are we there yet? Understanding the challenges faced in complying with the General Data Protection Regulation (GDPR). In *Proceedings of the 2nd International Workshop on Multimedia Privacy and Security (MPS '18)*. ACM. <https://arxiv.org/pdf/1808.07338>
- Tsakalakis, N., Stalla-Bourdillon, S., Walker, M., & Carmichael, L. (2025). A framework for compliance with Regulation (EU) 2024/1689 for SMEs. *Laws*, 5(3), 40. <https://www.mdpi.com/2624-800X/5/3/40>
- United Nations University. (2024). Framework for the governance of artificial intelligence (UNU Tech Brief No. 5). https://digitallibrary.un.org/record/4082680/files/UNU-TB_5-2024_Framework-for-Governance-of-AI.pdf
- Walters, J., Dey, D., Bhaumik, D., & Horsman, S. (2024). Complying with the EU AI Act. In S. Nowaczyk et al. (Eds.), *Artificial Intelligence. ECAI 2023 International Workshops* (pp. 65–75). Springer. https://link.springer.com/chapter/10.1007/978-3-031-50485-3_5
- Wernick, A., & Meding, K. (2025). Beware! The AI Act can also apply to your AI research practices. arXiv. <https://arxiv.org/abs/2506.03218>
- William Fry LLP. (2024). A practical guide to the extraterritorial reach of the AI Act. <https://www.williamfry.com/knowledge/a-practical-guide-to-the-extraterritorial-reach-of-the-ai-act/>
- European Commission Community of Practice on Public Procurement of AI. (2025). EU AI Model Contractual Clauses (MCC-AI). <https://public-buyers-community.ec.europa.eu/communities/procurement-ai/resources/updated-eu-ai-model-contractual-clauses>