Stanford – Vienna
Transatlantic Technology Law Forum

A joint initiative of
Stanford Law School and the University of Vienna School of Law

European Union Law Working Papers

No. 122

The EU AI Act's Silent Impact on Corporate Roles

Maria Lucia Passador

2025

European Union Law Working Papers

Editors: Siegfried Fina and Roland Vogl

About the European Union Law Working Papers

The European Union Law Working Paper Series presents research on the law and policy of the European Union. The objective of the European Union Law Working Paper Series is to share "works in progress". The authors of the papers are solely responsible for the content of their contributions and may use the citation standards of their home country. The working papers can be found at http://ttlf.stanford.edu.

The European Union Law Working Paper Series is a joint initiative of Stanford Law School and the University of Vienna School of Law's LLM Program in European and International Business Law.

If you should have any questions regarding the European Union Law Working Paper Series, please contact Professor Dr. Siegfried Fina, Jean Monnet Professor of European Union Law, or Dr. Roland Vogl, Executive Director of the Stanford Program in Law, Science and Technology, at:

Stanford-Vienna Transatlantic Technology Law Forum
http://ttlf.stanford.edu

Stanford Law School
Crown Quadrangle
559 Nathan Abbott Way
Stanford, CA 94305-8610

University of Vienna School of Law
Department of Business Law
Schottenbastei 10-16
1010 Vienna, Austria

About the Author

Maria Lucia Passador is an Assistant Professor of Corporate Law and Financial Markets Regulation, Bocconi University, Milan (Italy); Associated Researcher, European Banking Institute; Research Fellow, Baffi Centre on Economics, Finance and Regulation; Affiliate, Transatlantic Technology Law Forum (TTLF), Stanford Law School.

General Note about the Content

Suggested Citation

This European Union Law Working Paper should be cited as:
Maria Lucia Passador, The EU AI Act's Silent Impact on Corporate Roles, Stanford-Vienna European Union Law Working Paper No. 122, http://ttlf.stanford.edu.

Copyright

Abstract

The European Union's AI Act is poised to reshape corporate governance and compliance well beyond Europe's borders. By expanding the responsibilities of directors, board secretaries, compliance officers, and in-house counsels, the Act redefines how companies must approach AI oversight, accountability, and risk management.

Board secretaries will need to embed AI governance into board procedures, ensuring directors fully understand the risks and opportunities tied to AI deployment. Compliance officers face heightened duties to implement robust risk management frameworks, conduct impact assessments, and manage regulatory reporting obligations. In-house counsels must address the complex allocation of liability, negotiate contractual safeguards, and anticipate conflicts in cross-border compliance regimes.

The AI Act's extraterritorial scope is particularly consequential for US companies: any AI system that touches the EU market—whether directly developed or simply used in an EU context—triggers regulatory obligations. High-risk AI systems carry stringent requirements around post-market monitoring, transparency, and human oversight.

Rather than focusing on granular requirements, this article highlights the AI Act's structural implications for corporate strategy and legal advisory functions, offering a forward-looking roadmap for mitigating AI-related risks while aligning governance and compliance practices with evolving global standards. For US executives and advisors, the AI Act serves as both a compliance challenge and a governance opportunity: it signals how the European regulation may set the tone for international AI governance and reshape liability, supply chains, and operational models in the transatlantic corporate landscape. In addition to charting regulatory effects, the paper makes a distinct legal-methodological contribution: by disaggregating the corporation into its governance roles, it provides the analytical framework that the AI Act itself leaves implicit, rendering its obligations operational within corporate practice.

Table of Contents

Believe me, Mr. Manager, I am an "unrealized" character, dramatically speaking;

and I find myself not at all at ease in their company.

Leave me out of it, I beg you.

— Luigi Pirandello, Six Characters in Search of an Author

I. Introduction: The AI Act and Its Transformative Impact on Key Stakeholders in the Legal Landscape

AI has moved from a peripheral tool to a central driver of corporate governance transformation reshaping business, governance, and society. Much like Prometheus gifting fire to humanity, AI grants corporations unparalleled analytical power, automation efficiencies, and strategic foresight. Yet, as in the ancient myth, this gift comes with risks that demand careful regulation. The European Union's Artificial Intelligence Act (the "AI Act" or the "Act")[1] seeks to harness AI's potential while mitigating harm, ensuring innovation aligns with the EU's core values. It introduces a risk-based framework[2] to uphold fundamental rights enshrined in the Charter of Fundamental Rights of the European Union, including data protection,[3] non-discrimination,[4] and access to remedies.[5] The AI Act distinguishes four levels of risk—unacceptable, high, limited, and minimal—

[1] 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), 2024 O.J. (L 238) 1, pmbl. recital 26.

[2] Lily Ballot Jones, Julia Thornton & Daswin De Silva, *Limitations of Risk-Based Artificial Intelligence Regulation: A Structuration Theory Approach,* 5 DISCOV. ARTIF. INTELL. 14 (2025); Martin Ebers, *Truly Risk-Based Regulation of Artificial Intelligence: How to Implement the EU's AI Act,* 16 EUR. J. RISK REGUL. 684 (2025), http://dx.doi.org/10.1017/err.2024.78; Isabel Kusche, *Possible Harms of Artificial Intelligence and the EU AI Act: Fundamental Rights and Risk,* J. RISK RES. 1 (May 2024), doi:10.1080/13669877.2024.2350720; Johanna Chamberlain, *The Risk-Based Approach of the European Union's Proposed Artificial Intelligence Regulation: Some Comments from a Tort Law Perspective*, 14 EUR. J. RISK REGUL. 1 (2023), https://doi.org/10.1017/err.2022.38.

[3] Charter of Fundamental Rights of the European Union art. 8, Dec. 18, 2000, 2000 O.J. (C 364) 1.

[4] Charter of Fundamental Rights of the European Union art. 21, Dec. 18, 2000, 2000 O.J. (C 364) 1.

[5] Charter of Fundamental Rights of the European Union art. 47 and pmbl. recital 6, Dec. 18, 2000, 2000 O.J. (C 364) 1. *See also* Oskar Josef Gstrein, *European AI Regulation: Brussels Effect versus Human Dignity?,* Z. EUR.-RECHTL. STUD. 755 (April 2022), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4214358; IE UNIVERSITY, DEMOCRACY RELOADED: AI TO PROTECT AND PROMOTE DEMOCRATIC GOVERNANCE (2025), https://site.unibo.it/hypermodelex/en/publications/2025-1-ie-university-ai4-democracy.pdf/@@download/file/2025-1-IE-UNIVERSITY-AI4-DEMOCRACY.pdf; Anna Pirozzoli, *The Human-centric Perspective in the Regulation of Artificial Intelligence,* 9 EUR. PAPERS (2024).

but it is the high-risk tier that matters most for corporate practice. This category is not abstract; it cuts directly into the marrow of ordinary business functions. Recruitment platforms that automatically rank candidates, workplace monitoring tools that track productivity, and performance dashboards that influence promotion or dismissal decisions all fall within its scope, as do credit scoring engines used by banks and fintech firms to decide who merits a loan or a mortgage. Insurers, too, cannot ignore the fact that algorithms calculating health or life premiums on the basis of personal data are treated as high-risk, since they touch on access to essential services. Even the provision of utilities such as electricity or telecommunications can come under this heading, where AI systems are used to decide on eligibility, continuity, or disconnection of service. Educational technologies that admit students, grade examinations, or police cheating, like safety components of critical infrastructure—energy grids, water supply, or transport systems controlled by predictive algorithms—are also firmly within the high-risk classification. The result is that the legal architecture of the AI Act is woven directly into the daily life of corporations: what appears on paper as a regulatory taxonomy translates in practice into a taxonomy of business activity, where credit, insurance, employment, education, and infrastructure are redefined as domains of heightened vigilance.

One of the AI Act's most contentious aspects lies in its sector-agnostic, risk-based approach.[6] This ostensibly pragmatic methodology raises significant concerns regarding its applicability and enforcement. This means that AI systems used in vastly different contexts—such as healthcare diagnostics and financial fraud detection—may be subjected to uniform obligations. From a corporate perspective, this approach creates a challenging compliance landscape. On one hand, it

[6] Unlike the U.S. model, which in general often relies on ex post enforcement through agencies such as the FTC or DOJ, the EU adopts an ex ante compliance regime that requires companies to implement risk management, documentation, and conformity assessments before deploying AI systems. This proactive methodology raises significant concerns regarding its applicability and enforcement.

inevitably leads to over-regulation in some cases and regulatory blind spots in others.[7] On the other hand, each company developing AI systems must undertake exhaustive risk assessments,[8] maintain extensive documentation, and ensure conformity with the Act's complex governance structures. For established enterprises, these requirements may be absorbed within existing regulatory compliance frameworks. However, for start-ups and SMEs, the administrative burden could stifle innovation and deter market entry.[9]

Moreover, the AI Act's extraterritorial reach, extending to providers and deployers of AI systems whose output is used within the EU, imposes compliance obligations on non-EU entities, potentially affecting global AI supply chains.[10] By potentially reshaping global AI supply chains and regulatory frameworks, the Act underscores its relevance for a wide international audience. As a result, this article is not only pertinent to EU-based readers but also highly relevant for non-EU policymakers, legal scholars, and industry leaders seeking to understand the broader impact of the AI Act on global markets and regulatory landscapes. For US corporations and policymakers in particular, the extraterritorial scope raises concrete questions: How should a US bank, a Silicon Valley start-up, or a multinational tech firm adapt its AI strategy to EU rules that apply regardless of where the system is built? This article, however, does not stop at describing these compliance burdens in general terms. It moves beyond them by analysing how the AI Act's provisions concretely reshape role-specific legal obligations for board secretaries, compliance officers, and in-house counsel, and by mapping their duties against existing fiduciary and liability doctrines in both EU and U.S. corporate law.

---

[7] 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), 2024 O.J. (L 238) 1, pmbl. recital 26.

[8] Jonas Schuett, *Risk Management in the Artificial Intelligence Act*, 15 EUR. J. RISK REGUL. 367 (2024) https://doi.org/10.1017/err.2023.1.

[9] AI Act, supra note 1, arts. 9, 11, 17, 43, and 62.

[10] AI Act, supra note 1, art. 2. *See also* Patrick Van Eecke & Bartholomäus Regenhardt, *Article 2. Scope*, *in* THE EU ARTIFICIAL INTELLIGENCE (AI) ACT: A COMMENTARY 22 (Nikolaus Forgó, Ceyhun Necati Pehlivan & Peggy Valcke eds., 2024).

As the regulatory landscape continues to evolve, the AI Act represents both an opportunity and a challenge for corporations.[11] On the one hand, it provides a structured legal environment that fosters trust and legal certainty in AI applications, as well as defines the boundaries for sharing best practices and providing sandboxes. On the other hand, its broad-brush, risk-based framework necessitates careful implementation strategies to ensure that the regulation achieves its intended objectives without unduly burdening industry stakeholders. Whether the AI Act will serve as a beacon of responsible AI governance or a bureaucratic constraint remains to be seen—a determination that will largely depend on how effectively it is interpreted, enforced, and adapted to the realities of AI deployment in practice. Much like AI itself, the AI Act is not static; it represents an ambitious attempt to impose order upon an ever-evolving technological landscape. However, it also faces the risk of remaining incomplete or inadequate, subject to continuous revision as innovation progresses. Indeed, the EU has already contemplated—and is likely to implement—postponements of enforcement.[12] At the same time, it bears emphasizing that the AI Act was drafted and passed before generative AI systems became a central force in research and business applications.[13] The regulation has not yet been updated to reflect the novel risks and governance challenges that generative AI introduces, even though policy discussions on this point are ongoing. This temporal gap underscores both the strength and (especially) the fragility of the Act: it is written to rein in a technology that continually evolves, but it inevitably lags behind fast-moving breakthroughs such as generative AI.

---

[11] Margot E. Kaminski, *Regulating the Risk of AI*, 103 B.U. L. REV. 1347 (2023), https://www.bu.edu/bulawreview/files/2023/11/KAMINSKI.pdf; Marco Barenkamp, *Der AI Act: Historische Chance Wegbürokratisiert?*, 16 WIRTSCHAFTSINFORMATIK & MANAGEMENT 87 (2024).

[12] Daphné Leprince-Ringuet & Miriam Partington, EU Could Pause AI Act Rollout Amid Industry Backlash: 'It's Really Toxic', *Sifted* (May 28, 2025), https://sifted.eu/articles/eu-ai-act-pause-analysis.

[13] The OECD's June 2025 working paper on generative AI (ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD), *The Effects of Generative AI on Productivity, Innovation and Entrepreneurship* (OECD Publishing 2025), https://www.oecd.org/en/publications/the-effects-of-generative-ai-on-productivity-innovation-and-entrepreneurship_b21df222-en.html) underscores the technology's role in transforming productivity, innovation, and entrepreneurship—highlighting benefits such as automating routine tasks, enhancing creativity, and lowering entry barriers, while flagging risks tied to trust, overreliance, and human expertise gaps.

Whether the AI Act is a finished work or still in progress, one reality is clear: AI regulation will always be an inherently dynamic challenge, a moving target. Yet, this debate cannot be framed solely as a question of regulatory flexibility versus rigidity. The absence of a structured legal framework—or an excessively lenient approach—carries significant risks, including systemic threats that could undermine fundamental rights, market stability, and public trust. Unregulated AI development, particularly in high-risk domains, poses profound ethical and societal concerns, from algorithmic bias and privacy violations to broader economic and security vulnerabilities. Thus, the question is not merely whether regulation should be adaptive but also how robust it must be to ensure that technological progress does not outpace legal safeguards. The ongoing tension between regulation and deregulation makes the search for balance a practical necessity—one that will shape the trajectory of AI governance for years to come. The AI Act, therefore, should not be viewed solely as a constraint on innovation but as a critical mechanism for steering AI development in a direction that is both responsible and sustainable.

This has far-reaching implications for how AI systems are developed, deployed, and governed across sectors—yet much of its practical enforcement will occur within the governance structures of private firms. These organisations must translate legal obligations into operational practice.[14] That translation is not abstract. It is mediated by specific *corporate actors*—compliance officers, in-house legal counsels, and board secretaries (namely corporate secretaries)—who serve as the institutional fulcrums of regulatory internalisation.

[14] Key stakeholders include corporate entities using AI, legal professionals advising on compliance, regulators overseeing AI applications, and consumers whose rights are protected. Businesses deploying AI in high-risk sectors—employment, finance, and critical infrastructure—must meet strict transparency, risk management, and oversight obligations. Legal professionals, whether in private practice or in-house, must now adopt a multidisciplinary approach encompassing data protection, liability, and sector-specific rules. Regulators, including national market surveillance authorities and the European AI Board, face the challenge of uniform enforcement, requiring enhanced expertise and cross-border coordination. Consumers gain enhanced protections against opaque AI decisions and discrimination, yet they also bear the burden of asserting their rights within an increasingly complex regulatory framework.

While the AI Act's general architecture—its scope, classification model, and compliance mechanisms— has received considerable attention from policy analysts and law firms,[15] and some have begun to analyse the AI Act's implications for corporate boards[16], financial law[17] and regulatory authorities,[18] further analysis is needed on how the AI Act reshapes the distribution of legal responsibilities across different functions. In particular, the AI Act prescribes what must be done, but not who, within a corporate entity, must do it. In doing so, it effectively assumes that compliance is a coherent, unitary function—that corporate actors can seamlessly translate legal requirements into practice, without friction, fragmentation, or intra-organisational contestation. The AI Act does not allocate responsibility within corporate structures; instead, it presumes organisational unity. This presumption has no doctrinal basis in corporate law, but it carries functional implications for compliance allocation. It elides the complex and distributed nature of decision-making within firms, where responsibility for compliance, governance, and legal oversight is typically fragmented across specialised roles. This article challenges that implicit assumption by foregrounding the differentiated

---

[15] Nancy B. Rapoport & Joseph R. Tiano, Jr, *Fighting the Hypothetical: Why Law Firms Should Rethink the Billable Hour in the Generative AI Era*, 20 WASH. J.L. TECH. & ARTS 41 (2025), https://digitalcommons.law.uw.edu/cgi/viewcontent.cgi?article=1351&context=wjlta; John Armour & Mari Sako, *AI-enabled Business Models in Legal Services: From Traditional Law Firms to Next-Generation Law Companies?,* 7 J. PROFESSIONS & ORG. 27 (2020). *See also* Zixuan Luo, *How Artificial Intelligence Is Reshaping Legal Practice*, NYU J. L. & BUS. ONLINE (2022), https://www.nyujlb.org/single-post/how-artificial-intelligence-is-reshaping-legal-practice.

[16] Floris Mertens, *The Use of Artificial Intelligence in Corporate Decision-Making at Board Level: A Preliminary Legal Analysis.* Financial Law Institute Working Paper Series 2023-01 (Jan. 27, 2023), https://financiallawinstitute.ugent.be/wp-content/uploads/2023/11/2023-01.pdf; Martin Petrin, *AI, New Technologies, and Corporate Governance: Three Phenomena* 47 SEATTLE U. L. REV. 1639 (2024), https://digitalcommons.law.seattleu.edu/sulr/vol47/iss5/4/; Paolo Agnese, Francesca Romana Arduino & Domenico Di Prisco, *The Era of Artificial Intelligence: What Implications for the Board of Directors?* 25 CORPORATE GOVERNANCE 272 (2025); ARUN SUNDARARAJAN, HOW CORPORATE BOARDS MUST APPROACH AI GOVERNANCE (Nov. 1, 2024) https://ssrn.com/abstract=5016014; Geneviève Helleringer & Florian Möslein, *AI & the Business Judgment Rule: Heightened Information Duty*, U. CHI. L. REV. ONLINE (2025), https://lawreview.uchicago.edu/online-archive/ai-business-judgment-rule-heightened-information-duty; Katja Langenbucher, *AI Judgment Rule(s)*, U. CHI. L. REV. ONLINE (2025), https://lawreview.uchicago.edu/online-archive/ai-judgment-rules; Maria Lillà Montagnani & Maria Lucia Passador, *Fiduciary Duties and Business Judgment Rule 2.0 in the AI Act Age* (forthcoming 2026).

[17] Maria Lucia Passador & Giovanni Bravi, *AI Meets Financial Regulation: Advancing the Algorithmic Shift.* EBI Working Paper Series (forthcoming 2025), https://ssrn.com/abstract=5224392; Antonella Sciarrone Alibrandi, Maddalena Rabitti & Giulia Schneider, *The European AI Act's Impact on Financial Markets: From Governance to Co-Regulation.* EBI Working Paper Series no 138 (2023), https://ssrn.com/abstract=4414559; Maria Lucia Passador, *AI in the Vault: AI Act's Impact on Financial Regulation.* Bocconi Legal Studies Research Paper No 4898828, 56 LOY. U. CHI. L.J. (forthcoming 2025), https://ssrn.com/abstract=4898828; Alessio Azzutti, *AI Governance in Algorithmic Trading: Some Regulatory Insights from the EU AI Act* (Aug. 27, 2024) https://ssrn.com/abstract=4939604.

[18] Maria Lucia Passador, *AI Act and the ECB: Steering Financial Supervision in the EU,* 30 COLUM. J. EUR. L. 259 (2025).

internal architecture through which the AI Act's obligations will be interpreted, operationalised, and contested. Rather than treating "the company" as a single compliance subject, the analysis disaggregates its internal actors—focusing in particular on board secretaries, compliance officers, and in-house legal counsels. These roles are not only structurally embedded in corporate governance frameworks, but also bear distinct relationships to the AI Act's substantive provisions. By treating corporate compliance as a *distributed institutional practice* rather than a unitary legal act, the article aims to render visible the organisational and normative frictions that are likely to arise in the implementation of AI regulation. Methodologically, this move is not descriptive alone: it applies corporate law analysis to supply the very guidelines the legislative text omits, showing how compliance must be allocated across roles. Consider, for instance, a U.S. bank deploying an AI credit scoring tool in Europe: the institution must redesign its risk management system to satisfy EU ex ante conformity assessments, while also navigating potential liability under U.S. consumer credit law. Or take a Silicon Valley HR-tech start-up expanding into the EU: its automated hiring algorithms must undergo EU fundamental rights impact assessments, exposing the firm to regulatory scrutiny it would not face at home.

The analysis focuses on three key corporate roles: board secretaries, compliance officers, and in-house legal counsels. These are not merely ancillary organisational functions but legally embedded and professionally codified roles whose institutional design predates the AI Act. Each plays a distinct part in mediating between the external demands of law and the internal machinery of corporate governance. As such, they are sites at which regulatory obligations are interpreted, translated, and operationalised—each with its own epistemic framework, institutional loyalties, and exposure to legal risk. For U.S. corporations, other roles central to American governance are also involved: Chief Risk Officers, who oversee enterprise-wide risk frameworks; Chief Privacy or Data Officers, who manage

data governance and General Data Protection Regulation (GDPR)[19] alignment; and Audit Committees, which U.S. boards rely on for oversight of compliance and disclosure obligations. These actors play functions parallel to their European counterparts but often with broader mandates, making them critical to any transatlantic compliance strategy.

The core contribution of this study is to render visible—and analytically tractable—the legal and organisational dynamics through which the AI Act is internalised. Rather than treating the corporation as a monolithic actor, the article disaggregates it into legally meaningful sites of role-specific responsibility.[20] In doing so, it reframes the AI Act not solely as a technocratic instrument of external regulation, but as a catalyst for *intra-corporate governance reform*. By theorising corporate roles as *legal intermediaries*—that is, actors who translate regulatory norms into operational routines—the paper highlights how legal compliance becomes a process of institutional negotiation, shaped by divergent mandates, bounded discretion, and role-specific vulnerabilities.

Taking inspiration from Pirandello's *Six Characters in Search of an Author*, this article examines whether the AI Act will truly shape the future of AI governance or whether, like Pirandello's characters, it will remain a work in progress, awaiting its definitive form. Through a detailed analysis of the regulation's provisions, its implications for corporate actors, and its potential long-term trajectory, the discussion aims to provide key takeaways for legal professionals, policymakers, and businesses navigating this evolving landscape.

The discussion unfolds as follows: Part 2 situates the AI Act within the broader context of European AI governance, examining its key provisions and regulatory philosophy. Part 3 identifies the constellation of actors governed by the AI Act, distinguishing internal corporate roles from external stakeholders such as providers, deployers, and regulators. Parts 4 to 6 examine in turn the functions

[19] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), 2016 O.J. (L 119) 1.

[20] *See also* Martin Petrin, *Corporate Management in the Age of AI,* 2019 COLUM. BUS. L. REV. 965, 972 (2019).

and legal obligations of board secretaries, compliance officers, and in-house counsels. The concluding Part reflects on the AI Act's future, on how a role-differentiated approach to AI governance may inform broader debates on regulatory design, liability distribution, and the institutional preconditions for responsible AI development.

The stage is set. The roles are assigned. The question remains: will the AI Act bring coherence to AI governance, or will its characters remain in search of an author?

II. AI Act: Regulatory Framework and Governance Objectives

In keeping with the familiar adage that America invents, China copies, and Europe regulates,[21] the EU has introduced the AI Act: an ambitious and unprecedented legislative framework designed to harmonise AI governance across the internal market while safeguarding fundamental rights, security, and the rule of law. It seeks to prevent a fragmented regulatory landscape—where Member States might impose diverging standards—by establishing a uniform, risk-based classification system that balances innovation with accountability.

At its core, the AI Act embraces a tiered approach to risk management,[22] distinguishing between AI systems that pose an unacceptable risk[23]—which are outright prohibited[24]—and those classified as high-risk, which are subject to stringent legal and technical requirements.[25] The first

[21] Enrique Dans, *The United States Invents, China Imitates… and Europe Regulates?*, Medium (Jan. 27, 2024), https://medium.com/enrique-dans/the-united-states-invents-china-imitates-and-europe-regulates-e465ff293d82.

[22] Ebers, *Truly Risk-Based Regulation of Artificial Intelligence: How to Implement the EU's AI Act*, supra note 2; Schuett, *Risk Management in the Artificial Intelligence Act*, supra note 8.

[23] AI Act, supra note 1, art. 5. *See also* Els J. Kindt & Catherine Jasserand, *Article 5. Prohibited AI Practices*, *in* THE EU ARTIFICIAL INTELLIGENCE (AI) ACT: A COMMENTARY 105 (Nikolaus Forgó, Ceyhun Necati Pehlivan & Peggy Valcke eds., 2024).

[24] Paul Voigt & Nils Hullen, *What AI Practices Are Prohibited?, in* THE EU AI ACT: ANSWERS TO FREQUENTLY ASKED QUESTIONS 37 (Paul Voigt & Nils Hullen eds., 2024).

[25] Henry Fraser & José-Miguel Bello y Villarino, *Acceptable Risks in Europe's Proposed AI Act: Reasonableness and Other Principles for Deciding How Much Risk Management Is Enough,* 15 EUR. J. RISK REGUL. 431. *See also* Claudio Novelli, *Taking AI Risks Seriously: A New Assessment Model for the AI Act*, 39 AI & SOC'Y 2493 (2024); Johann Laux, Sandra Wachter & Brent Mittelstadt, *Trustworthy Artificial Intelligence and the European Union AI Act: On the Conflation of Trustworthiness and Acceptability of Risk*, 18 REGULATION & GOVERNANCE 3 (2024).

category includes practices deemed incompatible with EU values,[26] including the use of AI for subliminal manipulation,[27] social scoring by public authorities,[28] and certain biometric categorisation systems.[29] The second one includes AI systems deployed in sensitive areas such as law enforcement, employment, and critical infrastructure,[30] and it covers AI applications used in biometric identification,[31] migration control, and access to essential services[32]—areas where AI has a profound impact on individuals' rights and societal structures. These systems must adhere to a robust compliance framework encompassing data governance, human oversight,[33] transparency obligations, risk mitigation, and cybersecurity resilience. A third category encompasses limited-risk AI, which triggers specific transparency obligations. Examples include chatbots and recommendation systems, where users must be informed they are interacting with AI. The final category, minimal-risk AI, remains largely outside the scope of binding regulation, though industry standards and codes of conduct are expected to guide good practice. Taken together, this tiered framework translates the abstract notion of "AI risk" into a practical governance map for corporations, signalling where compliance resources must be concentrated and where lighter-touch obligations suffice.

This sector-agnostic, risk-based approach is both the AI Act's greatest strength and its most immediate challenge: it mirrors the EU's historical approach to digital regulation, following in the footsteps of the GDPR by setting global benchmarks for AI governance.[34] Because uniform

---

[26] Rostam Josef Neuwirth, *Prohibited Artificial Intelligence Practices in the Proposed EU Artificial Intelligence Act* (2022), https://ssrn.com/abstract=4261569.

[27] AI Act, supra note 1, art. 5(1)(a).

[28] AI Act, supra note 1, art. 5(1)(c).

[29] AI Act, supra note 1, art. 5(1)(g).

[30] AI Act, supra note 1, art. 6, Annex III. *See also* Guillaume Couneson, *Article 6. Classification Rules for High-Risk AI Systems*, *in* THE EU ARTIFICIAL INTELLIGENCE (AI) ACT: A COMMENTARY 193 (Nikolaus Forgó, Ceyhun Necati Pehlivan & Peggy Valcke eds., 2024).

[31] AI Act, supra note 1, Annex III.

[32] AI Act, supra note 1, Annex III.

[33] Melanie Fink, *Human Oversight under Article 14 of the EU AI Act* (Feb. 14, 2025), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5147196 and Argyri Panezi, *Article 14. Human Oversight*, *in* THE EU ARTIFICIAL INTELLIGENCE (AI) ACT: A COMMENTARY 351 (Nikolaus Forgó, Ceyhun Necati Pehlivan & Peggy Valcke eds., 2024).

[34] Nathalie A. Smuha, *The Paramountcy of Data Protection Law in the Age of AI (Acts), in* TWO DECADES OF PERSONAL DATA PROTECTION. WHAT NEXT? (EDPS 20th Anniversary, Publications Office of the European Union 2024)

obligations apply across domains as diverse as healthcare diagnostics and financial fraud detection, firms face uneven compliance burdens. Large institutions may integrate AI Act requirements into existing regulatory frameworks—folding conformity assessments and risk audits into well-developed compliance departments—while start-ups and SMEs may find the administrative load prohibitive. For legal advisors, the point is not that the Act balances innovation against regulation in the abstract, but that it requires a careful calibration of internal governance: designing documentation systems that keep pace with iterative AI updates, embedding risk management into enterprise-wide frameworks, and ensuring technical transparency obligations are matched by legally robust reporting structures.

The extraterritorial scope of the AI Act amplifies these challenges. Any AI system whose output is used within the EU falls under the AI Act, regardless of where it was developed or deployed.[35] The regulation is designed to prevent regulatory arbitrage, ensuring that AI developers and corporations cannot bypass EU rules simply by relocating operations to more permissive jurisdictions.[36] Moreover, this extraterritorial approach aligns with the EU's broader digital sovereignty strategy,[37] reinforcing its position as a global standard-setter. A U.S. bank using AI-driven credit scoring for EU clients must undergo EU-prescribed conformity assessments. A multinational tech firm offering AI-powered chatbots to EU consumers must comply with transparency and disclosure requirements, even if development occurs entirely outside Europe. These examples illustrate that EU law effectively travels with the AI system, creating a compliance perimeter that is both territorial and functional. For corporate counsels and company secretaries, the implications are

https://ssrn.com/abstract=4874388; Josephine Wolff, William Lehr & Christopher S Yoo, *Lessons from GDPR for AI Policymaking*, 27 VA. J. L. & TECH. (2024), https://ssrn.com/abstract=4528698.

[35] Jan Šamlot, *The Artificial Intelligence Act and Its Application on Non-EU Persons, in* TURKISH-CZECH CROSS-BORDER TRADE INFRASTRUCTURE: ENSURING THE DOOR BETWEEN CENTRAL AND EASTERN EUROPE AND THE NEAR EAST REMAINS OPEN 95 (Alexander J. Bělohlávek, Naděžda Rozehnalová & Jan Šamlot eds., 2024), https://ssrn.com/abstract=4990462.

[36] AI Act, supra note 1, art. 5.

[37] Tessel van Oirsouw, *AI, Digital Sovereignty, and the EU's Path Forward: A Case for Mission-Oriented Industrial Policy* (Nov. 20, 2024), https://ash.harvard.edu/resources/ai-digital-sovereignty-and-the-eus-path-forward-a-case-for-mission-oriented-industrial-policy/; WORLD ECONOMIC FORUM, WHAT IS DIGITAL SOVEREIGNTY AND HOW ARE COUNTRIES APPROACHING IT? (JAN. 10, 2025), https://www.weforum.org/stories/2025/01/europe-digital-sovereignty/.

immediate. EU obligations may collide with third-country laws—most notably U.S. trade secret protections that restrict disclosure of proprietary algorithms, even as EU regulators demand transparency. Compliance officers must ensure documentation and oversight mechanisms are accessible to EU authorities, while also safeguarding against liability exposures in home jurisdictions, where EU-mandated disclosures can migrate into shareholder litigation or consumer class actions. The extraterritorial dimension of the AI Act therefore does more than complicate compliance: it transforms EU regulation into a transatlantic governance challenge, forcing corporations to align global risk management systems with European expectations and to anticipate conflicts of law that were once peripheral but now sit at the centre of strategic planning. Whether this approach will lead to greater global harmonisation or provoke resistance from other AI superpowers remains an open question, but its international impact is likely to be profound and long-lasting.

III. Key Stakeholders Under the AI Act: Six Characters in Search of an Author

Pirandello's six characters arrive unfinished, haunting a rehearsal, demanding an author to complete their fragmented story. The AI Act's cast is less spectral but no less unsettled: roles are inscribed in law, yet coherence awaits the many "authors" of regulation, courts, and corporate practice. The parallel illuminates both promise and limit—the characters here are obligations, not phantoms, yet the play of governance remains unfinished.

What sets the AI Act apart, however, is not merely the breadth of its regulatory net but the specificity with which it delineates who owes what obligation. Whereas most regulatory frameworks—including the GDPR—focus on the conduct to be controlled, the AI Act goes further: it focuses on the cast. By expressly cataloguing providers, importers, distributors, deployers, regulators, and even public authorities—and by indirectly reaching into the practices of data suppliers through strict rules on training and testing datasets—the Act requires its obligations to be internalised by companies through their governance structures. Crucially, the AI Act does not, strictly speaking,

assign statutory duties to compliance officers, board secretaries, or in-house counsel. Rather, these obligations, formally directed at providers and deployers, must be translated into practice by management decisions about how compliance is organised internally. In this sense, the law prescribes what must be done but leaves to corporate governance the task of deciding who within the firm will do it. This legislative choice is more than bureaucratic drafting. It shifts the legal imagination from a model where compliance is an abstract behavioral standard to one where compliance becomes a role-bound responsibility embedded in institutional architecture. This move matters for at least three reasons. First, it mirrors the complex reality of AI, which is rarely the product of a single actor but the outcome of distributed chains of design, training, distribution, and deployment. Second, it operationalizes accountability: by tethering duties to identified roles, the AI Act makes enforcement and liability tractable in practice. And third, it provides a governance map for corporations, compelling them to ask not just what must be done, but how responsibility must be distributed among their own officers and committees.[38] In this sense, the AI Act is not only a compliance code but also a dramaturgical script—introducing a cast of regulatory characters whose interactions will define how AI governance unfolds in practice. This structural feature underpins the central metaphor of this article: it assembles its characters on stage, but leaves open the question of how they will perform their roles in the evolving drama of AI governance.

The following analysis adopts a subject-centric approach to examine the principal entities to whom the AI Act is explicitly addressed, as well as those whom it does not directly target but whose roles will nonetheless be profoundly affected by its regulatory framework. To maintain scope and focus, this study examines in depth the corporate actors most directly affected by the regulation, while briefly noting other stakeholders and directing further discussion to the existing literature. The sequence that follows—A through F—is not incidental. It mirrors the structural logic of the AI Act

[38] This structural reading exemplifies the legal methodology adopted throughout the paper: by mapping obligations onto specific institutional roles, the analysis develops normative guidance that the AI Act itself does not supply.

itself, moving from the point of technological origin outward toward the social periphery. First come the *Architects* and *Brokers of the Shadows*, who generate or supply the raw material of AI; then the *Gatekeepers* who introduce those systems into the market; followed by the *Enforcers* and *Overseers*, whose task is to police and supervise compliance. Only after tracing this institutional arc do we arrive at the *Silent Protagonists*—the individuals whose rights and lives are most directly shaped by AI—and, finally, the *Overlooked* figures within corporations, whose duties may be less visible yet decisive in translating regulatory mandates into governance practice. The order thus reflects a deliberate dramaturgy: from production, to mediation, to enforcement, to impact, and ultimately to the hidden custodians of compliance.

A. The Architects (and the Brokers of the Shadows): From AI Providers and Developers To Data Brokers and Data Marketplaces

At the foundation of the AI Act's regulatory framework lie *providers*—the entities responsible for developing, training, and placing AI systems on the market or putting them into service within the EU. Defined as "a natural or legal person, public authority, agency, or other body that develops an AI system or has an AI system developed with a view to placing it on the market or putting it into service under its own name or trademark, whether for payment or free of charge,"[39] providers bear the heaviest regulatory burdens.[40]

(i) … and the Brokers of the Shadows: Data Brokers and Data Marketplaces

In the narrative, data brokers and data marketplaces emerge as—elusive yet omnipresent entities operating in the liminal space between legality and opacity. They do not create AI but feed

[39] AI Act, supra note 1, art. 3(4).

[40] Their obligations vary depending on the risk classification of their AI systems, with the most stringent requirements applying to high-risk AI systems as listed in AI Act, supra note 1, Annex III.

it, serving as the traffickers of the digital age's most coveted commodity: data. They aggregate, curate, and monetize vast datasets, supplying the raw material for training and fine-tuning AI models.

The AI Act introduces comprehensive regulatory provisions concerning data governance, particularly in relation to data brokers and data marketplaces, which play a critical role in the development and training of artificial intelligence systems.[41] While it does not explicitly define "data brokers" or "data marketplaces," several articles and recitals address the governance of data, data quality requirements, and the role of data providers in ensuring AI system compliance.

A key aspect of the AI Act is the regulation of training, validation, and testing data used to develop AI models: high-risk AI systems that utilise data for training purposes must adhere to strict data governance and management practices.[42] These requirements ensure that datasets used in AI development, including those acquired from data brokers or sourced from data marketplaces, meet high standards of accuracy, representativeness, and fairness to prevent biases that could impact fundamental rights, particularly in cases where AI outputs influence future decisions.[43]

Furthermore, the AI Act interacts with the EU's broader data governance framework, particularly in the context of the European Data Spaces initiative,[44] which facilitates trustworthy and non-discriminatory access to high-quality data for AI training. The role of data brokers and data marketplaces is crucial in this ecosystem, as they facilitate the trade of large-scale datasets, which are fundamental for the development of AI systems. However, their operations are subject to strict compliance requirements, especially regarding personal data protection. This emphasis on personal data protection is not merely a technical requirement but reflects a deeper continuity with the EU's broader regulatory tradition. Much as the GDPR entrenched a rights-based model of digital

---

[41] Although with reference to the previous draft of the AI, *see* Santiago Andrés Azcoitia & Alba Ribera Martínez, *Data Marketplaces and the Data Governance Act: A Business Model Perspective* (Sept. 18, 2023), https://competitionlawblog.kluwercompetitionlaw.com/2023/09/18/data-marketplaces-and-the-data-governance-act-a-business-model-perspective/.

[42] AI Act, supra note 1, art. 10.

[43] Kusche, *Possible Harms of Artificial Intelligence and the EU AI Act: Fundamental Rights and Risk*, supra note 2.

[44] EUROPEAN COMMISSION, DATA SPACES, https://digital-strategy.ec.europa.eu/en/policies/data-spaces.

governance, the AI Act similarly grounds its legitimacy in the protection of data rights and, by extension, human rights. In both frameworks, the EU deliberately elevates the individual as the normative reference point of regulation, making dignity, autonomy, and fairness the touchstones against which technological systems are assessed. This choice is neither inevitable nor universal: one might have expected AI regulation to be framed primarily around product safety, innovation incentives, or market integrity. Yet the EU has chosen a path that places human welfare at the center, treating both data and algorithmic processes as domains in which individual rights must prevail. Introducing this connection early underscores that the AI Act, like the GDPR before it, is less about technical compliance in isolation and more about embedding fundamental rights into the architecture of digital governance.

Lastly, the Act clarifies that the AI regulatory framework does not override existing EU laws on data protection, including the GDPR and the ePrivacy Directive,[45] which impose obligations on data controllers and processors.

B. The Gatekeepers: Importers, Distributors, and Deployers

The AI Act's regulatory scope extends well beyond developers, imposing significant compliance duties on those introducing, distributing, and deploying AI systems in the EU. Importers,[46] distributors,[47] and deployers[48] act as key gatekeepers, ensuring compliance with legal and ethical standards. This layered regulatory approach reflects a core principle: accountability extends across the entire AI lifecycle, from market entry to application in employment, finance, healthcare, and education.

---

[45] Directive 2002/58, of the European Parliament and of the Council of 12 July 2002 concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications), 2002 O.J. (L 201) 37 (EC).

[46] AI Act, supra note 1, art. 25.

[47] AI Act, supra note 1, art. 24.

[48] AI Act, supra note 1, art. 26.

Distributors—who place AI systems on the market without major modifications[49]—must verify CE marking, documentation, and providers' and importers' compliance.[50] If they become aware of non-compliance, they must suspend distribution and notify authorities. This structure prevents AI systems developed outside the EU from bypassing regulatory requirements, reinforcing legal certainty and consumer protection.

Deployers—organisations integrating AI into operations, decision-making, or public services—bear the broadest obligations. They must ensure regulatory compliance, including data protection, transparency, and human oversight, and conduct regular assessments to mitigate risks to fundamental rights.[51]

By holding importers, distributors, and deployers accountable, the AI Act shifts governance from mere technological oversight to active risk management. Deployers—whether businesses, financial institutions, hospitals, or universities—must balance AI's efficiencies with legal duties of fairness and transparency, ensuring AI serves the public interest without compromising fundamental rights.

C. The Enforcers: Public Authorities and Law Enforcement

One of the most contentious aspects of the AI Act is its regulation of AI use by public sector deployers, particularly in the domains of law enforcement, immigration, and border control.[52] The Act takes a firm stance against certain AI applications deemed incompatible with fundamental rights, explicitly prohibiting predictive policing,[53] which relies on algorithmic assessments of individuals' likelihood to commit crimes, and social scoring,[54] which in turn involves assigning individuals scores

[49] AI Act, supra note 1, art. 3(7).

[50] AI Act, supra note 1, art. 24.

[51] AI Act, supra note 1, art. 26. High-risk AI deployers face regulatory audits and potential financial penalties under Chapter VII, Section 1.

[52] *Ex multis, see* Kasia Söderlund & Stefan Larsson, *Enforcement Design Patterns in EU Law: An Analysis of the AI Act,* 3 DIGITAL SOC'Y 41 (2024).

[53] AI Act, supra note 1, art. 5(1)(c).

[54] AI Act, supra note 1, art. 5(1)(d).

based on their social behavior or personal characteristics. These prohibitions reflect deep concerns over the potential for algorithmic discrimination, exacerbation of existing biases, and the erosion of due process and individual autonomy. At the same time, it is important to stress that these prohibitions are not confined to the public sector. Article 5(1)(c) and (d) adopt broad market-facing language, banning the *placing on the market* or *putting into service* of prohibited AI systems regardless of whether the actor is public or private. In practice, this means that private providers and developers are primarily addressed by the prohibitions, while public authorities are regulated insofar as they might procure or deploy such systems. The bans therefore serve a dual function: ex ante, by restricting providers from offering such systems on the EU market, and ex post, by constraining public deployers in sensitive domains such as policing, migration, or social services.

However, beyond these outright bans, the AI Act also imposes stringent restrictions on biometric identification technologies, particularly real-time and post-event remote biometric identification (RBI) systems used in public spaces.[55]

The AI Act's regulatory approach to public sector deployers illustrates the EU's broader attempt to establish a regulatory model that prioritizes fundamental rights although allowing room for narrowly tailored security applications. Yet, the Act does not resolve all concerns surrounding government AI use. The effectiveness of its safeguards will largely depend on the rigor of national enforcement, the independence of judicial or administrative oversight bodies, and the willingness of courts to challenge overbroad security justifications. Moreover, given the rapid pace of technological advancement, the Act's provisions may soon face pressure to adapt to emerging AI capabilities, raising the question of whether its restrictions will remain effective in preventing disproportionate surveillance while ensuring legitimate security needs are met.

[55] AI Act, supra note 1, Annex III.

D. The Overseers: Regulators and Compliance Bodies

The AI Act establishes a robust multi-tiered enforcement framework, ensuring that compliance is not merely aspirational but effectively monitored and sanctioned.[56] At the core of this structure lies a decentralized system of national supervisory authorities,[57] complemented by a European Artificial Intelligence Board (EAIB)[58], which provides coordination and guidance at the EU level. This governance model mirrors the structure introduced by the GDPR, in which national data protection authorities work alongside the European Data Protection Board to ensure harmonized application across Member States. However, the AI Act's enforcement mechanisms introduce additional layers of oversight and cooperation, reflecting the complexity of AI governance and the need for sector-specific expertise.

E. The Silent Protagonists: Consumers, Workers, and Society

At the heart of the AI Act lies a consistent regulatory philosophy already visible in the GDPR: the insistence that digital governance must ultimately safeguard the rights, freedoms, and agency of individuals. Where the earlier data protection regime enshrined privacy and data dignity as fundamental rights, the AI Act extends this normative trajectory to algorithmic decision-making itself. In doing so, it shifts the focus from abstract technical conformity to the lived experience of consumers, workers, and citizens—those who are most exposed to the consequences of AI systems in their daily lives. Legally, their relevance lies in the fact that the AI Act is fundamentally a rights-based regulation: although consumers, workers, and citizens do not bear direct statutory duties under

---

[56] On this topic, *see* Hans-W. Micklitz & Giovanni Sartor, *Compliance and enforcement in the AIA through AI*, 43 YEARBOOK EUR. L. 297 (2024).

[57] AI Act, supra note 1, art. 70.

[58] AI Act, supra note 1, art. 65. *See also* Claudio Novelli et al., *A Robust Governance for the AI Act: AI Office, AI Board, Scientific Panel, and National Authorities,* 16 EUR. J. RISK REGUL. 566 (2025); Paul Voigt & Nils Hullen, *How Is the AI Act Implemented and Enforced?, in* THE EU AI ACT. ANSWERS TO FREQUENTLY ASKED QUESTIONS 37 (Paul Voigt & Nils Hullen eds., 2024), chapter 6; Maria Lucia Passador, *AI in the Vault: AI Act's Impact on Financial Regulation*, supra note 17.

the Act, they are its ultimate normative reference point. The AI Act's risk-based framework, prohibitions, and high-risk obligations are explicitly designed to safeguard their fundamental rights under the EU Charter, positioning them as the ultimate beneficiaries—and, thus. the silent protagonists—of the regulatory architecture. The measure of the Act's effectiveness, therefore, lies not in the precision of its technical annexes but in its capacity to protect these silent protagonists of the digital transition. Workers operating under algorithmic management, consumers unknowingly profiled by opaque AI models, and citizens navigating an increasingly automated public sphere all stand at the center of this legal experiment. These individuals, often unaware of the mechanisms shaping their opportunities, risks, and rights, are the silent protagonists of this legislative shift.[59]

As to workers,[60] AI-powered decision-making tools have become pervasive in employment contexts, from automated hiring systems to performance-tracking software and algorithmic scheduling. Under the AI Act, systems deployed in employment and worker management are deemed high-risk, thereby triggering the relevant obligations.[61]

Consumers, too, are vulnerable to AI systems designed to analyze their behavior, predict purchasing patterns, and personalize digital experiences. While personalization can improve convenience and user satisfaction, it may also open the door to exploitative practices such as price discrimination, microtargeting, and behavioral manipulation. To counter these risks, the AI Act establishes transparency obligations for AI systems that interact directly with individuals—such as chatbots and recommendation engines—requiring that people are informed when they are engaging with an AI rather than a human. These obligations are concretized in Articles 50–52, which impose

---

[59] Karolina Iwańska et al, *Towards an AI Act that Serves People and Society: Strategic Actions for Civil Society and Funders on the Enforcement of the EU AI Act* (Aug. 2024), https://europeanaifund.org/wp-content/uploads/2024/09/240827_FINAL_AI_ACT_Enforcement.pdf.

[60] On labor law matters, *see* Chiara Cristofolini, *Navigating the Impact of AI Systems in the Workplace: Strengths and Loopholes of the EU AI Act from a Labour Perspective* (July 18, 2024), https://illej.unibo.it/article/view/19796; Zahra Yusifli, *Labour Rights and the EU Artificial Intelligence Act: How to Get Away with High-Risk AI*. University of Luxembourg Law Research Paper No 2025-01 (Jan. 15, 2025), https://ssrn.com/abstract=5098359.

[61] AI Act, supra note 1, arts. 9 and 29.

duties to disclose when individuals interact with conversational AI, when biometric categorisation or emotion recognition systems are used, and when deepfakes or other synthetic content are generated.[62]

F. The Overlooked: Directors, Board Secretaries, and In-House Counsels

As the AI Act establishes a harmonized legal framework for AI, corporate entities face an evolving landscape of compliance, risk management, and ethical governance.[63] Among these corporate actors, directors naturally remain at the forefront of corporate decision-making and are therefore not 'overlooked' in any substantive sense. Indeed, their fiduciary and oversight duties in relation to AI are the subject of a separate discussion in a companion paper.[64] Their appearance here

---

[62] For a thorough comment about this provision, *see* Thomas Gils, *Article 50. Transparency Obligations for Providers and Deployers of Certain AI Systems*, *in* THE EU ARTIFICIAL INTELLIGENCE (AI) ACT: A COMMENTARY 776 (Nikolaus Forgó, Ceyhun Necati Pehlivan & Peggy Valcke eds., 2024).

[63] On the latter aspect, *see* Robert C. Solomon, *Corporate Roles. Personal Virtues: An Aristolelean Approach to Business Ethics*, 2 BUS. ETHICS Q'LY 317 (1992) (highlighting how business ethics has become embedded in corporate practice and education, with managerial virtue and responsibility placed at the core of governance).

[64] Montagnani & Passador, supra note 16. Please consider that, as the corporate governance structures of European jurisdictions vary significantly, shaping the composition, role, and obligations of board directors in ways that directly influence the implementation of regulatory mandates such as those introduced by the AI Act. Broadly speaking, to this end, EU corporate models can be categorised into unitary and dual-board systems, with each framework imposing distinct responsibilities on directors in terms of compliance, risk oversight, and strategic decision-making. In jurisdictions such as the United Kingdom and Italy, companies primarily adopt a unitary board structure, where executive and non-executive directors sit on the same board, collectively responsible for corporate decision-making and compliance. This model tends to centralise AI governance within the board itself, making directors directly accountable for ensuring that AI-related risks are managed and regulatory obligations fulfilled. By contrast, Germany and the Netherlands operate under a dual-board system, where supervisory and management boards are institutionally separated, with the former overseeing strategic and compliance issues while the latter handles operational matters. In such systems, the AI Act's requirements on high-risk AI governance, transparency, and risk mitigation may fall primarily within the remit of the management board, whereas the supervisory board exercises oversight and ensures alignment with broader corporate governance principles. France presents yet another variation, offering companies the flexibility to choose between unitary and dual-board structures, thereby influencing the degree to which AI compliance is a board-level responsibility versus a delegated function within corporate risk management teams. Additionally, the presence of worker representatives in the supervisory boards of countries such as Germany and Sweden introduces an additional layer of AI-related scrutiny, as labour concerns regarding AI-driven decision-making, algorithmic bias, and workplace automation are more likely to be actively addressed at the governance level. These structural distinctions have profound implications for the enforcement of AI regulations, as the allocation of responsibility for compliance, risk oversight, and liability mitigation depends not only on the statutory obligations set forth in the AI Act but also on the specific governance model in place. A comparative assessment of these frameworks is therefore crucial in understanding how AI regulation reshapes corporate oversight and the evolving role of board directors across different European jurisdictions.

is only to underscore the continuity between visible board-level responsibility and the less conspicuous—but equally consequential—roles that follow.

As the AI Act establishes a harmonized legal framework for AI, corporate entities face an evolving landscape of compliance, risk management, and ethical governance. Among these corporate actors, directors naturally remain at the forefront of corporate decision-making; however, as they are the subject of a separate discussion in a companion paper, our focus here is on the not-to-be-forgotten figures in corporate governance, whose responsibilities, though less conspicuous, are no less consequential in shaping AI compliance and risk management. The Overlooked—comprising board secretaries, compliance officers, and in-house counsels—serve as the key figures in translating regulatory requirements into corporate policies, ensuring that AI governance aligns with both legal obligations and strategic business objectives. It is true that regulatory obligations have long been formally addressed to the company as a legal person, without prescribing the precise internal pathways through which compliance must be operationalised. The AI Act is not exceptional in this respect. What is distinctive, however, is how its dense and technical obligations redistribute weight across corporate roles that are usually less visible. Translating conformity assessments, post-market monitoring, and documentation duties into practice inevitably falls to board secretaries, compliance officers, and in-house counsels. By foregrounding these actors, the analysis highlights the organisational fragmentation of compliance—revealing how distinct institutional loyalties, technical capacities, and exposures to liability shape the way AI regulation is internalised within the firm.

Their role is particularly critical in the context of Title III, Chapter 2 of the AI Act, which details obligations related to high-risk AI systems, including conformity assessments,[65] post-market monitoring,[66] and the maintenance of technical documentation.[67] Needless to say, the degree of influence exercised by in-house counsels in AI compliance and governance is inextricably linked to

[65] AI Act, supra note 1, art. 43.
[66] AI Act, supra note 1, art. 72.
[67] AI Act, supra note 1, art. 11.

the structural allocation of compliance and risk management functions within a corporation. In jurisdictions or corporate frameworks where compliance is highly centralised—often under the direct oversight of a chief compliance officer or a dedicated legal and risk management department—legal professionals may assume a more strategic role, shaping AI governance policies, negotiating regulatory risks, and advising the board on liability mitigation. Their involvement is typically proactive, ensuring that AI deployment aligns with regulatory mandates and corporate risk tolerance. Conversely, in decentralised compliance structures—where risk oversight is dispersed across multiple departments or delegated to regional subsidiaries—the role of in-house counsels may be less pronounced, often limited to providing ex-post legal assessments or addressing AI-related disputes once they arise. In such cases, their capacity to influence AI governance at an early stage is diminished, as operational compliance decisions may be taken by business units with varying levels of legal oversight. This fragmentation can lead to inconsistencies in AI risk management strategies, increasing the likelihood of regulatory exposure. Thus, the impact of legal professionals in ensuring AI compliance is not merely a function of regulatory obligations but is also contingent on the internal corporate architecture governing compliance and risk oversight.

Collectively, the Overlooked shape the corporate response to AI regulation, ensuring that businesses not only meet compliance requirements but also proactively manage AI-related risks and ethical considerations. By bridging the gap between legal mandates and corporate strategy, they define how AI is governed within organisations, influencing the long-term sustainability and trustworthiness of AI-driven innovations. From a U.S. perspective, it is also important to recognize the role of Chief Risk Officers, Chief Privacy Officers, and Audit Committees. While not explicitly referenced in the AI Act, these functions are deeply embedded in U.S. corporate governance. CROs can integrate AI risk into broader enterprise risk management systems; CPOs serve as natural counterparts to EU Data Protection Officers in aligning AI with data protection law; and Audit Committees act as a board-level checkpoint for AI-related disclosures and internal controls. Together, they provide an

additional layer of accountability that mirrors, and in some cases extends, the European governance model.

IV. Board Secretaries Under The AI Act

Board secretaries, traditionally tasked with ensuring regulatory compliance and facilitating communication between the board and corporate stakeholders,[68] now bear the additional burden of ensuring AI-related disclosures and governance structures align with the AI Act's stringent transparency and oversight provisions. Given the Act's implications for companies deploying AI in key business functions—including recruitment, risk assessment, and customer interaction—the board of directors must ensure robust compliance mechanisms are in place, with the secretary playing a pivotal role in aligning AI governance with corporate policies and regulatory requirements.

A. Legal and Governance Implications

High-risk AI systems are subject to enhanced obligations, particularly where they impact fundamental rights, safety, and legal compliance.[69] These include AI applications in employment and recruitment processes,[70] creditworthiness assessments,[71] and critical infrastructure management.[72] Companies deploying such AI must follow mandatory risk management systems, data governance frameworks, transparency measures, and human oversight mechanisms.[73] The board of directors is responsible for ensuring that corporate AI strategies comply with these requirements, necessitating the implementation of internal policies governing AI deployment, documentation of compliance efforts, and periodic auditing of AI-related risks. From a U.S. corporate law perspective, these

[68] *Ex multis*, on the role of board secretaries, *see* Bin Liu, David Ahlstrom & Yutong Zhang, *The Schizophrenic Board Secretary: An Embedded Agent Between Multiple Stakeholders and Financial Misconduct,* BR. ACCOUNT. REV. 101323 (2024).
[69] AI Act, supra note 1, art. 6.
[70] AI Act, supra note 1, Annex III, § 5.
[71] AI Act, supra note 1, Annex III, § 6.
[72] AI Act, supra note 1, Annex III, § 8.
[73] AI Act, supra note 1, arts. 8-15.

obligations resonate directly with the fiduciary duties of directors under Delaware law. The AI Act's ex ante requirements for risk management, data governance, and human oversight can be analogized to *Caremark* duties of oversight:[74] directors must ensure that adequate reporting systems exist to monitor AI-related risks that are mission critical to the firm's operations. A failure to implement or monitor such systems could expose boards not only to European regulatory penalties but also to derivative litigation in Delaware courts, where plaintiffs may argue that directors consciously disregarded red flags concerning AI compliance. In this respect, the AI Act operationalizes duties that closely parallel the oversight obligations articulated in *In re Caremark International Inc. Derivative Litigation*[75] and its progeny, including *Marchand v. Barnhill* and *Boeing Co. Derivative Litigation*.[76] Under Delaware law, directors are expected not only to implement reporting systems but also to ensure those systems are adequate to capture mission-critical risks. Courts have emphasized that a failure to establish or monitor such systems amounts to a breach of the duty of loyalty, particularly when the underlying risk is central to the company's business model. AI governance, when viewed through this lens, is not merely a European regulatory novelty but a transatlantic benchmark: the Act identifies AI compliance as a risk of such magnitude that it must be subject to continuous board-level oversight. Consequently, the absence of adequate AI risk monitoring may expose directors and officers to derivative suits in U.S. courts, with plaintiffs plausibly alleging that AI constitutes a "mission-critical" compliance domain under Caremark.

While at first glance the secretary's role in AI oversight may resemble familiar compliance functions—ensuring board processes reflect tax, accounting, or securities law obligations—the AI Act introduces a qualitative difference. Traditional compliance domains generally impose ex post reporting or financial control duties grounded in codified statutory requirements. By contrast, AI

[74] *In re Caremark International Inc. Derivative Litigation*, 698 A.2d 959 (Del. Ch. 1996).
[75] *In re Caremark* supra note 74.
[76] *See Marchand v. Barnhill*, 212 A.3d 805 (Del. 2019) and *In re the Boeing Co. Derivative Litig.*, No. 2019-0907 (Del. Ch. Sept 7, 2021).

governance entails ex ante integration of risk management, transparency, and human oversight mechanisms into the very architecture of corporate decision-making. The board secretary is not merely checking compliance boxes but facilitating the translation of open-textured regulatory standards (e.g., "adequate risk management," "sufficient human oversight") into ongoing governance practices. In this sense, AI obligations operate less as discrete statutory mandates and more as continuous governance functions—closer to fiduciary oversight than to compartmentalized compliance. The secretary's responsibility thus occupies a hybrid normative space: analogous in form to other compliance domains, yet distinct in substance because it requires embedding evolving regulatory expectations into the board's deliberative and monitoring routines.

Additionally, given the broad scope of prohibited practices,[77] corporate policies must incorporate strict due diligence mechanisms to prevent inadvertent violations, particularly where AI-driven analytics, customer segmentation, and risk assessments are concerned.

From a governance perspective, as a deployer, a listed company is required to ensure that high-risk AI systems undergo continuous monitoring, conformity assessments, and logging of AI decision-making processes.[78] Moreover, AI impact assessments, analogous to Data Protection Impact

[77] AI Act, supra note 1, art. 5.

[78] These topics are covered in several articles: (i) continuous monitoring (Article 72 AI Act outlines the requirements for post-market monitoring by providers of high-risk AI systems. Providers must establish and document a post-market monitoring system that actively and systematically collects, documents, and analyses relevant data on the performance of high-risk AI systems throughout their lifetime); (ii) conformity assessments (Article 43 AI Act specifies the conformity assessment procedures for high-risk AI systems. Providers must ensure that their high-risk AI systems undergo the relevant conformity assessment procedure prior to being placed on the market or put into service. This includes either internal control or assessment involving a notified body, depending on the availability and application of harmonized standards or common specifications); (iii) logging of AI decision-making processes (Article 12 AI Act mandates that high-risk AI systems must technically allow for the automatic recording of events (logs) over the lifetime of the system. Logging capabilities must enable the recording of events relevant for identifying situations that may result in the high-risk AI system presenting a risk, facilitating post-market monitoring, and monitoring the operation of high-risk AI systems); (iv) obligations of deployers (Article 26 AI Act outlines the obligations of deployers of high-risk AI systems. Deployers must take appropriate technical and organizational measures to ensure they use such systems in accordance with the instructions for use accompanying the systems. Deployers are also required to monitor the operation of the high-risk AI system based on the instructions for use and inform providers if the use of the system may result in presenting a risk. Additionally, deployers must keep the logs automatically generated by the high-risk AI system for a period appropriate to the intended purpose of the system). These articles collectively impose specific obligations on AI providers and deployers to ensure the continuous monitoring, conformity assessments, and logging of AI decision-making processes for high-risk AI systems.

Assessments (DPIAs) under the GDPR, must be conducted where AI usage could affect individual rights.[79] The secretary of the board of directors, as the custodian of corporate governance and compliance frameworks, must integrate AI-related compliance within board discussions, ensuring that AI risk management is embedded in corporate policies, internal controls, and audit processes. Lastly, the extraterritorial scope entails that board secretaries of multinational corporations must coordinate governance and compliance strategies across jurisdictions, ensuring that AI governance standards applied at global headquarters are compatible with EU expectations. In practice, this includes aligning internal policies to accommodate EU-specific conformity assessments, even when development or deployment occurs outside the EU.[80]

B. Operational Compliance and Board Responsibilities

The AI Act mandates a robust internal compliance structure for AI governance, requiring a risk management system that continuously evaluates and mitigates risks arising from AI deployment.[81] So the secretary of the board of directors must ensure that AI governance is formally integrated into the company's Enterprise Risk Management (ERM) framework, involving[82]:

1. Regular AI impact assessments to document and assess AI-related risks and ensure compliance with fundamental rights safeguards.[83]
2. AI conformity assessments and technical documentation obligations,[84] ensuring that AI systems used within the company meet regulatory requirements before deployment.

---

[79] Marija Boban, *GDPR and Data Protection Impact Assessment (DPIA),* in ECONOMIC AND SOCIAL DEVELOPMENT: BOOK OF PROCEEDINGS 215 (2020); IT GOVERNANCE PUBLISHING (ITGP), EU GENERAL DATA PROTECTION REGULATION (GDPR): AN IMPLEMENTATION AND COMPLIANCE GUIDE (2017); Nathalie A. Smuha, *The Paramountcy of Data Protection Law in the Age of AI (Acts),* supra note 34.

[80] For example, a U.S.-based technology firm deploying an AI-powered credit risk model through a European subsidiary must ensure that the system complies with arts. 9–15 of the AI Act, even if model training occurred entirely outside the EU. The secretary of the board must coordinate with compliance officers in both regions to ensure AI logs, risk assessments, and human oversight procedures are harmonised and accessible to EU regulators upon request.

[81] AI Act, supra note 1, art. 9.

[82] Schuett, *Risk Management in the Artificial Intelligence Act*, supra note 8.

[83] AI Act, supra note 1, art. 27.

[84] AI Act, supra note 1, art. 11.

3. Robust logging and transparency measures,[85] facilitating oversight by both internal auditors and external regulators.
4. Human oversight mechanisms,[86] ensuring that AI decisions, particularly those affecting employees, customers, or investors, are subject to meaningful human review to prevent undue reliance on algorithmic decision-making[87].

For multinationals operating across regions, these responsibilities pose additional challenges. Non-EU entities must integrate AI risk management structures that are interoperable with EU obligations, requiring board secretaries to work across legal, IT, and compliance teams located in different jurisdictions. For instance, AI systems developed in the U.S. but deployed in Europe for HR screening or financial scoring must undergo EU-prescribed conformity and transparency reviews. Ensuring that AI logs, documentation, and oversight mechanisms are available for EU regulators—even if the systems are hosted or managed abroad—requires proactive cross-border compliance infrastructure.

Furthermore, the AI Act requires deployers of high-risk AI systems to report any serious incidents or malfunctions that could pose risks to health, safety, or fundamental rights to relevant market surveillance authorities.[88] The secretary of the board of directors must ensure that internal reporting channels are established for such obligations, coordinating with legal, compliance, and IT security teams to facilitate prompt disclosures and prevent regulatory breaches.

C. AI and Corporate Disclosure Requirements

National authorities are empowered to also oversee compliance with AI-related obligations.[89] This aligns with existing EU disclosure frameworks such as:

[85] AI Act, supra note 1, arts. 12-13.
[86] AI Act, supra note 1, art. 14.
[87] Fink, *Human Oversight under Article 14 of the EU AI Act*, supra note 33.
[88] AI Act, supra note 1, art. 20.
[89] AI Act, supra note 1, art. 74.

- The Market Abuse Regulation (MAR),[90] which could apply where AI-driven trading or risk assessment mechanisms influence financial market behaviours[91].
- The Corporate Sustainability Reporting Directive (CSRD),[92] which mandates AI-related disclosures in environmental, social, and governance (ESG) reports.
- The Digital Operational Resilience Act (DORA),[93] which imposes cybersecurity and resilience requirements for AI-driven financial services.

As a result, the secretary of the board of directors must ensure that AI risk disclosures are accurately reported in annual reports, investor briefings, and sustainability disclosures, ensuring compliance with both financial and AI-specific regulatory frameworks.

Cross-border compliance is particularly complex in the context of disclosure obligations. Non-EU issuers listed on EU markets or whose AI systems affect EU-based consumers must ensure that their disclosures under frameworks like MAR or CSRD reflect AI-related risks, irrespective of their operational base. This includes coordinating ESG and AI disclosures to meet the expectations of both EU and home-country regulators, necessitating transnational internal reporting and legal review processes.

D. Best Practices

The AI Act necessitates not only formal compliance but a proactive and structured approach to AI governance at the board level. The secretary of the board of directors emerges as the institutional bridge between regulatory mandates, corporate policies, and board oversight. The

[90] Regulation (EU) No. 596/2014 of the European Parliament and of the Council of 16 April 2014 on market abuse (Market Abuse Regulation), 2014 O.J. (L 173) 1 (EU).

[91] Azzutti, *AI Governance in Algorithmic Trading: Some Regulatory Insights from the EU AI Act*, supra note 17.

[92] Directive (EU) 2022/2464 of the European Parliament and of the Council of 14 December 2022 amending Regulation (EU) No. 537/2014, Directive 2004/109/EC, Directive 2006/43/EC and Directive 2013/34/EU, as regards corporate sustainability reporting, 2022 O.J. (L 322) 15 (EU).

[93] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector, 2022 O.J. (L 333) 1.

practices outlined below are grounded in specific provisions of the AI Act (notably Articles 9–15 on risk management, human oversight, transparency, and technical documentation, and Articles 62–64 on reporting obligations), in EU governance frameworks such as the CSRD, the DORA, and the MAR, as well as in comparative corporate law doctrines including the Caremark line of oversight cases in Delaware jurisprudence and the Corporate Governance Codes. Each "best practice" translates these requirements into concrete tasks the secretary can implement:

1. Embed AI compliance into governance structures. In line with Articles 9–15 AI Act (risk management, transparency, and oversight) and by analogy with board-level duties under the Corporate Governance Codes and Delaware Caremark oversight jurisprudence, the secretary should ensure that AI-related risks are placed on standing board agendas and integrated into the Enterprise Risk Management framework. This can be operationalised by scheduling quarterly board briefings on AI risks, coordinating training sessions for directors, and ensuring that audit and risk committees explicitly review AI conformity assessments as part of their mandate.
2. Facilitate AI risk reporting and oversight. The secretary must design processes that enable transparent and timely reporting of AI risks to the board. This includes coordinating conformity assessments for high-risk AI systems, ensuring that management reports on AI deployments contain sufficient detail, and establishing escalation protocols for AI-related incidents. Rigorous scrutiny of such reports helps directors fulfil their fiduciary duties of oversight and loyalty.
3. Align AI disclosures with financial and ESG reporting requirements. Given the convergence of AI regulation with sustainability and market disclosure regimes, the secretary plays a critical role in ensuring coherence between AI-related disclosures and broader corporate reporting. This means embedding AI governance into annual reports, investor presentations, and ESG

disclosures, highlighting both compliance efforts and ethical safeguards. Properly aligned disclosures can enhance investor confidence and reduce litigation risk.

4. Develop and coordinate internal AI compliance frameworks. Beyond documentation, this involves operationalizing mechanisms such as AI impact assessments (akin to GDPR's Data Protection Impact Assessments), establishing human oversight protocols to prevent undue reliance on algorithmic outputs, and ensuring that regulatory reporting channels are reliable and auditable. The secretary must ensure that these frameworks are formally adopted by the board and periodically reviewed for adequacy.
5. Monitor evolving AI regulations and liaise with regulators. Because the AI Act is an evolving framework, the secretary must keep the board apprised of legislative amendments, delegated acts, and interpretive guidance from EU institutions and national supervisory authorities. Maintaining open communication with regulators not only ensures compliance but positions the company as a responsible participant in regulatory dialogues, reducing enforcement risk and reputational exposure.
6. Establish cross-border AI compliance protocols. For multinational companies, the extraterritorial reach of the AI Act requires uniform governance mechanisms across jurisdictions. The secretary must coordinate the standardization of AI-related documentation, audit trails, and incident reporting across subsidiaries, ensuring consistency with EU requirements while accommodating local legal norms. This may involve developing global AI compliance playbooks and ensuring that regional entities report into a central governance hub.

As AI technologies evolve and regulatory frameworks mature, listed companies must adopt a posture of continuous vigilance. The board secretary, by embedding AI compliance into governance routines and aligning legal obligations with ethical business conduct, ensures that the corporation not only avoids regulatory penalties but also builds long-term trust with investors, employees, and society at

large. In this sense, the secretary's role transcends procedural duties: they become a guardian of responsible AI governance within the corporate architecture.

V. Compliance Officers' Obligations Under the AI Act

Corporate compliance officers have long been pivotal in ensuring organisations adhere to legal, regulatory, and ethical standards. Their core responsibilities have historically encompassed corporate governance, financial compliance, data protection, anti-money laundering (AML), and consumer protection.[94] Key duties include establishing internal policies aligned with frameworks like GDPR and Markets in Financial Instruments Directive (MiFID II), conducting audits, implementing training programmes, and fostering organisational integrity and accountability.

Compliance officers also act as liaisons with regulatory bodies, overseeing due diligence to mitigate fraud risks and monitoring evolving legal requirements.[95] In highly regulated sectors like finance and healthcare, they safeguard against reputational damage by implementing robust controls, ultimately becoming a key competitive advantage for their own companies.[96] Notably, the AI Act does not explicitly identify compliance officers as regulated entities. Their obligations are therefore derivative: statutory duties under the Act attach to providers, deployers, importers, and distributors, yet within the corporate governance structure these duties must be translated into role-specific responsibilities. The compliance officer becomes the natural institutional conduit for this internalisation. Their mandate thus arises not directly from the AI Act, but from the transposition of statutory requirements into internal compliance systems—a process already familiar from data protection and financial regulation.

---

[94] https://www.innreg.com/blog/chief-compliance-officer-definition-and-responsibilities.

[95] *See also* Edward T. Dartley, *The Combined Role of General Counsel and the Chief Compliance Officer—Opportunities and Challenges*, PRAC. COMPLIANCE & RISK MGMT. FOR THE SEC INDUSTRY (May-June 2014), at 21, 21–23.

[96] Robert C. Bird & Stephen K. Park, *Turning Corporate Compliance into Competitive Advantage,* 19 U. PA. J. BUS. L. 286 (2017).

Although these responsibilities have remained largely consistent across industries, the rapid evolution of digital technologies has introduced new compliance challenges. The emergence of AI-driven decision-making processes and algorithmic transparency considerations surrounding automated systems has necessitated an expansion of compliance officers' duties. Their responsibilities span multiple dimensions, including governance, risk assessment, documentation, ongoing monitoring, and reporting.

First and foremost, compliance officers must ensure that AI systems falling within the high-risk category comply with the stringent requirements set out in Chapter III, Section 2, of the AI Act. This includes overseeing the implementation of a comprehensive risk management system,[97] which requires continuous identification, analysis, and mitigation of potential risks associated with the deployment and operation of AI. They must ensure that such risk assessments are conducted prior to market placement and updated regularly throughout the lifecycle of the AI system to account for evolving threats[98].

A critical responsibility of compliance officers is to guarantee the accuracy and completeness of technical documentation.[99] They must ensure that such documentation is prepared before an AI system or model is placed on the market and remains readily available for at least ten years post-deployment. The documentation must include detailed descriptions of the AI model's development process, training data sets, testing methodologies, performance metrics, and risk mitigation strategies, ensuring full traceability and transparency. Compliance officers are also responsible for ensuring that AI providers and deployers implement robust data governance frameworks,[100] which require that training, validation, and testing datasets are subject to rigorous quality control measures, minimising biases and ensuring compliance with data protection laws such as the GDPR.

---

[97] AI Act, supra note 1, art. 9.

[98] Schuett, *Risk Management in the Artificial Intelligence Act*, supra note 8.

[99] AI Act, supra note 1, arts. 11 (further detailed in Annex VI, concerning high-risk AI systems) and 53 (further detailed in Annex XI, concerning general-purpose AI models).

[100] AI Act, supra note 1, art. 10.

Additionally, compliance officers must facilitate and oversee post-market monitoring obligations in a manner that is proportionate to the nature of the AI technologies and the risks of the high-risk AI system,[101] ensuring that AI systems continue to meet regulatory requirements and operate within acceptable risk parameters after deployment. This involves the collection and analysis of real-world performance data, identification of potential failures or biases,[102] and prompt implementation of corrective actions. Moreover, compliance officers are tasked with ensuring that all AI providers fulfil their obligations, including specific requirements for importers and distributors regarding compliance verification, market surveillance cooperation, and the prevention of non-compliant AI products from entering the EU market.[103] They must establish clear internal policies to ensure that all AI-related activities align with these regulatory obligations.

Furthermore, compliance officers are mandated to liaise with the AI Office and relevant national competent authorities,[104] ensuring that all required documentation and compliance reports are submitted in a timely manner. They must also coordinate internal audits and facilitate external conformity assessments where required, particularly in cases where AI systems undergo third-party evaluation.[105] In instances where an AI system presents systemic risks, compliance officers are

[101] AI Act, supra note 1, art. 72.

[102] This obligation shall not cover sensitive operational data of deployers which are law-enforcement authorities.

[103] AI Act, supra note 1, arts. 23-26 (establishing a comprehensive framework for ensuring AI systems comply with EU regulations. Importer Obligations under Article 23 require verification that AI systems conform to regulations before market entry. This includes ensuring proper conformity assessments, documentation, and CE marking are in place. Importers must maintain documentation for 10 years and cooperate with authorities when requested. Distributor Obligations outlined in Article 24 mandate verification of CE marking and EU declaration of conformity. Distributors must ensure provider and importer compliance, maintain proper storage and transport conditions, take corrective actions for non-compliant systems, and cooperate with authorities); art. 25 (establishing Third-Party Provider Status, whereby any party that puts their name on a high-risk AI system, makes substantial modifications, or changes its purpose becomes a "provider." These new providers must ensure compliance with conformity assessments and cooperate with original providers by sharing information and providing technical assistance); art. 26 (requiring implementation of measures to ensure systems are used according to instructions. Deployers must assign qualified human oversight, ensure input data is relevant and representative, inform people when they're subject to high-risk AI systems, and cooperate with authorities); art. 74 (requiring to apply existing market surveillance regulations to AI systems. Authorities have access to documentation and datasets, may request source code access under certain conditions, and coordinate with other authorities to conduct joint compliance activities).

[104] AI Act, supra note 1, art. 54.

[105] AI Act, supra note 1, art. 43.

obligated to oversee the implementation of adversarial testing and cybersecurity measures,[106] ensuring resilience against vulnerabilities, data breaches, and potential misuse. The AI Act also places significant emphasis on the obligation to report serious incidents or non-compliance,[107] requiring compliance officers to establish internal reporting mechanisms and notify regulatory authorities without undue delay in the event of significant risks to health, safety, or fundamental rights.

Finally, compliance officers must ensure that high-risk AI systems comply with CE marking and the EU declaration of conformity,[108] which serve as legal attestations of compliance. Non-compliance with any of these obligations can result in substantial enforcement actions, including financial penalties.[109] Given the extensive scope of responsibilities under the AI Act, compliance officers must integrate AI-specific compliance frameworks into their organisations, ensuring proactive risk management, continuous regulatory adherence, and effective coordination with supervisory authorities to uphold the EU's commitment to safe and trustworthy AI.

A. Managing the Unmanageable: Practical Challenges in Regulatory Oversight

(i) Risk Management, Documentation and Logs

One of the most complex challenges for a compliance officer under the AI Act lies in the practical enforcement of risk management and ongoing monitoring obligations for high-risk AI systems, particularly in dynamic operational environments where AI-driven models continuously evolve. Article 9 mandates that risk management be a continuous, iterative process encompassing the entire lifecycle of an AI system. However, this requirement presupposes that risks can be systematically identified, assessed, and mitigated in advance, whereas in reality, many AI systems—particularly those leveraging machine learning, neural networks, and adaptive algorithms—

[106] AI Act, supra note 1, art. 55.
[107] AI Act, supra note 1, art. 83.
[108] AI Act, supra note 1, arts. 47-48.
[109] AI Act, supra note 1, art. 99.

demonstrate emergent behaviors that are not necessarily foreseeable at the time of deployment. The regulatory framework assumes a level of control and predictability that, in many instances, does not align with the way AI systems function in practice. A compliance officer, therefore, faces the formidable task of proving to regulatory authorities that risk management protocols are not only theoretically robust but also sufficiently adaptable to address risks that may materialize in ways that were not initially envisaged. This challenge becomes even more pronounced in the case of AI systems that rely on dynamic real-time data inputs, where external factors—such as market fluctuations, user interactions, or adversarial interference—can significantly alter system behavior in ways that were not anticipated in the initial compliance assessments. This becomes particularly problematic in cross-border contexts, where compliance teams in non-EU jurisdictions may have to align domestic documentation norms with EU requirements despite differences in legal definitions, language standards, or access to regulators.

The difficulties inherent in this obligation are further exacerbated by the requirement to maintain comprehensive technical documentation for a minimum of ten years post-deployment. This introduces significant operational and liability-related concerns, particularly for organizations deploying AI models that undergo frequent updates or iterative improvements. AI development is inherently fluid, with models often being retrained, fine-tuned, or even entirely replaced based on evolving datasets and business requirements. In such a scenario, ensuring that documentation remains accurate and reflective of the model in use at any given point in time becomes an immense challenge. A compliance officer must contend with the risk that documentation may become outdated, leading to discrepancies between recorded compliance measures and the actual state of the deployed AI system. More critically, regulatory scrutiny may retrospectively assess an organization's compliance based on past iterations of an AI model that no longer exist in their original form but remain documented. This issue is particularly acute in sectors such as finance, insurance, and healthcare, where even minor deviations in model behavior can have significant legal, financial, and

ethical implications. In these cases, compliance officers may find themselves in the precarious position of justifying past decisions based on records that no longer correspond to the actual AI system in operation, potentially exposing their organizations to legal liabilities or compliance risks.

(ii) Adversarial Testing and Evaluations

A particularly thorny issue arises in the context of adversarial testing and cybersecurity obligations under Article 15. The AI Act mandates that providers of high-risk AI systems conduct systematic evaluations to identify vulnerabilities, simulate attacks, and implement resilience measures. This requirement is grounded in a legitimate concern over AI system security, but it places compliance officers in a difficult position due to the inherent paradox of adversarial testing: the very act of probing an AI system for weaknesses can, in some cases, inadvertently introduce new ones. For instance, sophisticated AI models—such as large-scale language models or facial recognition systems—may be susceptible to prompt injection attacks, data poisoning, or model inversion techniques, where adversarial actors extract proprietary training data or manipulate outputs through carefully crafted inputs. If compliance officers mandate rigorous adversarial testing, they risk inadvertently revealing system weaknesses that could be exploited if not properly contained. Conversely, if they adopt a more conservative approach, they may fail to meet the stringent expectations set by regulatory authorities regarding risk mitigation. Furthermore, adversarial threats are not static; they evolve over time as external actors refine their attack methods. This means that compliance assessments that are valid at one point may quickly become obsolete, raising the question of whether regulatory expectations regarding adversarial robustness are truly reconcilable with the fluid and reactive nature of cybersecurity threats in AI applications[110].

[110] On cyber threats, *see* IE, DEMOCRACY RELOADED: AI TO PROTECT AND PROMOTE DEMOCRATIC GOVERNANCE (2025), supra note 5.

(iii) Explainability and Transparency

Another problematic area concerns the obligations related to AI explainability and transparency, particularly when requiring that high-risk AI systems be designed in a way that allows human users to interpret and understand their outputs.[111] This requirement is particularly challenging for compliance officers overseeing AI systems that rely on deep learning models, which are often inherently opaque due to their complex, multi-layered decision-making processes. The Act does not provide clear guidelines on how explainability should be measured or demonstrated in a way that satisfies regulatory expectations. Compliance officers may, therefore, find themselves in a position where they must enforce explainability requirements without a universally accepted framework for doing so. This issue is especially critical in high-stakes decision-making scenarios—such as AI-driven credit scoring, hiring processes, or judicial risk assessments—where affected individuals have a right to contest AI-generated decisions. If the organization fails to provide a satisfactory explanation for a given decision, it risks facing legal challenges, regulatory penalties, or reputational damage. The compliance officer, in this scenario, is required to strike a delicate balance between technical feasibility and regulatory expectations, ensuring that AI systems are not only compliant but also interpretable by non-technical stakeholders, a task that is far easier said than done. Yet it is critical to acknowledge that the requirement for explainability collides with a stubborn technical reality: all advanced AI systems function as black boxes. Complete decision-level explainability is, in most cases, impossible. This impossibility has been underscored across the literature. Some authors argue that explainability tools rarely fulfill the underlying legal purposes of reason-giving, such as respecting autonomy or due process, and instead serve mainly to strengthen institutional authority (by creating the appearance of accountability) without providing substantive transparency.[112] Other authors likewise caution that not all explanations serve the same audience—an explanation that satisfies a data scientist may be

[111] AI Act, supra note 1, art. 13.

[112] Hofit Wasserman-Rozen, Ran Gilad-Bachrach & Niva Elkin-Koren, *Lost in Translation: The Limits of Explainability in AI*, 42 CARDOZO ARTS & ENT. L.J. 391 (2024).

meaningless to a consumer or a regulator—and propose a 'Legal-XAI' framework precisely to bridge this gap.[113] And the illusion of explainability and risks of "fairwashing" are genuine dangers: post-hoc techniques like SHAP or LIME often provide only an appearance of transparency rather than true insight.[114] For compliance officers, the regulatory mandate is thus not to conjure impossible certainty but to demonstrate procedural accountability—through documentation, governance mechanisms, and human oversight—that shows regulators the organization has taken all reasonable steps to mitigate opacity.

(iv) Incident Reporting

Finally, the requirement to report serious incidents[115] or non-compliance to regulatory authorities places compliance officers in a particularly precarious position, especially within multinational corporations where AI systems may be deployed across multiple jurisdictions with varying regulatory requirements. The AI Act does not provide a precise definition of what constitutes a "serious incident," leaving room for interpretation.[116] Compliance officers must, therefore, make judgment calls on whether an AI system's deviation from expected behavior meets the threshold for mandatory reporting. This can create significant internal friction, particularly in cases where reporting an issue could have severe financial or reputational consequences for the organization. For U.S. multinationals, the stakes also include litigation risk: an incident disclosed in Europe could trigger parallel shareholder lawsuits in U.S. courts, product liability claims if harm is linked to defective AI outputs, or even consumer class actions alleging algorithmic discrimination. This dynamic reinforces

---

[113] Aniket Kesari, Daniela Sele, Elliott Ash & Stefan Bechtold, *Explaining Explainable AI* (2025) (manuscript at 1), https://ssrn.com/abstract=4972085.

[114] Victor Hugo Pereira Melo & Weysller Matuzinhos de Moura, *Explainable Artificial Intelligence: A Literature Review* (2025) (manuscript at 1), https://ssrn.com/abstract=5338183.

[115] AI Act, supra note 1, art. 73.

[116] Ayça Atabey, Lachlan Urquhart & Burkhard Schafer, *Article 73. Reporting of Serious Incidents*, *in* THE EU ARTIFICIAL INTELLIGENCE (AI) ACT: A COMMENTARY 1051 (Nikolaus Forgó, Ceyhun Necati Pehlivan & Peggy Valcke eds., 2024).

a familiar pattern in U.S. jurisprudence: foreign regulatory disclosures often migrate into the U.S. courtroom as predicates for domestic liability. In *Morrison v. National Australia Bank*,[117] the Supreme Court limited the extraterritorial reach of U.S. securities laws, yet subsequent lower court decisions have shown that foreign regulatory events—whether fines, investigations, or mandatory disclosures—can serve as factual triggers for Rule 10b-5 claims when they reveal material risks to U.S. investors. More recently, securities class actions arising from GDPR breaches illustrate the same trajectory: EU regulatory obligations generate disclosure events that U.S. plaintiffs reframe as omissions or misstatements under federal securities law. Against this backdrop, the AI Act's regime of prompt incident reporting, risk assessments, and conformity disclosures effectively supplies ready-made material for parallel litigation in American courts. A malfunctioning AI system disclosed to EU regulators may simultaneously constitute a "red flag" for Caremark oversight claims, a material omission under Rule 10b-5, or even a basis for product liability under U.S. tort law. In this sense, the Act operates as a transatlantic compliance catalyst: what begins as a European reporting obligation can end as a U.S. litigation exposure.

Internal stakeholders, such as legal teams or executive leadership, may exert pressure to minimize or delay reporting in order to mitigate potential fallout. In such scenarios, the compliance officer must navigate a politically charged environment, balancing regulatory obligations with corporate interests. Furthermore, in cases where an AI system is deployed across multiple jurisdictions, compliance officers must account for differing legal interpretations of what constitutes non-compliance, leading to further complexity in determining the appropriate course of action.

In short, a compliance officer's job under the AI Act goes far beyond box-checking. It means navigating a complex—and sometimes contradictory—regulatory landscape. The Act's requirements,

[117] *Morrison v. National Australia Bank*, 561 US 247 (2010).

while well-intentioned, impose obligations that, in practice, may be difficult—if not impossible—to fulfill with absolute certainty, particularly in light of the dynamic, evolving nature of AI technology. Meeting these challenges requires more than generic vigilance. Compliance officers must translate statutory obligations into enforceable governance infrastructures, negotiate vendor contracts that guarantee transparency, adapt explainability mandates into auditable legal standards, and anticipate the extraterritorial consequences of EU incident reporting. Their role is therefore constitutive: they are the actors through whom the AI Act's abstract duties crystallise into corporate responsibility and, ultimately, into personal accountability.

(v) Third Parties and Supply Chain Challenges

Another deeply challenging scenario for a compliance officer under the AI Act emerges in the context of third-party AI system integration and the associated supply chain liability. Many organisations, particularly those in finance, healthcare, and critical infrastructure, do not develop AI systems entirely in-house but instead integrate third-party AI components or rely on external providers for model training, deployment, and maintenance. Compliance officers must ensure that AI importers, distributors, and deployers meet the regulatory obligations applicable to high-risk AI systems. However, the AI Act introduces a fundamental asymmetry of control versus responsibility: while compliance officers are legally accountable for ensuring that AI systems used by their organisations comply with regulatory requirements, they often lack direct access to—or full control over—the underlying AI technology, which may be proprietary or managed by external vendors. This creates a structural blind spot, where compliance officers are expected to certify compliance without being able to independently verify key technical parameters.

For instance, consider a financial institution that deploys a third-party AI-powered fraud detection system. Under the AI Act, the compliance officer must ensure that the system adheres to the strict risk management, transparency, and documentation requirements set out in Articles 9-13. If a company uses an AI model provided by an external vendor, but the vendor refuses to disclose key

details about the model—such as its architecture, training data, and algorithmic logic—because they are considered proprietary trade secrets, the company's compliance officer faces a Catch-22 situation. In other words, the compliance officer is legally required under the AI Act to ensure transparency, assess risks, and verify compliance with regulations, but they lack access to the necessary information to do so. This creates a paradox: they are required to guarantee compliance, but they cannot access or audit the critical components necessary to make such a determination. For U.S. firms, the tension is even sharper: while EU regulators demand transparency and documentation ex ante, American law often protects proprietary AI models and data under trade secret or IP doctrines. The result is a structural clash between two regulatory cultures. By treating compliance officers as guarantors of AI transparency, the AI Act implicitly elevates their role to that of fiduciary gatekeepers. This resonates with U.S. debates on whether compliance officers should bear personal liability for systemic failures. The functional equivalence between European compliance duties and American officer responsibilities suggests a path for U.S. courts to analogize EU standards in defining the contours of officer oversight liability.[118]

This issue is exacerbated by the fact that many AI vendors operate under licensing agreements that explicitly prohibit reverse-engineering or detailed scrutiny of the AI model's internal workings. Thus, the compliance officer must either rely on contractual assurances—which may be insufficient in the eyes of regulators—or push for greater transparency, which vendors may resist due to intellectual property concerns.

Furthermore, the problem becomes even more acute in cases where AI models are dynamically updated via cloud-based APIs or external machine learning platforms. Many AI systems today operate on continuous learning architectures, where model parameters are updated in real-time based on new data inputs. This means that even if an AI system was fully compliant at the time of initial

[118] *See* Sean J. Griffith, *Corporate Governance in an Era of Compliance*, 57 WM. & MARY L. REV. 2075, 2077–96 (2016) (arguing that compliance functions do not originate in boards or corporate law but are imposed exogenously by enforcement agencies, thereby reshaping internal governance).

deployment, its behaviour could drift over time in ways that introduce biases, inaccuracies, or non-compliant decision-making processes. The AI Act mandates ongoing post-market monitoring, requiring compliance officers to ensure that the AI system continues to meet regulatory requirements even as it evolves. If the updates occur outside the compliance officer's direct oversight, they may struggle to identify when a previously compliant system begins to exhibit regulatory breaches—for example, if an AI-driven credit scoring system starts to disproportionately reject applicants from certain demographic groups due to subtle shifts in training data. The compliance officer, therefore, faces an insurmountable oversight challenge: they must ensure compliance over time, yet the system itself remains a moving target.

Another problematic aspect of third-party AI system integration arises in the context of cross-border regulatory conflicts. For US-based firms, this often means reconciling EU demands for transparency and documentation with US legal norms on trade secrets, liability, and IP protection. A compliance officer at a US bank or healthcare provider may find themselves in the middle of these tensions.

In such cases, the compliance officer finds themselves in an untenable position: either they insist on full compliance, potentially losing access to critical AI providers unwilling to meet EU transparency standards, or they accept partial compliance taking on the legal and regulatory risks associated with any non-conforming elements. This dilemma is particularly severe in industries where access to advanced AI technology is a competitive necessity, such as algorithmic trading, medical diagnostics, and cybersecurity[119]. The compliance officer must negotiate the competing pressures of regulatory adherence, business continuity, and technological competitiveness, all while facing potential enforcement actions if regulators determine that their organisation has failed to ensure full compliance. In such scenarios, liability risks are not confined to the organisation: under national corporate governance doctrines, compliance officers themselves may face claims of breach of duty if

[119] Astuti, *AI Governance in Algorithmic Trading: Some Regulatory Insights from the EU AI Act*, supra note 17.

they fail to implement adequate monitoring systems or contractual safeguards. This illustrates the dual exposure of the role: while the AI Act 'overlooks' them textually, domestic legal frameworks ensure that they cannot escape scrutiny.

A further complication arises when third-party AI systems operate as black boxes, making it difficult to assess compliance with explainability and fairness requirements. Many modern AI models, particularly deep learning architectures, are highly complex and lack intuitive interpretability. Regulators may demand that compliance officers demonstrate how a high-risk AI system reaches its decisions, insofar as the AI Act deployers and providers to ensure traceability, transparency, and human oversight, and empowers national market surveillance authorities to require disclosure of technical documentation and conformity evidence. In practice, this means regulators can request explainability documentation or post-hoc interpretability reports as part of their supervisory powers. The compliance officer must then decide whether to push for alternative AI solutions that offer greater interpretability (potentially at the cost of performance) or rely on post-hoc explainability techniques such as SHAP (Shapley Additive Explanations) or LIME (Local Interpretable Model-agnostic Explanations), which are not always accepted by regulators as sufficient proof of transparency. Compliance officers could be held personally accountable for failing to ensure adherence to AI standards—most directly through administrative enforcement by national supervisory authorities under Title VII (fines and corrective measures analogous to those under the GDPR). While the AI Act itself does not create individual liability in civil or criminal law, personal accountability may arise indirectly: in the EU, company law and employment law can impose disciplinary and contractual consequences on designated compliance officers; in the US, courts have increasingly analogised compliance functions to fiduciary gatekeeping roles, exposing officers to derivative suits or regulatory sanction where systemic compliance failures occur.

Finally, the compliance officer must also manage liability risks associated with AI system failures. Serious incidents involving AI systems—such as erroneous medical diagnoses, discriminatory hiring

decisions, or financial miscalculations—must be reported to regulatory authorities. However, determining responsibility in an AI supply chain involving multiple stakeholders is inherently ambiguous. If an AI system supplied by a third party produces a non-compliant outcome, is the provider responsible for failing to meet technical standards, or is the deploying organisation accountable for failing to conduct proper oversight? This ambiguity is particularly dangerous in high-risk sectors where AI failures can lead to real-world harm, such as aviation, healthcare, or criminal justice. Compliance officers must establish clear contractual liability frameworks, but given that many AI vendors operate under limitation-of-liability clauses, organisations deploying third-party AI may ultimately bear the regulatory burden, even if they had no direct control over the AI model's development.

All in all, the scenario of third-party AI integration and supply chain liability highlights the deep structural tensions within the AI Act's regulatory framework. Compliance officers are expected to guarantee compliance for AI systems they do not fully control, maintain transparency over models that operate as black boxes, enforce accountability across jurisdictions with conflicting legal frameworks, and monitor ongoing risks in AI systems that dynamically evolve over time. These challenges create a high-stakes, high-risk regulatory landscape, where compliance officers must constantly navigate competing pressures—ensuring full legal adherence without stifling innovation, enforcing regulatory standards without alienating key AI suppliers, and mitigating risks without assuming liabilities that cannot be reasonably managed. In doing so, the compliance officer's role ceases to be one of mere oversight and instead becomes a multidimensional strategic function, requiring deep expertise in law, technology, governance, and risk management—all while operating within an AI regulatory environment that is still evolving, and in many respects, inherently contradictory.

These cross-border conflicts—between the AI Act's transparency mandates and third-country IP, privacy, or trade laws—reveal the limits of unilateral regulation in a global market. As a result,

compliance officers must not only monitor internal systems but also manage extraterritorial exposure, translating EU regulatory expectations into enforceable, auditable processes across fragmented legal geographies.

B. Best Practices

Given the complexity of the regulatory landscape, a structured and proactive compliance approach is essential to mitigate legal, ethical, and operational risks associated with AI. Below are the best practices that corporate compliance officers should adopt, along with potential challenges and references to the relevant articles of the AI Act.

1. Engaging in Regulatory Dialogue and Industry Collaboration (including across jurisdictions): Given the AI Act's extraterritorial scope, compliance officers at multinational firms must monitor how national regulators in different jurisdictions interpret EU obligations and ensure that global vendors understand and accommodate European transparency and risk management requirements.
2. Establishing a Comprehensive AI Governance Framework: AI compliance should not be treated in isolation but as an integral component of overall corporate governance, aligning with regulatory, ethical, and ESG considerations. Many organisations lack a centralised AI governance framework, leading to fragmented compliance efforts across different departments. This can result in inconsistencies in AI oversight and difficulties in maintaining accountability.
3. Implementing a Dynamic Risk Management System: Compliance officers should ensure that risk management frameworks account for the full lifecycle of AI, from development to deployment and post-market monitoring. This includes:
    - Identifying risks related to bias, discrimination, fundamental rights violations, and cybersecurity vulnerabilities.

- Conducting periodic re-evaluations of risk exposure, particularly when AI systems undergo modifications or updates.
- Applying risk mitigation measures proportionate to the severity of potential harm.

A key difficulty is balancing risk mitigation with AI innovation. Overly restrictive compliance measures may stifle the organisation's ability to leverage AI's full potential, whereas insufficient oversight could expose the company to regulatory penalties and reputational damage.

4. Ensuring Rigorous Data Governance and Transparency: Compliance officers must ensure that all AI models are trained, validated, and tested using high-quality, representative, and unbiased datasets. Key actions include:
   - Implementing data quality controls to prevent discrimination and bias.[120]
   - Ensuring compliance with GDPR and other data protection laws when processing personal data for AI training.
   - Establishing documentation procedures to record data provenance, transformation processes, and usage policies.[121]

   AI systems relying on historical data may inadvertently replicate existing biases. For example, an AI-driven hiring tool trained on past recruitment data may reinforce discriminatory hiring patterns if not properly audited. Balancing dataset neutrality and AI efficiency remains a significant challenge.
5. Maintaining Comprehensive Technical Documentation and Traceability: Technical documentation is a crucial component of AI compliance, particularly for high-risk AI systems. Compliance officers should establish rigorous documentation protocols, ensuring that all AI systems adhere to the requirements set out in Article 53 and Annex XI. This includes:

[120] AI Act, supra note 1, art. 10.
[121] AI Act, supra note 1, art. 53.

- Maintaining detailed records of model development, datasets used, performance benchmarks, and changes made over time.
- Ensuring that documentation is accessible for regulatory audits and remains available for at least ten years after an AI system is placed on the market.
- Recording risk mitigation strategies and conformity assessments to demonstrate regulatory compliance.

Many organisations struggle with documentation standardisation, particularly in dynamic AI environments where models undergo frequent updates. Failure to maintain up-to-date records may result in non-compliance penalties and legal liability.

6. Strengthening Post-Market Monitoring and Incident Reporting Mechanisms: Once AI systems are deployed, compliance officers must oversee continuous monitoring processes to detect potential compliance failures or adverse effects on users. Key actions include:
   - Establishing post-market monitoring programmes[122] to collect real-world data on AI system performance.
   - Implementing early warning systems to detect algorithmic bias, inaccuracies, or security breaches.
   - Ensuring that any serious incidents or malfunctions are promptly reported to competent authorities.[123]

   The true challenge is that AI failures may not always be immediately apparent.
7. Conducting Regular Compliance Audits and Internal Reviews: AI compliance is an evolving discipline that requires periodic reassessment. Compliance officers should establish a structured audit process to:
   - Evaluate AI system performance against regulatory benchmarks.

[122] In line with the relevant provision (AI Act, supra note 1, art. 61).
[123] AI Act, supra note 1, Article 73.

- Identify and rectify non-conformities before they escalate into compliance breaches.
- Validate third-party AI providers and vendors to ensure their adherence to regulatory standards.

AI systems may develop unintended consequences over time, particularly in machine learning applications where models adapt autonomously. Regular audits must be robust enough to detect deviations before they lead to regulatory action.

8. Enhancing Staff Training and Organisational Awareness: AI compliance is not solely the responsibility of compliance officers—it requires engagement across all business units. Compliance teams should:
   - Provide AI ethics and compliance training to employees who interact with AI systems.
   - Educate senior management on regulatory obligations and the potential legal implications of AI misuse.
   - Develop guidelines for responsible AI deployment, ensuring that employees understand ethical considerations alongside regulatory requirements.

   Unfortunately, many organisations lack AI literacy among key personnel, which can lead to improper AI usage or inadvertent non-compliance. Training programmes must be comprehensive and tailored to different employee roles.
9. Engaging in Regulatory Dialogue and Industry Collaboration: AI regulation is evolving rapidly, and compliance officers must remain engaged with regulatory authorities and industry stakeholders to stay ahead of emerging legal developments. It is essential to:
   - Establish communication channels with the AI Office and national competent authorities.
   - Participate in industry working groups and regulatory consultations to provide input on AI governance frameworks.
   - Monitor legislative updates and adapt internal compliance strategies accordingly.

The AI regulatory landscape is still evolving, and organisations must be prepared to adapt their compliance frameworks as new legal interpretations and enforcement guidelines emerge. Overall, by implementing these best practices, corporate compliance officers can ensure that their organisations remain compliant with the AI Act while fostering ethical and responsible AI development. Given the complexity of AI governance, a proactive, risk-based approach is essential to navigate regulatory challenges, safeguard corporate integrity, and maintain public trust in AI-driven decision-making systems.

VI. In-House Counsels' Strategic Approach Under The AI Act

In-house (or general) corporate counsels, who already navigate a complex web of compliance requirements,[124] will also need to establish rigorous internal oversight mechanisms to guarantee adherence to the new AI regulations. From their viewpoint, the AI Act presents a multifaceted regulatory landscape that requires strict compliance mechanisms and risk assessments to avoid legal liabilities and potential sanctions.[125]

A significant aspect is related to the abovementioned classification of high-risk AI systems, including AI used in financial services, HR recruitment processes, risk assessment models, and consumer credit scoring—areas highly relevant to listed companies. The legal counsel must ensure that all high-risk AI systems undergo the required conformity assessment procedures before being deployed.

Additionally, companies leveraging AI for consumer analytics, workforce management, or automated decision-making must conduct algorithmic bias assessments and ensure compliance with GDPR.

---

[124] Robert C. Bird & Stephen Kim Park, *The Domains of Corporate Counsel in an Era of Compliance,* 53 AM. BUS. L.J. 203, 208-218 (2016).

[125] *See* HUNTON ANDREWS KURTH LLP, THE EU AI ACT GUIDE FOR IN-HOUSE LAWYERS (FEB. 2025), https://www.hunton.com/assets/htmldocuments/ai-act-guide.pdf; THE IMPACT AI WILL HAVE (AND IS HAVING) ON IN-HOUSE COUNSEL, https://www.alfainternational.com/publications_news/the-impact-ai-will-have-and-is-having-on-in-house-counsel/; THE EU ARTIFICIAL INTELLIGENCE ACT: WHAT IN-HOUSE COUNSEL NEED TO KNOW (MAR. 19, 2024), https://www.acc.com/resource-library/eu-artificial-intelligence-act-what-house-counsel-need-know?check_logged_in=1.

For listed companies, the AI Act introduces corporate governance obligations that necessitate board-level oversight on AI strategy. Companies deploying AI systems must ensure internal audit processes for AI risk management.[126] This requires the legal counsel to: (i) establish AI governance frameworks aligned with corporate compliance policies; (ii) advise the board of directors on AI risk exposure; (iii) implement contractual safeguards when engaging AI vendors; (iv) oversee regulatory reporting and risk disclosures.

In the event of AI-related harm or compliance failures, a company may face liability claims, particularly under the EU Product Liability Directive and emerging AI-specific liability regimes.

One of the most consequential aspects of the AI Act for corporate governance is the requirement for fundamental rights impact assessments (FRIA).[127] Any company deploying high-risk AI that could significantly affect individual rights, consumer protection, or employment decisions must conduct ex-ante legal evaluations to assess whether the system aligns with EU fundamental rights standards.[128] This demands a multidisciplinary legal and compliance approach, involving collaboration between corporate counsel, and data protection officers (DPOs) to ensure AI models comply with GDPR, the Digital Services Act,[129] and sector-specific regulations.

If needed, corporate counsel must proactively engage with national market surveillance authorities, ensuring that their organisation remains informed about evolving regulatory interpretations and adjusts internal compliance policies accordingly.

---

[126] AI Act, supra note 1, Article 17.

[127] AI Act, supra note 1, Article 27.

[128] On the critical role of high-risk AI on fundamental rights in the AI Act, *see* Fraser & Bello y Villarino, *Acceptable Risks in Europe's Proposed AI Act: Reasonableness and Other Principles for Deciding How Much Risk Management Is Enough,* supra note 25.

[129] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act), 2022 O.J. (L 277) 1.

The Act's post-market monitoring and reporting obligations[130] require companies to continuously evaluate the performance of AI systems, report serious incidents to regulators, and implement risk-mitigation mechanisms in case of unforeseen failures. This means that corporate legal teams must closely collaborate with IT, compliance, and internal audit teams to ensure AI-related risks are dynamically managed throughout the system's operational lifecycle.

A. Challenges and Legal Complexities for In-House Counsels

One of the most pressing concerns for in-house legal teams lies in the classification and management of high-risk AI systems. Counsels must navigate intricate requirements related to transparency, risk mitigation, human oversight, and post-market monitoring. This is especially problematic for multinational corporations operating across different regulatory jurisdictions, as compliance strategies must align both with EU law and the organisation's broader operational frameworks.

A particularly problematic scenario arises in the context of AI-driven recruitment and employee monitoring. The AI Act imposes stringent obligations on AI systems used for hiring, performance evaluation, and workplace surveillance. Employers leveraging AI for decision-making in these domains must ensure non-discrimination, fairness, and explainability. However, the legal ambiguity surrounding algorithmic bias and indirect discrimination poses a substantial risk. In-house counsels must be prepared to address potential legal disputes regarding unfair hiring practices or wrongful terminations linked to opaque AI-driven assessments. Ensuring compliance while balancing business efficiency with GDPR, non-discrimination, and workers' rights is a formidable challenge.

Moreover, liability allocation in cases of AI malfunctions or regulatory breaches presents an additional burden. Given the AI Act's emphasis on human accountability, in-house counsels must

[130] AI Act, supra note 1, Article 72.

work closely with compliance officers, HR teams, and external AI providers to draft robust contractual agreements that clearly define responsibilities, liability frameworks, and risk-sharing mechanisms. From a US corporate law perspective, this function closely mirrors the role of general counsel: not a purely advisory organ; rather, a corporate gatekeeper entrusted with independent responsibility for ensuring compliance.[131] This gatekeeping conception is deeply rooted in U.S. law: courts have emphasized that corporate counsel must "report up" material compliance failures to the board, as codified in Rule 1.13 of the ABA Model Rules of Professional Conduct.[132] After the Sarbanes–Oxley Act, this duty was reinforced through SEC regulations requiring attorneys appearing before the Commission to report evidence of material violations of securities laws or breaches of fiduciary duty.[133] By situating AI compliance within this same gatekeeping framework,[134] the AI Act reinforces a conception of in-house counsel as both strategic legal advisor and institutional safeguard. For U.S. audiences, this parallel is critical: it suggests that the evolving fiduciary and professional obligations of corporate counsel in the age of AI may be illuminated—and potentially reshaped—by the European model.

---

[131] ACC, ROLE OF GENERAL COUNSEL (SEPT. 2009), https://www.acc.com/sites/default/files/resources/vl/membersonly/InfoPAK/700992_3.pdf; Richard S. Gruner, *General Counsel in an Era of Compliance Programs*, 46 EMORY L.J. 1113, 1144 (1997); Deborah A. DeMott, *The Discrete Roles of General Counsel*, 74 FORDHAM L. REV. 955, 960 (2005); Ben W. Heineman, Jr., *The General Counsel as Lawyer-Statesman* 7 (Harv. L. Sch. Program on the Legal Prof. 2010), https://clp.law.harvard.edu/assets/General_Counsel_as_Lawyer-Statesman.pdf.

[132] The American Bar Association's Rule 1.13(b) accordingly provides that "if a lawyer for an organization knows that an officer, employee or other person associated with the organization is engaged in action … that is a violation of a legal obligation to the organization … and that is likely to result in substantial injury to the organization, then the lawyer shall proceed … in the best interest of the organization."

[133] Sarbanes–Oxley Act of 2002, § 307, codified at 15 U.S.C. § 7245; 17 C.F.R. pt. 205 (https://www.sec.gov/rules-regulations/2003/01/implementation-standards-professional-conduct-attorneys). *See* Bird & Park, supra note 124, at 212-3.

[134] *Cf.* Griffith, supra note 118, at 2083–96 (documenting how compliance functions emerge not from boards or corporate statutes but from external enforcement pressures, reconfiguring traditional conceptions of corporate governance).

B. Best practices

Because the compliance-officer best practices are intentionally more expansive, the counsel guidance below distills role-specific priorities into a concise but substantive roadmap. The emphasis is not on duplicating operational tasks but on highlighting how in-house legal teams can serve as the strategic hinge between regulatory obligations, board oversight, and litigation exposure. Their role demands both technical fluency in AI regulation and a lawyer's instinct for liability allocation, disclosure management, and cross-border legal risks. On a daily basis, in-house counsels must weave the AI Act into the broader fabric of corporate law, governance, and contractual architecture by focusing on the following priorities:[135]

1. Drafting AI-related contractual clauses to manage liabilities in partnerships with AI providers. In-house counsel must ensure that contractual frameworks capture the AI Act's obligations and allocate liability clearly. Key clauses include:
    - Warranties of compliance with AI Act standards.
    - Indemnities against regulatory breaches and penalties.
    - Transparency obligations ensuring vendors provide conformity documentation.
    - Balanced protections where EU disclosure mandates conflict with U.S. trade secret protections.
2. Conducting legal risk assessments for AI models in critical operations. Legal review should complement technical testing by identifying legal vulnerabilities:
    - Product liability exposure under EU directives.
    - Risks of algorithmic discrimination or breach of fundamental rights.
    - Shareholder litigation triggers under U.S. securities law.

[135] *See also* FRESHFIELDS, USING ARTIFICIAL INTELLIGENCE: THE TOP ACTIONS GENERAL COUNSEL SHOULD TAKE (FEB. 4, 2023), https://technologyquotient.freshfields.com/post/102itlx/using-artificial-intelligence-the-top-actions-general-counsel-should-take.

- Cross-border conflicts where AI deployment in one jurisdiction triggers liability in another.

3. Reviewing AI procurement agreements for vendor compliance. Procurement contracts must be more than transactional—they must secure enforceable compliance guarantees:
    - Obligations on data governance, bias audits, and incident reporting.
    - Cooperation duties with EU regulators in case of investigation.
    - Rights of audit or external certification where AI vendors resist full disclosure.
4. Developing AI compliance frameworks within the corporation. Counsel should embed legal compliance into corporate governance frameworks:
    - Drafting policies that align with Articles 66 (accountability) and 74 (market surveillance).
    - Delivering training to executives and staff on AI's legal and ethical risks.
    - Ensuring AI risk management is integrated into existing compliance and disclosure structures.
5. Managing extraterritorial risks through contractual design. Contracts must anticipate jurisdictional conflict by:
    - Selecting governing law and jurisdiction for AI-related disputes.
    - Allocating liability between EU-based and non-EU entities.
    - Addressing tensions between EU transparency mandates and U.S. IP protections.
6. Integrating AI governance with corporate risk management. AI oversight must not be siloed but linked to enterprise-wide frameworks:
    - Aligning with COSO, ISO 31000, and comparable risk models.
    - Conducting regular AI legal audits and risk exposure mapping.
    - Ensuring directors can demonstrate Caremark-level oversight of AI as a mission-critical risk.

7. Engaging with regulators and industry bodies. Proactive engagement enhances credibility and foresight:
    - Maintaining dialogue with the European AI Office and national authorities.
    - Participating in industry consortia, standards bodies, and regulatory consultations to anticipate enforcement trends.
8. Enhancing contractual protections in corporate transactions. AI-related liability must be anticipated in deals and partnerships:
    - Building liability-transfer mechanisms into supplier and vendor contracts.
    - Demanding warranties, indemnities, and representations in M&A agreements.
    - Ensuring AI portfolios of acquisition targets are EU-compliant before closing.
9. Embedding AI ethics and corporate social responsibility. Legal strategy must also advance reputational and ESG objectives:
    - Adoption of EU AI Ethics Guidelines to evidence commitment to "trustworthy AI."
    - Deployment of fairness and bias mitigation mechanisms to support ESG reporting.
    - Integration of AI governance into CSR narratives to build investor and stakeholder trust.
10. Overseeing enforcement, disclosure, and reporting obligations In-house counsel must act as stewards of disclosure and audit readiness:
    - Coordinating regulatory reporting and incident notifications.
    - Ensuring conformity documentation is maintained, accurate, and accessible.
    - Anticipating that EU disclosures may create litigation risks in U.S. courts, including shareholder or consumer actions.

VII. Mastering the Fire of AI Governance and the Path Ahead

The AI Act imposes structure upon an evolving technological force that otherwise risks slipping into unpredictability, opacity, and unchecked influence. At the heart of this regulatory transformation lies a diverse ensemble of corporate actors and, among them, in particular "the Overlooked"—board secretaries, compliance officers, and in-house counsels—who emerge as central figures in translating AI governance into actionable corporate policy. They are the intermediaries between regulatory mandates and boardroom decisions, ensuring that AI risk assessments, compliance frameworks, and liability considerations align with both the AI Act's provisions and broader corporate strategy. As Kaminski and Selbst caution, the AI Act functions as a 'legal exoskeleton'—a hard regulatory shell wrapped around softer technical standards.[136] For US audiences, this reframing shows why EU regulation is not just a European story but a practical governance challenge for American companies with global reach, and much of the law's substance will be filled in later by European regulators and standards bodies, complicating transatlantic compliance planning.[137]

Under the AI Act, AI compliance is not merely an operational requirement but a strategic necessity. Legal risk is not confined to directors and AI providers; it permeates the entire corporate structure. While the AI Act does not expressly codify statutory duties for compliance officers, board secretaries, or legal counsel, its detailed allocation of obligations to providers, deployers, and other regulated actors (Arts. 16–29) compels firms to distribute those duties internally. In this way, the Act may nonetheless influence how American articulate the scope of such officer oversight obligations, particularly in litigation where plaintiffs argue that AI-related risks were consciously disregarded.

---

[136] *See* Griffith, supra note 118, at 2077–82 (introducing compliance as an exogenous governance function imposed by enforcement agents, thereby challenging the traditional shareholder–manager agency cost paradigm).

[137] Margot E. Kaminski & Andrew D. Selbst, *An American's Guide to the EU AI Act*. U. Colorado Law Legal Studies Research Paper No. 25-18 (July 30, 2025), https://ssrn.com/abstract=5373345, 138-9.

Each and every corporate role discussed in this paper must proactively address AI-related risks, ensuring that liability is managed and mitigated across the organization. Companies failing to align their AI governance with regulatory expectations risk not only fines but also reputational damage and loss of stakeholder trust. For American boards, this strategic necessity will inevitably involve Audit Committees, CROs, and CPOs, acting as a bridge between European regulatory expectations and U.S. corporate governance practices, ensuring that AI oversight is integrated into established risk, privacy, and audit frameworks.

Moreover, the AI Act is not a static regulation but an evolving framework: much like AI itself, the law governing it will continue to adapt, necessitating an agile compliance approach that anticipates future amendments. Hence, from boardroom discussions to risk assessment methodologies, AI must be embedded into decision-making processes to ensure sustainable and responsible deployment.

As Pirandello's six characters needed a script, the AI Act gives today's corporate actors a regulatory playbook—but one that defines obligations in functional terms rather than by corporate office. It is management that must translate these duties into concrete roles within the firm. But just as Pirandello's drama resists a definitive conclusion, so too does AI governance remain a work in progress. The AI Act may be comprehensive, yet its implementation, interpretation, and enforcement will shape its ultimate impact. Future research will explore whether this framework succeeds in balancing innovation with accountability or whether its rigid structures require further evolution to accommodate AI's continual transformation. The path ahead is clear: all corporate actors must not merely react to AI regulation but actively shape their governance strategies, ensuring that AI serves both economic progress and fundamental human rights. And there is more. For US academics and practitioners, the AI Act provides a rare external laboratory where officer-level compliance obligations are being formalized by statute. By studying how European courts and regulators enforce these role-specific duties, US judges and scholars can draw on comparative evidence when shaping doctrines of fiduciary oversight, officer liability, and gatekeeping responsibilities in the age of AI. In

this sense, the AI Act's capacity to become a global benchmark will depend not only on EU enforcement but also on the extent to which corporations internalize its obligations through their governance structures.