LUISS

Department of Business and Management

Course of Business Cyberlaw

Compliance Obligations of Generative AI system for business use in the EU AI Act

Prof. Eugenio Prosperetti

SUPERVISOR

Odongoo Ser-Od 287781

CANDIDATE

Academic Year 2024/2025

Table of contents:

Abstract

Generative artificial intelligence (GenAI), which offers previously unheard-of capabilities in data analysis, automated decision-making, and content production, has quickly transitioned from experimental deployment to mainstream business practice. However, despite its potential, GenAI poses significant legal and regulatory issues, especially in the EU. The first thorough attempt to govern AI using a risk-based framework is the EU's Artificial Intelligence Act (AI Act), which places strict requirements on companies that develop and implement high-risk systems. The way firms must plan, execute, and defend the use of AI is drastically altered by these regulations, which include those pertaining to risk management, data governance, transparency, human oversight, and post-market monitoring.

Through scholarly discussion, case law, and doctrinal legal research, this thesis investigates the regulatory environment surrounding generative AI in corporate set- tings. It looks into how the AI Act's requirements are translated into practical compliance plans, paying particular emphasis to how small and medium-sized businesses are disproportionately affected. The analysis draws attention to the ambiguity caused by conflicting legislative obligations and the lack of uniform enforcement practices among Member States. The way that courts expand algorithmic accountability is demonstrated by judicial developments like the SCHUFA (C-634/21) and Uber cases, which emphasize that algorithmic scores, flags, or deactivations must be seen as legally binding decisions that are subject to safeguards.

The results show a double dynamic: while regulatory requirements impose significant costs for compliance and risk aversion, they also give companies the chance to stand out through ethical use of GenAI, trust, and transparency. Businesses can turn legal obligations into strategic advantages by integrating compliance into governance frameworks. This helps them gain credibility and customer trust in fiercely competitive industries.

The thesis concludes that more uniformity and clarity within the EU framework are necessary for the effective regulation of generative AI. Compliance

should be viewed as a tool of governance as well as a legal requirement, integrating ethical responsibility and accountability into the core of corporate decision-making.

Introduction

The use of Generative Artificial Intelligence (GenAI) in commercial decision-making has quickly become revolutionary. Industries ranging from marketing and finance to human resources and compliance management are changing as a result of its capacity to produce text, graphics, and sophisticated data outputs. However, the very characteristics that make GenAI so potent, its opacity, dependence on large datasets, and ability to produce autonomous results, also give rise to urgent legal and regulatory issues. Accountability, fairness, and transparency issues are no longer merely theoretical; they now have a tangible impact on how businesses function and how people react to the results of automated judgments.

The European Union has responded to these challenges with the adoption of the Artificial Intelligence Act, which introduces a risk-based framework for the design, use, and monitoring of AI systems. Alongside this, existing instruments such as the General Data Protection Regulation continue to shape the regulatory environment, often creating overlapping obligations. Businesses therefore face the dual difficulty of understanding complex requirements and managing the uncertainty that arises from fragmented enforcement. These legal challenges are not abstract; they directly affect how firms deploy generative AI and whether they can build trust in its use.

This thesis examines the legal and regulatory challenges of generative AI in business contexts through doctrinal analysis of legislation, case law, and academic literature. It investigates the compliance obligations set by the AI Act, the practical impact of risk

based classification on firms, and the ethical concerns that persist around bias, privacy, and transparency. Judicial developments such as SCHUFA and Uber illustrate how courts are expanding the scope of algorithmic accountability, reinforcing the importance of compliance duties.

The analysis is structured into three chapters: the first explores the compliance framework and sanctions under the AI Act; the second considers business implications and risk-based decision-making; and the third addresses ethical concerns that cut across law and practice. The conclusion draws these strands together, arguing that compliance should be seen not only as a legal requirement but also as a form of governance capable of embedding accountability into the core of business decision-making.

CHAPTER 1: COMPLIANCE IN THE AI ACT–RELEVANT PROVISIONS AND SANCTIONS

One of the most significant restrictions introduced by the EU AI Act is outlined in Article 5(1)(a), which prohibits the use of AI systems that deploy subliminal techniques beyond an individual's consciousness in ways that may materially distort behavior and cause physical or psychological harm. While this provision is critical for protecting fundamental rights, its implications for commercial applications of generative AI are profound. For instance, businesses using large generative AI models (LGAIMs) for personalized advertising, dynamic pricing, or consumer engagement could risk violating this article if their systems manipulate users' behavior without informed awareness. However, legal scholars have criticized the vague nature of this provision. Bulgakova observes that the Act lacks a precise definition of what constitutes "subliminal techniques" or "psychological harm," leaving businesses uncertain about how to remain compliant. This legal ambiguity increases the possibility of regulatory overreach or underenforcement in commercial contexts, in addition to making compliance evaluations more difficult for AI developers and deployers. Businesses that

use AI-driven nudging techniques in marketing or interface design, in particular, could have to negotiate a complex legal landscape under the Act's current phrasing. [1]

1.1 OVERVIEW OF THE AI ACT OBJECTIVES AND SCOPE OF LEGISLATION

The world's first complete legislative framework devoted to regulating artificial intelligence is the European Union's Artificial Intelligence Act (AI Act). [2] This was introduced in April 2021 and formally adopted in March 2024. [3]This horizontal legislative effort was a result of the EU's wider digital agenda, which includes Digital Strategy and the White Paper on AI, and placed a strong emphasis on both innovation and ethical supervision. [4] The Act responds to the increasing integration of AI in critical sectors, such as public administration, healthcare, education, and finance, while addressing the systemic concerns these technologies bring to safety, democracy, and fundamental rights. [5]

[6]With an emphasis on both innovation and ethical monitoring, the EU's broader digital agenda which included the Digital Strategy and the White Paper on AI led to the creation of this horizontal legislative endeavor. [7]The Act addresses the systemic threats these technologies pose to safety, democracy, and fundamental rights while responding to the growing integration of AI in important industries, including public administration, healthcare, education, and finance. [8]

---

[1] D. Bulgakova, "La pratica proibita dell'intelligenza artificiale," *Theory and Practice of Forensic Science and Criminalistics* 32, n. 3 (2023), pp. 89-112.
[2] H.-W. Micklitz – G. Sartor, "Compliance and enforcement in the AIA through AI," *Yearbook of European Law* 43 (2024), pp. 297-341.
[3] Ibid.
[4] Ibid.
[5] Ibid.
[6] Kusche, "Possible harms of artificial intelligence and the EU AI Act: fundamental rights and risk," *Journal of Risk Research* 0, n. 0 (s.d.), pp. 1-14.
[7] Ibid.
[8] Kusche, "Possible harms of artificial intelligence and the EU AI Act: fundamental rights and risk," *Journal of Risk Research* 0, n. 0 (s.d.), pp. 1-14.

[9]The so-called "Brussels Effect," or the EU's ability to influence global digital standards through domestic law, lends support to this goal. According to academics like Isabel Kusche, the Act positions the EU as a global standard-setter for risk-based AI governance in addition to being a market regulator. [10]This effect is further reinforced by its extraterritorial reach, which applies to any AI system deployed within the EU, regardless of the provider's location. This has significant ramifications for international corporations. [11] Article 114 of the Treaty on the Functioning of the European Union (TFEU), which gives the EU the authority to enact policies that guarantee the efficient operation of the internal market, serves as the foundation for the Act. [12]Since Member States had started putting different national AI initiatives into practice, one of the main reasons was to avoid regulatory fragmentation. [13]The Act strikes a balance between market integration and the core principles of the EU, such as democracy, rule of law, and the defense of fundamental rights, by standardizing regulations throughout the union.[14] The AI Act complements existing digital legislation, such as the General Data Protection Regulation (GDPR), the Digital Services Act (DSA), and the Cybersecurity Act. [15] While the GDPR focuses on data protection, the AI Act targets the development, classification, and deployment of AI systems. [16] Together, these instruments create a coherent and future-proof regulatory environment.[17] The Act applies to both public and private actors involved in the development, deployment, or use of AI systems within the EU, including providers outside the EU whose systems affect EU residents. [18]It covers a broad range of systems, notably general-purpose AI (GPAI) and generative AI models, which can serve as the foundation for high-risk applications under Annex

[9] Ibid.
[10] Ibid.
[11] MICKLITZ - SARTOR, *Compliance and enforcement in the AIA through AI*, cit.
[12] Ibid.
[13] D. Bulgakova, “La pratica proibita dell’intelligenza artificiale,” *Theory and Practice of Forensic Science and Criminalistics* 32, n. 3 (2023), pp. 89-112.
[14] Ibid.
[15] Ibid.
[16] Ibid.
[17] Ibid.
[18] Ibid.

III. [19] For instance, a model like GPT-4 integrated into an HR recruitment tool may trigger compliance obligations due to its potential impact on individuals.

[20]Recognizing this, the final version of the Act adopted in 2023 introduced specific transparency obligations for GPAI systems (Article 53), and additional requirements for advanced "foundation models." [21] These include risk management, technical documentation, and mitigation of systemic risks, especially relevant for commercial uses in hiring, credit scoring, or content personalization, where legal and ethical stakes are particularly high.

1.1.1 DEFINITION AND CLASSIFICATION OF AI SYSTEMS, WITH A FOCUS ON GENERATIVE AI

[22]The EU Artificial Intelligence Act introduces a series of legal definitions that are central to understanding the scope and structure of compliance obligations, especially in the context of generative AI systems used in business operations. [23]At the heart of the regulatory framework is the term "AI system", defined in Article 3(1) as "a machine-based system designed to operate with varying levels of autonomy and that, for explicit or implicit objectives, can generate outputs such as predictions, recommendations or decisions influencing physical or virtual environments." [24]This broad and technologically neutral definition ensures that the Act captures both narrowly focused AI applications, such as customer service chatbots or credit scoring algorithms, and more advanced models like GPT-4 or Stable Diffusion, which are capable of producing human-like text, images, or sound with minimal human

[19] KUSCHE, *Possible harms of artificial intelligence and the EU AI act: fundamental rights and risk*, cit.
[20] Ibid.
[21] Ibid.
[22] Kusche, *Possible harms of artificial intelligence and the EU AI Act: fundamental rights and risk*, cit.
[23] Ibid.
[24] Ibid.

prompting. [25]The expansive scope of the term has been widely welcomed for its future- proofing potential, yet it also raises questions about overbreadth and enforceability in light of evolving AI capabilities.[26] In the final compromise of the AI Act, lawmakers introduced the concept of general-purpose AI (GPAI). [27]These are models designed to perform a wide range of tasks, including speech and image recognition, translation, content generation, or question answering. [28] The reason for adding this definition is to address the challenges posed by highly adaptable foundation models that can be fine- tuned for many applications. [29]Although GPAI models are not automatically considered high-risk, their use in sensitive fields like medical diagnostics or recruitment can make the overall system high-risk. [30]This means that obligations for compliance depend not only on the model itself but also on how it is applied in real- world, high-impact scenarios.[31] The Act's risk-based classification system provides the core mechanism for determining the extent of regulatory obligations. [32] AI systems are divided into four categories: unacceptable risk, high risk, limited risk, and minimal risk. Unacceptable-risk systems, such as AI used for social scoring by public authorities or those exploiting the vulnerabilities of children or persons with disabilities, are banned outright under Article 5. [33]High-risk AI systems, governed primarily by Article 6 and detailed in Annex III, include those deployed in sectors like employment, education, law enforcement, and critical infrastructure. [34] These systems must comply with a range of stringent obligations, including risk management procedures (Article 9), data governance standards (Article 10), technical documentation (Article 11), transparency

[25] KUSCHE, *Possible harms of artificial intelligence and the EU AI Act: fundamental rights and risk*, in *Journal of Risk Research*, pp. 1–14.
[26] Ibid.
[27] Ibid.
[28] Ibid.
[29] Ibid.
[30] Ibid.
[31] Ibid.
[32] Ibid.
[33] KUSCHE, *Possible harms of artificial intelligence and the EU AI act: fundamental rights and risk*, cit.
[34] Ibid.

requirements (Article 13), and post-market monitoring (Articles 61–73). By contrast, limited-risk systems such as chatbots or deepfake generators are subject mainly to transparency requirements (e.g., user disclosure that they are interacting with AI), while minimal-risk systems, like AI in video games or spam filters, are largely exempt from mandatory compliance obligations.[35] The AI Act also introduces a risk-based classification system, where systems are labeled as:

- Unacceptable risk (banned): e.g., AI systems used for social scoring by public authorities or those that exploit vulnerabilities of children or disabled persons.
- High-risk: AI used in critical infrastructure, employment, education, law enforcement, and similar sectors. These require strict obligations including risk management, data governance, human oversight, and technical documentation.
- Limited risk: AI systems requiring transparency obligations, such as chatbots that must inform users they are interacting with AI.
- Minimal risk: Systems like AI in video games or spam filters, which fall outside major regulatory burdens.

[36]The classification system, while logically coherent in theory, proves more difficult to implement in practice, especially for generative AI models. [37]These models are often not designed for a specific use but rather made available for third-party integration across diverse sectors, some of which may fall under the high-risk category. [38]For instance, a company may use a foundation model like GPT-4 to automate initial candidate screening in recruitment a use case explicitly listed in Annex III. [39]In such scenarios, the model itself may not be inherently high-risk, but the overall application becomes high-risk by association. [40]This functional coupling between model and

[35] Cit.
[36] S. Wachter, "Limitations and Loopholes in the EU AI Act and AI Liability Directives: What This Means for the European Union, the United States, and Beyond," *SSRN Electronic Journal* (2024), pp. [s.l.].
[37] Ibid.
[38] Ibid.
[39] S. Wachter, "Limitations and Loopholes in the EU AI Act and AI Liability Directives: What This Means for the European Union, the United States, and Beyond," *SSRN Electronic Journal* (2024), pp. [s.l.]..
[40] Ibid.

deployment context introduces significant regulatory ambiguity, especially for businesses attempting to assess their obligations in complex, modular AI systems.[41] Recital 60 of the AI Act attempts to address this challenge by clarifying that GPAI models "may contribute to the functioning of high-risk AI systems" and thus may be subject to documentation and transparency requirements even if they are not directly classified as high-risk. [42] Moreover, Article 6(2) stipulates that any AI system intended to be used in a high-risk domain as listed in Annex III must be treated as high-risk, regardless of the model's original purpose.[43] However, this provision introduces a compliance paradox for foundation model providers: while they may not have control over downstream applications, they are nonetheless expected to anticipate potential high-risk uses and proactively mitigate risks through design, documentation, and responsible release strategies.[44] Legal scholars have raised concerns about this context- dependent approach. [45]Wachter (2024) argues that the Act's hybrid logic combining ex ante classification with post hoc application-based risk assessment creates "legal uncertainty and regulatory fragmentation,"

especially across Member States with differing enforcement strategies. [46]Kusche (2024) similarly warns that the definitional fluidity of GPAI and high-risk applications opens the door to "political interpretation and selective compliance," particularly when economic incentives favor rapid deployment over cautious alignment with regulatory thresholds. These concerns are amplified in business environments where foundation models are embedded into proprietary workflows that evolve rapidly, often without the technical documentation or oversight mechanisms envisioned by the Act.

[41] Ibid.
[42] , *Full article: Possible harms of artificial intelligence and the EU AI act: fundamental rights and risk*, cit.
[43] Ibid.
[44] WACHTER, *Limitations and Loopholes in the EU AI Act and AI Liability Directives: What This Means for the European Union, the United States, and Beyond*, cit.
[45] Ibid.
[46] KUSCHE, *Possible harms of artificial intelligence and the EU AI act: fundamental rights and risk*, cit.

Concerns regarding this context-dependent approach have been voiced by legal scholars. [47]Wachter (2024) contends that "legal uncertainty and regulatory fragmentation" are caused by the Act's hybrid logic, which combines before classification with subsequent application-based risk assessment. Article 101 outlines specific enforcement powers related to the responsibilities of GPAI providers. It applies to providers that fail to cooperate with the European Commission, for example, by withholding technical documentation or submitting misleading information. [48]In parallel, Article 99 sets out the sanctions for serious breaches of core obligations tied to high-risk AI systems, which can reach fines of up to €35 million or 7% of a company's worldwide annual revenue. [49]Fines under Article 101 are capped at €15 million or 3% of global turnover, reflecting the European Union's growing recognition of the systemic importance of GPAI models, even outside direct high-risk applications. These provisions ensure that foundational model providers are not exempt from oversight simply because their models are versatile or market-neutral.

[50]Ultimately, the AI Act's treatment of generative and general-purpose AI models reveals a complex balance between flexibility and enforceability. [51]On one hand, the framework seeks future-proof regulation by focusing on function and impact rather than technological specificity. [52]On the other hand, the resulting compliance burden is fragmented across providers, deployers, and third-party integrators, each of whom may interpret risk and responsibility differently. For business users of generative AI, particularly those integrating such tools into high-risk functions like hiring, finance, or

[47] WACHTER, *Limitations and Loopholes in the EU AI Act and AI Liability Directives: What This Means for the European Union, the United States, and Beyond*, cit.
[48] Ibid.
[49] Ibid.
[50] KUSCHE, *Possible harms of artificial intelligence and the EU AI act: fundamental rights and risk*, cit.
[51] Ibid.
[52] Ibid.

healthcare, this fragmented structure poses significant legal and operational challenges. It also underscores the need for robust internal governance, interdisciplinary compliance teams, and clear contractual obligations between model developers and downstream users. As enforcement mechanisms evolve, particularly through the AI Office and national competent authorities, businesses will need to navigate an increasingly layered regulatory landscape where the classification, deployment, and context of AI systems determine not only legal obligations but also market access within the European Union.

1.1.2 LEGAL AND PRACTICAL CHALLENGES IN CLASSIFICATION

[53]The classification framework has drawn criticism for its lack of definitional clarity and the practical difficulty of determining whether a system is high-risk. [54]As outlined by Kusche and others, the risk categories depend on subjective interpretations of concepts like "impact on fundamental rights," making it possible for identical systems to be classified differently depending on the sector or even the Member State enforcing the Act. [55] Small and medium-sized businesses (SMEs), which might not have the legal or technical expertise necessary to evaluate compliance risks, face an especially difficult task. These businesses must understand overlapping legal responsibilities under the AI Act, GDPR, and sectoral legislation, undertake internal risk assessments, and interact with third-party conformity assessment agencies. This complexity is made much more difficult for companies that use generative AI by the quick speed at which technology is developing and the newness of GPAI regulations.

---

[53] , *Article 5: Prohibited AI Practices | EU Artificial Intelligence Act*, [s.d.]consultabile su https://artifi- cialintelligenceact.eu/article/5/.

[54] KUSCHE, *Possible harms of artificial intelligence and the EU AI act: fundamental rights and risk*, cit.

[55] , *Article 6: Classification Rules for High-Risk AI Systems | EU Artificial Intelligence Act*, [s.d.]consultabile su https://artificialintelligenceact.eu/article/6/.

Another issue arises from Article 7, which allows the European Commission to update Annex III, the list of high-risk AI systems, using a set of evaluative criteria, including potential harm, the number of people affected, and societal impact. [56]This means the classification of a given system may evolve, adding another layer of uncertainty for business actors already trying to implement compliance measures. [57]

1.1.3 EXAMPLES: CHATGPT AND BUSINESS USE

[58]Recent debates in the European Parliament have raised the question of whether models like ChatGPT should be classified under high-risk or foundation model rules. While such models are not inherently high-risk, their deployment in sectors such as education, finance, or healthcare can trigger high-risk classification depending on their influence on individual rights, safety, or access to services.

[59]For example, if a company uses ChatGPT to provide initial customer assessments for loans applications, that use may fall under the "access to essential services" category in Annex III. Similarly, generative AI used in medical triage tools, legal document drafting, or hiring algorithms could all be considered high-risk applications.

[60]The classification of AI systems under the AI Act is both foundational and fraught with complexity. [61]While the risk-based structure provides a theoretically elegant way to scale regulatory obligations, the contextual and evolving nature of general-purpose and generative AI systems reveals significant regulatory gaps and compliance

[56] , *Article 7: Amendments to Annex III | EU Artificial Intelligence Act*, [s.d.]consultabile su https://artificialintelligenceact.eu/article/7/.
[57] , *European Commission, official website - European Commission*, 2025consultabile su https://commission.europa.eu/index_en.
[58] , *European Commission, official website - European Commission*, cit.
[59] , *Article 7: Amendments to Annex III | EU Artificial Intelligence Act*, cit.
[60] T. KARATHANASIS, *Guidance on Classification and Conformity Assessments for High-Risk AI Systems under EU AI Act*, [s.d.].
[61] , *Full article: Possible harms of artificial intelligence and the EU AI act: fundamental rights and*

risk, cit.

challenges. Businesses integrating generative AI must navigate a highly dynamic classification landscape, balancing innovation with legal certainty and ethical responsibility. [62]Going forward, clearer guidelines, updated regulatory interpretations, and greater technical support will be essential for ensuring that the classification system supports both compliance and responsible innovation.

1.2 COMPLIANCE OBLIGATIONS FOR HIGH-RISK AI SYSTEMS

1.2.1 RISK MANAGEMENT SYSTEMS AND ASSESSMENT

[63]One of the core compliance obligations imposed by the EU Artificial Intelligence Act (AI Act) on high-risk AI systems is the implementation of a comprehensive, lifecycle-based risk management system. [64]Codified under Article 9, this requirement establishes a structured framework obliging providers to identify, analyze, evaluate, and mitigate risks throughout all phases of an AI system's lifecycle, including development, deployment, and post-market use. The AI Act adopts a risk-based regulatory model whereby legal obligations scale with the potential impact of the system on health, safety, and fundamental rights. [65] High-risk AI systems

Particularly those employed in sensitive domains such as employment, law enforcement, and critical infrastructure, must adhere to an ongoing risk management process, broadly aligned with established principles of product safety governance. [66]Article 9 thus reflects a preventative

logic that aims to mitigate harm before it materializes, grounded in the principles of proportionality and accountability.

---

[62] , *Recital 60 | EU Artificial Intelligence Act*, [s.d.]consultabile su https://artificialintelligenceact.eu/re- cital/60/.

[63] , *Article 5: Prohibited AI Practices | EU Artificial Intelligence Act*, cit.

[64] , *Article 9: Risk Management System | EU Artificial Intelligence Act*, [s.d.]consultabile su https://arti- ficialintelligenceact.eu/article/9/.

[65] , *Article 5: Prohibited AI Practices | EU Artificial Intelligence Act*, cit.

[66] , *Article 9: Risk Management System | EU Artificial Intelligence Act*, cit.

This risk management process begins in the pre-market phase, during which providers are required to conduct a conformity assessment and define internal procedures to document both foreseeable and emergent risks. This includes evaluating not only the system's intended use but also "reasonably foreseeable misuse," such as user error, adversarial manipulation, or model drift. Risks that cannot be eliminated must be reduced to an acceptable residual level. Any remaining risks must be clearly communicated to users through documentation and usage instructions.

Under Article 9(2), a compliant risk management system must incorporate several core components: the identification and analysis of known and foreseeable risks; assessment of the severity and probability of harm; and implementation of mitigation strategies that are technically and ethically robust. Notably, the Act does not mandate specific risk management tools; instead it requires a proportionate response calibrated to the system's complexity, purpose, and operational context.

Generative AI systems, such as those built on large language models like GPT, present particular challenges in this regard. Their general purpose and nature complicate traditional risk assessment, as outputs cannot always be anticipated or controlled. In high-stakes environments such as recruitment, credit scoring, or personalized advertising, mitigation may necessitate layered safeguards including input moderation, real-time output filtering, adversarial testing, and stress simulations to detect and reduce systemic risks.

Furthermore, the AI Act mandates ongoing testing and refinement of mitigation mechanisms. [67] This includes regular performance evaluations, bias audits, and robustness assessments to ensure the system continues to operate safely and fairly as it interacts with real-world users. [68] In this regard, the Act encourages a proactive stance, whereby risk prevention is embedded into both technical development and governance structures.

[67] J. S. BUTT, *Analytical Study of the World's First EU Artificial Intelligence (AI) Act*, *International Journal of Research Publication and Reviews*, 5(33), 2024.
[68] Ibid

The obligation to monitor risks does not end at deployment. [69] Article 72 imposes a post-market monitoring duty, requiring providers to establish systems that collect and analyze operational data to detect performance deviations, emerging risks, and non- compliance. [70]When serious incidents occur, such as breaches of safety or fundamental rights, providers must notify national market surveillance authorities within fifteen days of becoming aware of the issue, pursuant to Article 73.[71] Crucially, the AI Act also extends risk management obligations to users (or deployers) who substantially modify an AI system or use it beyond the provider's intended scope. In such cases, the user is deemed a provider and must comply with the full range of regulatory requirements. [72]This mechanism underscores the EU's commitment to shared responsibility within the AI lifecycle, particularly where changes could compromise the system's safety or compliance profile.

In sum, the risk management obligation under the AI Act is dynamic and iterative. It spans the entire AI lifecycle and requires providers and, in some cases, users to invest in governance frameworks that prioritize transparency, robustness, and human- centered safeguards. While the burden may be particularly acute for small and medium- sized enterprises (SMEs), the Act's lifecycle approach is ultimately designed to foster the development and deployment of safe, trustworthy, and ethically aligned AI technologies within the EU internal market.

1.2.2 DATA GOVERNANCE AND DATA QUALITY

Among the essential compliance obligations introduced by the EU Artificial Intelligence Act (AI Act) for high-risk systems, data governance and data quality play a central role. [73] Codified under Article 10, these requirements ensure that data used

[69] , *Article 72: Post-Market Monitoring by Providers and Post-Market Monitoring Plan for High-Risk AI Systems | EU Artificial Intelligence Act*, [s.d.]consultabile su https://artificialintelligenceact.eu/article/72/.

[70] , *Article 73: Reporting of Serious Incidents | EU Artificial Intelligence Act*, [s.d.]consultabile su https://artificialintelligenceact.eu/article/73/.

[71] Ibid.

[72] , *Article 28: Notifying Authorities | EU Artificial Intelligence Act*, [s.d.]consultabile su https://artificialintelligenceact.eu/article/28/.

[73] , *Article 10: Data and Data Governance | EU Artificial Intelligence Act*, [s.d.]consultabile su https://artificialintelligenceact.eu/article/10/.

throughout the AI system lifecycle, particularly for training, validation, and testing, meets the highest standards of quality to avoid harmful, discriminatory, or inaccurate outcomes. For businesses integrating generative AI models into high-risk domains such as recruitment, healthcare, or financial services, complying with these standards is technically challenging and legally indispensable.

The AI Act requires high-risk AI providers to establish data governance frameworks ensuring transparency, accountability, and traceability. These frameworks must set clear rules for data collection, cleaning, labeling, annotation, and aggregation, ensuring each step is documented and systematically monitored. Notably, data governance extends throughout the entire AI lifecycle, encompassing post-market monitoring and performance evaluation.

[74]To facilitate traceability, providers must maintain detailed technical documentation outlining the origin, structure, and processing of data used in the system. This documentation must be available for review by market surveillance authorities, making it critical for legal compliance and ensuring that data management practices remain transparent and verifiable.

A core concern of the AI Act is the processing of special categories of personal data, such as biometric, health, or political data. Providers must implement adequate safeguards to ensure such sensitive data is handled in compliance with broader frameworks like the General Data Protection Regulation (GDPR), ensuring lawful, secure, and ethical usage.[75] Businesses must establish legal grounds and technical safeguards for handling sensitive data, such as user consent or data anonymization procedures.

[76]Article 10 of the AI Act outlines the most explicit and detailed data quality requirements in EU AI law to date. High-risk AI systems must use datasets that are

[74] BUTT J. S., Analytical Study of the World's First EU Artificial Intelligence (AI) Act, 2024, *International journal of research publication and reviews*, 5 (33), 2024.

[75] , *EU AI Act: first regulation on artificial intelligence*, su *Topics | European Parliament*, 2023consul- tabile su https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regula-tion-on-artificial-intelligence.

[76] , *Article 10: Data and Data Governance | EU Artificial Intelligence Act*, cit.

relevant, representative, complete, and free from significant errors or bias. [77]These stipulations ensure that the system's predictions or decisions accurately reflect reality and fairly represent all relevant population groups, mitigating the risk of biased or discriminatory outcomes.

In high-risk business applications, especially when using generative AI for decision- making or content creation, poor data quality can lead to serious consequences, including reputational harm, regulatory penalties, and violations of fundamental rights. Providers are therefore expected to continuously assess and test their datasets, identifying potential biases such as historical discrimination in hiring data and adopting mitigation strategies. Ongoing evaluation is critical for ensuring the system's outputs are fair and representative of diverse demographic groups.

While early drafts of the AI Act initially demanded that datasets be "error-free," subsequent industry consultations have acknowledged that absolute accuracy is often unattainable in real-world scenarios. Nevertheless, the obligation to strive for the highest achievable data quality remains both a legal and ethical imperative under the Act.

Importantly, the AI Act treats data governance and quality as integral components of continuous risk management. Post-market surveillance obligations require providers to actively monitor and re-evaluate data quality during the system's operation, particularly in response to shifts in user behavior or environmental factors. [78] For example, if a generative AI system used for financial forecasting starts producing inaccurate outputs due to changing economic conditions, the provider must update both the system and its datasets to reflect the latest information.[79] This continuous quality control mechanism aligns with the broader goals of the AI Act ensuring fairness, transparency, and safety across all stages of the AI lifecycle. In high-risk business

[77] Ibid.

[78] , *Article 61: Informed Consent to Participate in Testing in Real World Conditions Outside AI Regulatory Sandboxes | EU Artificial Intelligence Act*, [s.d.]consultabile su https://artificialintelligenceact.eu/article/61/.

[79] Ibid.

applications, such as automated loan decisions or insurance underwriting, the reliability of data directly influences the system's legal compliance and commercial viability.

In conclusion, data governance and data quality are fundamental to the EU AI Act's regulatory framework for high-risk AI systems. For businesses deploying generative AI, fulfilling these obligations requires integrating technical tools, legal safeguards, and ethical frameworks to promote fairness and transparency throughout the data lifecycle. As data forms the foundation of all AI systems, the EU's focus on rigorous data governance reflects its overarching aim to foster a trustworthy and rights- respecting digital economy.

1.2.3 DOCUMENTATION, RECORD-KEEPING, AND TRANSPARENCY

For high-risk AI systems, the EU Artificial Intelligence Act (AI Act) lays out a thorough compliance structure, with requirements for technical documentation, automated logging, and transparency at its core. These responsibilities are crucial from a governance standpoint, guaranteeing the safe, moral, and legal implementation of AI systems in ways that protect fundamental rights, as well as from a regulatory standpoint, facilitating conformance assessments and post-market enforcement.

Under Article 11 of the AI Act, providers of high-risk AI systems must compile and maintain detailed technical documentation demonstrating compliance with the Act’s requirements. This documentation must include, among other elements, the system’s design specifications, intended purpose, decision logic, risk management procedures, and conformity assessments, as described in Annex IV. It must be updated throughout the lifecycle of the AI system and retained for at least ten years after market placement or commissioning, Analytical Study.

These requirements are not only formalistic but play a foundational role in both ex- ante

(pre-market) and ex-post (post-market) regulatory scrutiny. Authorities must be able to inspect this documentation during audits or investigations to verify compliance. For SMEs, the Act provides simplified obligations, but core components of conformity, safety, and reliability must still be demonstrated.

However, concerns have been raised about the feasibility of applying Article 11 uniformly across the AI ecosystem, particularly in the case of large generative AI models (LGAIMs). Given their general-purpose nature, providers of LGAIMs might be unable to document risks for all possible applications. [80]Legal scholars and technical experts have proposed shifting toward a use-based documentation model, where responsibilities are shared between developers and deployers depending on their actual role and knowledge in the value chain.

Article 12 of the AI Act states that high-risk AI systems are equipped with logging capabilities that automatically record key operational events and system parameters. These logs serve several regulatory functions: they facilitate traceability, enable post- incident investigations, and support the overall transparency and accountability of AI system behavior.

Logs must be maintained for at least six months and be made accessible to competent authorities upon request. The requirement ties directly to the system's operational lifecycle and is particularly critical when AI systems are deployed in safety- critical or rights-sensitive contexts. Logging obligations are often embedded in the technical documentation file, supporting both conformity assessments and risk monitoring.

The implementation of this obligation raises questions about feasibility in complex deployment chains, especially when the developer and deployer are different entities. In the case of LGAIMs, for example, meaningful logging may require cooperation across the value chain to ensure relevant actors (developers, deployers, users) have access to and control over the necessary operational data.

[81]Transparency is another cornerstone of the AI Act's compliance system.

---

[80] , *Article 11: Technical Documentation | EU Artificial Intelligence Act*, [s.d.]consultabile su https://ar- tificialintelligenceact.eu/article/11/.

[81] , *Article 12: Record-Keeping | EU Artificial Intelligence Act*, [s.d.]consultabile su https://artificialin- telligenceact.eu/article/12/.

Article 13 requires providers to furnish users with clear, accessible, and understandable information about the high-risk AI system. This includes explanations of the system's purpose, capabilities, and limitations, expected performance, foreseeable risks, and required human oversight procedures.

The goal is to ensure that users can operate the AI system safely and appropriately, while also being able to identify and respond to system errors, biases, or misuses. Transparency is particularly important for systems used in sensitive sectors such as employment, healthcare, or public administration. In such domains, failure to properly inform users can exacerbate risks to individuals' rights and safety.

Critiques have also emerged around Article 13's limited scope. While it currently applies only to high-risk systems, scholars argue that transparency obligations should be extended to developers and deployers of all impactful general-purpose AI models, especially in professional contexts.

Such expansions would foster better public trust, content authenticity, and ethical use, particularly in domains like journalism, education, and automated content generation.[82] The concept of transparency under Article 13 also overlaps with broader EU goals of user empowerment, informed consent, and fundamental rights protection. It supports not only responsible usage but also aligns with GDPR's fairness and accountability principles.

Articles 11, 12, and 13 of the EU AI Act function collectively to ensure that high- risk AI systems remain accountable, traceable, and safely operable throughout their lifecycle. Technical documentation anchors the legal traceability of system design and compliance; logging enables real-time and retrospective oversight; and transparency equips users to fulfill their own oversight responsibilities while mitigating the risks of misuse or overreliance.

[82] , *Article 13: Transparency and Provision of Information to Deployers | EU Artificial Intelligence Act*, [s.d.]consultabile su https://artificialintelligenceact.eu/article/13/.

Moreover, in light of emerging general-purpose AI models, there is a growing consensus that documentation and transparency regimes must evolve to reflect shared responsibilities,

risk-based proportionality, and use-specific obligations. As AI systems become increasingly integrated into critical business and societal domains, these obligations become not just regulatory checklists, but pillars of ethical and lawful AI governance.

1.2.4 HUMAN OVERSIGHT AND ACCOUNTABILITY

Human oversight is a cornerstone of the EU Artificial Intelligence Act (AI Act), particularly in relation to high-risk AI systems. Recognizing that technical safeguards alone are insufficient to fully mitigate all risks posed by AI, the Act mandates the integration of appropriate human control mechanisms to ensure that such systems operate in a safe, lawful, and ethically sound manner. Article 14 of the AI Act explicitly requires high-risk AI systems to be designed and developed in such a way that natural persons can exercise effective oversight throughout the system's life cycle. This oversight is intended not only to prevent harm, but also to uphold fundamental rights, safety, and democratic values, core priorities of the EU's approach to trustworthy AI. In this framework, human oversight serves as a final safeguard, ensuring that AI systems do not produce outcomes that conflict with legal or ethical norms, even when they function according to design.

Article 14 sets out several key obligations. Oversight measures must be commensurate with the

AI systems' autonomy, use context, and associated risks. Importantly, the Act does not impose a uniform standard but calls for "appropriate" human oversight tailored to the specific system.

Human operators must be enabled to understand the system's capabilities and limitations, monitor its performance, and, where necessary, override or discontinue its operation. These requirements reflect the broader principle of meaningful human control, which is operationalized through oversight models such as "human-in-the- loop" (HITL), where human input is required before the system can act, and "human- on-the-loop" (HOTL), where a human supervises the system and can intervene at any

time. [83]Oversight measures must be technically and organizationally robust enough to detect anomalies, prevent unsafe behavior, and ensure accountability throughout the AI system's operation.

The explanatory function of Recital 47 reinforces this requirement. It underscores the potential for serious harm in sectors where high-risk AI systems are integrated into products that affect health and safety, such as in healthcare diagnostics, manufacturing robots, or autonomous machinery. It stresses that oversight mechanisms must be capable of functioning in complex, real-world environments, and highlights the necessity for these systems to be reliable and accurate, particularly when their decisions significantly impact individuals' lives. Thus, Recital 47 not only contextualizes the human oversight requirement in terms of risk management and safety but also links it to the EU's product safety regime.

The effective implementation of human oversight requires a clear division of responsibilities between providers and deployers. Providers who develop and market the AI system must embed oversight mechanisms during the design and development phase. This involves integrating features such as interpretability tools, override functions, and user interfaces that facilitate informed human intervention. Article 29(4)(b) further obliges providers to supply comprehensive instructions for use that allow deployers to understand and implement oversight effectively.

Deployers, those who use the AI system in practice, must implement these mechanisms operationally. They are responsible for assigning oversight duties to qualified personnel, ensuring that these individuals are trained to understand the system's behavior, identify when intervention is necessary, and act decisively to mitigate risks. In doing so, the AI Act adopts a dual compliance model: oversight must be designed by the provider and exercised by the deployer, creating accountability at both the technological and operational levels.

A particularly important aspect of human oversight is its function in mitigating automation bias, the cognitive tendency to over-rely on AI system outputs without

[83] , *Article 14: Human Oversight | EU Artificial Intelligence Act*, [s.d.]consultabile su https://artificialin- telligenceact.eu/article/14/.

sufficient critical evaluation. This phenomenon can lead to unchallenged acceptance of flawed or discriminatory outputs, especially when operators do not fully grasp the AI's limitations. Article 14(4)(c) directly addresses this concern, requiring that oversight mechanisms equip humans to remain alert to automation bias, properly interpret outputs, and choose to override or disregard AI decisions when appropriate. Effective human oversight therefore demands not only the capacity to act, but also the competence and confidence to question the system's decisions. This requires ongoing training and awareness, particularly in contexts involving sensitive data or consequential decision-making.

Ultimately, the emphasis on human oversight and accountability within the AI Act reflects a fundamental regulatory objective: to ensure that AI remains subordinate to human judgment and legal standards, even in increasingly autonomous contexts. Oversight is not merely a safeguard against malfunction but a mechanism of democratic control over technologies that affect rights, safety, and social trust. By embedding human oversight as both a design requirement and an operational duty, the EU AI Act affirms that accountability cannot be delegated to machines.

The EU AI Act recognizes that regulation cannot end at the point of market placement or deployment. Instead, it mandates a system of post-market monitoring to ensure ongoing safety, reliability, and legal compliance of high-risk AI systems in real- world use. [84] As high-risk systems may evolve or interact with dynamic environments, the importance of surveillance beyond the development phase becomes clear. Article 72 of the AI Act forms the legal foundation for this phase, requiring providers to proactively collect, assess, and act on real-world data to identify and mitigate unforeseen risks. This is reinforced in Recital 81, which underscores the need for continuous compliance monitoring, especially in systems that incorporate adaptive learning or undergo modifications after deployment.

Article 72 introduces a comprehensive obligation for providers of high-risk AI systems to implement a structured post-market monitoring system. This includes the

[84] Cit.

establishment of a formal monitoring plan, which must be part of the system's technical documentation. Such a plan is expected to cover the collection and analysis of data relating to the performance, functionality, and safety of the AI system in actual operational contexts. It must incorporate inputs from

end-users, affected persons, and interconnected digital systems. This plan should be updated throughout the lifecycle of the AI system to ensure that compliance gaps or emerging risks are promptly addressed. The European Commission is set to provide a standardized template for this plan through an implementing act by February 2026, aiding providers in ensuring consistency and quality in surveillance activities. The goal is not only to catch performance drift or algorithmic bias but also to support corrective improvements and maintain alignment with fundamental rights.[85] Beyond surveillance, the AI Act establishes a parallel requirement for the formal reporting of serious incidents, as set out in Article 73. [86]These include malfunctions or unintended consequences of an AI system that may result in death, serious harm to health, significant disruption to critical infrastructure, or violations of fundamental rights, as defined under Article 49. These provisions mark a critical shift from optional or informal disclosures to a compulsory, timely reporting regime. Recital 82 emphasizes that such mechanisms are essential to ensure rapid intervention by market authorities and to safeguard public trust. This duty is central to the broader risk-based regulatory framework of the AI Act, which seeks not only to prevent harm but to foster accountability among AI providers.[87]

Providers must notify the appropriate market monitoring body of the Member State where a major occurrence occurs in accordance with Article 73. There are strict rules governing the timing of such reporting. Reporting of a death must happen right away and within ten days at the latest. The incident must be reported within two days if it involves widespread impairment of essential infrastructure. The timeframe is 15 days

[85] , *Article 73: Reporting of Serious Incidents | EU Artificial Intelligence Act*, cit.
[86] , *Article 49: Registration | EU Artificial Intelligence Act*, [s.d.]consultabile su https://artificialintelli- genceact.eu/article/49/.
[87] , *Article 73: Reporting of Serious Incidents | EU Artificial Intelligence Act*, cit.

following the provider's reasonable grounds for establishing a causal or likely link between the event and the AI system for any other major incidents. If necessary for prompt notice, preliminary reports with insufficient details may be filed, followed by a full report. Although providers are ultimately in charge, deployers are also supposed to notify providers of any irregularities or incidents they come across in real-world scenarios. [88]

Deployers may bring the issue up with authorities directly if providers do nothing. Furthermore, any natural or legal person has the right to file a complaint about any infractions of the AI Act, including unreported events, with the appropriate surveillance body under Article 85. Because of the structured ecosystem these tiered responsibilities provide for continuous oversight, authorities are able to respond quickly when systemic problems arise.

1.3 SANCTIONS FOR NON-COMPLIANCE CATEGORIES OF INFRINGEMENTS AND CORRESPONDING PENALTIES.

A risk-based framework is established under the EU Artificial Intelligence Act (AI Act), which is backed by a tier-based system of penalties for non-compliance under Article 99. Depending on the severity of the breach and the risk profile of the AI system, penalties might range from €7.5 million to €35 million, or up to 7% of global turnover. This strategy upholds the Act's dual goals of fostering innovation and defending basic liberties.

Sanctions apply not only to AI providers but also to actors across the entire AI lifecycle, including importers, distributors, and deployers. In addition to fines, the AI Act authorizes non-financial measures, such as market bans and suspension of CE certifications, which may have more immediate operational impact.

The Act does not rigidly classify violations but aligns penalties with its risk taxonomy: prohibited practices like social scoring attract the harshest fines, while procedural breaches, such as misinformation to regulators, are penalized less severely

[88] , *Article 85: Right to Lodge a Complaint with a Market Surveillance Authority | EU Artificial Intelligence Act*, [s.d.]consultabile su https://artificialintelligenceact.eu/article/85/.

but still taken seriously. Article 55(2) also requires that penalties remain proportionate, particularly for SMEs, which may lead to enforcement asymmetries.

Yet doubts remain about the regime's effectiveness. Large tech firms may absorb even the highest fines as costs of doing business, while Member States vary in enforcement capacity and willingness. As Philipp Hacker notes, enforcement is further weakened by fragmentation, as AI supervisory bodies often lack coordination with those responsible for liability and redress. This creates gaps especially when generative or high-risk AI systems cause harm but fall between regulatory regimes like the AI Act, GDPR, and liability directives.

Thus, while Article 99 lays the foundation for compliance, its real-world impact depends on effective enforcement. [89]The next section examines the institutional mechanisms responsible for carrying out these sanctions beginning with the EU AI Office and its coordination with national authorities.

Effective enforcement mechanisms are indispensable to the integrity of any regulatory framework, and the EU AI Act is no exception. While the Act outlines substantive obligations particularly for high-risk and general-purpose AI (GPAI) systems—its success ultimately depends on the strength and clarity of the institutional architecture responsible for oversight.

This architecture comprises both EU-level and national authorities, with the newly created EU AI Office positioned as the central coordinating body. However, enforcement is not monolithic: it varies according to the classification of AI systems (prohibited, high-risk, or GPAI), and particularly complex challenges arise in the supervision of GPAI models, which operate across jurisdictions and often exhibit systemic and unpredictable risks.[90]

In this context, coordinated enforcement, harmonized legal interpretation, and cross- border regulatory cooperation are essential not just to avoid inconsistent application of

[89] KARATHANASIS T., Guidance on Classification and Conformity Assessments for High-Risk AI Systems under EU AI Act, [s.d.].

[90] , *EU AI Act: first regulation on artificial intelligence*, cit.

the Act, but to prevent enforcement gaps that could be exploited by powerful actors or novel AI architectures.

1.3.2 ESTABLISHMENT AND MANDATE OF THE EU AI OFFICE

The European AI Office, formally established under the European Commission within DG CNECT, serves as the principal EU-level authority for implementing and supervising the AI Act. It holds a dual role: regulatory oversight and coordination, particularly in relation to GPAI systems, such as ChatGPT, Gemini, and other foundation models with transformative capabilities.

Pursuant to Article 101, the Office's mandate includes issuing implementing and delegated acts, conducting independent model evaluations, coordinating national authorities, and crucially imposing administrative sanctions. It also assumes a supervisory role in identifying and monitoring systemic GPAI risks, including models that may exert

cross-sectoral influence or pose threats to fundamental rights.

However, while the Office has broad authority on paper, questions remain about its institutional capacity. [91]It is unclear whether the Office has sufficient technical expertise, legal leverage, or operational independence to scrutinize complex proprietary systems, especially when dealing with powerful global AI providers.

1.3.3 SUPERVISORY POWERS AND ENFORCEMENT CAPABILITIES

The AI Office oversees compliance not only at the model level but, in cases where the same provider deploys user-facing applications, also at the application level.

Where GPAI models are embedded within high-risk systems, the Office must coordinate closely with national market surveillance authorities, who retain primary enforcement powers for sector-specific risks.

To streamline enforcement, the Office facilitates communication between sectoral regulators, maintains shared compliance databases, and provides strategic support to

[91] , *Article 101: Fines for Providers of General-Purpose AI Models | EU Artificial Intelligence Act*, [s.d.]consultabile su https://artificialintelligenceact.eu/article/101/.

Member States. It also plays a crucial role in cross-regulatory alignment particularly with bodies tasked with enforcing the Digital Services Act (DSA) and Digital Markets Act (DMA) ensuring an integrated governance approach where AI systems intersect with digital platform regulation.[92]

Yet despite its integrative ambitions, the Office's effectiveness may be hindered by jurisdictional overlaps, resource disparities among Member States, and the absence of a GDPR-style "one-stop-shop" mechanism for AI. These challenges raise concerns about fragmented oversight and regulatory uncertainty issues explored in subsequent sections.

1.3.4 MODEL EVALUATION AND SYSTEMIC RISK MITIGATION

A distinctive and increasingly consequential function of the EU AI Office lies in its authority to evaluate general-purpose AI (GPAI) models for systemic risks. This mandate reflects the EU's recognition that highly capable AI models, particularly foundation models deployed across multiple sectors, may pose unique challenges that transcend traditional product safety regulations.

To operationalize this responsibility, the Office develops standardized tools and benchmarks for assessing model capabilities, safety features, and risk profiles. When a GPAI model is suspected of posing systemic risk, whether due to scale, unpredictability, or societal impact, the Office may initiate a structured dialogue with the provider, request technical documentation, and undertake an independent evaluation. In theory, this may include source code analysis, though in practice, such assessments are likely to face significant technical and legal obstacles, particularly where proprietary technologies are involved.

If a model is found to violate the Act or fails to sufficiently mitigate identified risks, the AI Office has the power to impose corrective measures or even mandate the model's withdrawal from the EU market. However, this raises concerns about enforceability, especially in relation to global models not headquartered within the EU's jurisdiction.

[92] , *Article 28: Notifying Authorities | EU Artificial Intelligence Act*, cit.

Supporting this process is a Scientific Panel of Independent Experts, tasked with advising on evaluation methodologies, issuing alerts, and contributing to the classification of systemic models. While this advisory layer adds epistemic legitimacy to regulatory decision-making, questions remain about the institutional independence of the panel, the transparency of its alert procedures, and the legal status of its risk assessments. For example, it is unclear whether a panel-issued alert triggers mandatory enforcement or simply invites discretionary review by the AI Office.[93]

This function, the detection and containment of systemic risk, represents a fundamental test of the AI Office's capacity to balance innovation with safety. Yet its success will depend on whether technical ambition is matched by institutional resources, cross- border cooperation, and legal clarity. [94]These challenges are further magnified in the next section, which examines how enforcement is harmonized across the EU's fragmented regulatory landscape.

1.3.5 CODES OF PRACTICE AND INTERNATIONAL COOPERATION

Beyond direct enforcement, the AI Office seeks to foster compliance through the facilitation of voluntary codes of practice, developed in coordination with the AI Board and relevant stakeholders by 2025. These codes serve as interim benchmarks, offering guidance on regulatory expectations until formal European standards are adopted.

Providers that adhere to them benefit from a presumption of conformity, a feature particularly advantageous for small and medium-sized enterprises (SMEs) attempting to navigate complex technical and legal obligations.

While these voluntary instruments provide much-needed regulatory clarity, their effectiveness may vary in practice. As soft law tools, they lack binding force, and there

[93] , *The AI Office: What is it, and how does it work? | EU Artificial Intelligence Act*, [s.d.]consultabile su https://artificialintelligenceact.eu/the-ai-office-summary/.

[94] WACHTER, *Limitations and Loopholes in the EU AI Act and AI Liability Directives: What This Means for the European Union, the United States, and Beyond*, cit.

is a risk that larger AI developers may exert disproportionate influence over their content, potentially shaping standards that reflect industry convenience rather than public interest. Moreover, without systematic monitoring and enforcement mechanisms, codes of practice may struggle to ensure genuine accountability, especially in the context of high-impact, rapidly evolving AI applications.

If voluntary approaches fail to deliver sufficient levels of compliance, the AI Office retains the power to propose binding common specifications through implementing acts, effectively converting best practices into enforceable obligations. This dual-track strategy underscores the EU's broader regulatory logic: to encourage innovation through flexibility while retaining the option to harden soft law where necessary.[95]

At the international level, the AI Office plays a crucial diplomatic role, acting as the EU's external voice in global AI governance. It engages with multilateral institutions, fosters dialogue with GPAI developers, and facilitates knowledge-sharing across academia, civil society, and the open-source community. By promoting the EU's values-based approach to trustworthy AI, emphasizing fundamental rights, democratic accountability, and human oversight, the Office seeks to shape the global normative environment for AI regulation. Yet this ambition faces significant geopolitical challenges. Competing regulatory standards, particularly between the EU's precaution stance and the more market-oriented models in the U.S, and permissive environments in China, may limit the EU's influence. Whether the EU can assert leadership or merely function as a normative outlier will depend on its ability to align internal consistency with credible external engagement.[96]

As the AI Office extends its role from rulemaking to coordination and diplomacy, it also turns inward to promote experimentation and collaborative learning across Member States. The next section examines one such mechanism: regulatory sandboxes and institutional support structures aimed at enabling innovation while maintaining regulatory oversight.

[95] , *The AI Office: What is it, and how does it work? | EU Artificial Intelligence Act*, cit.
[96] Ibid.

1.3.6 COLLABORATION, SANDBOXES, AND SUPPORT FOR SMES

In pursuit of innovation-friendly regulation, the AI Office collaborates with Member State authorities to establish AI regulatory sandboxes as controlled environments where novel AI systems can be tested under regulatory supervision before full deployment. These sandboxes aim to lower compliance risks for providers, for instance, small and medium-sized enterprises (SMEs), by offering early feedback and fostering dialogue with regulators.

However, while regulatory sandboxes offer a promising model for experimentation and repetitive compliance, they also raise questions about regulatory consistency and legal certainty. Without clear baseline criteria or harmonized procedures, sandbox outcomes may vary significantly across Member States, potentially resulting in uneven application of the AI Act or the inadvertent creation of national-level loopholes. There is also the risk that sandboxes become a vehicle for regulatory capture if dominant actors influence sandbox agendas or disclosure remains opaque.

To address broader SME challenges, the AI Office also provides centralized resources, outreach campaigns, and explanatory materials aimed at simplifying the regulation's requirements. This support is critical in light of the disproportionate burden often faced by smaller providers, who may lack in-house legal and technical capacity to navigate the AI Act’s layered obligations. Still, questions remain about the effectiveness and reach of these initiatives, particularly in Member States with underdeveloped AI ecosystems or limited national-level regulatory expertise.

In sum, the AI Office is not merely an enforcement body but a coordinating hub, promoting harmonized implementation, mitigating systemic risks, and enabling regulatory experimentation. Its role is particularly salient in relation to Generative AI systems, whose global diffusion and rapid development test the limits of both traditional enforcement and regulatory foresight.

Yet no single institution can manage this complexity alone. As the next section explores, the success of the AI Act will depend on how effectively EU-level and

national authorities coordinate enforcement responsibilities across a fragmented and multi-level regulatory landscape. [97]

1.4 COORDINATED ENFORCEMENT IN PRACTICE: WHO DOES

WHAT?

The enforcement of the EU AI Act operates within a multi-level governance model, which manages both Union and national levels. This design portrays the international nature of AI development and integration, while acknowledging the necessity of the enforcement of optimized to sector-specific applications.

The core of this system has two primary actors: the EU AI Office, functioning under the control of the European Commission, and the national authorities assigned by each Member State. This model aims to bring a balanced centralized coordination within the normal local implementation, ensuring uniformity in the interpretation of the Act and context supervision.

The AI Office and national authorities operate under a similar logic of responsibilities that complement each other. The EU AI Office focuses primarily on general-purpose AI (GPAI) systems, mainly those expected to cause systemic or transnational threats. For the national bodies, they supervise high-risk AI systems marketed or used within their territories.

The AI Office takes the lead in implementing GPAI-related obligations, for instance, transparency, codes of conduct, and market surveillance for numerous foundation models. By contrast, national authorities serve as the first point of contact for providers and users. Their responsibilities include conducting compliance checks, responding to complaints, and imposing corrective measures to be initiated or penalties in case of breach of conduct.

This approach theoretically allows the EU to enhance the strategic management of the AI Office alongside the related expertise of Member States. However, it also displays

[97] *The AI Office: What is it, and how does it work? | EU Artificial Intelligence Act*, cit..

concerns about overlap, ambiguity, and regulatory divergence, especially when AI systems affect both national and Union-level domains. [98]

[99]Implementation of these regulations varies depending on the type of AI system integrated and the scale of risk it involves. For GPAI models with wide usage and systemic impact, the EU AI Office ensures consistency across borders. Inevitably, for AI systems used in sector-specific contexts, such as biometric surveillance, education, or the healthcare sector, the national authorities take primary responsibility.

In hybrid cases, where a GPAI model is integrated into a high-risk application, both governance levels may share regulatory implementation roles. These scenarios demand careful coordination to minimize conflicting assessments that could lead to regulatory uncertainty for providers and jeopardize the credibility of the framework that was initially effective. Given this structure, coordination is not optional; it is essential.

> Without coordination, there is a high risk of duplicated investigations, inconsistent interpretations of compliance obligations, and even conflicting sanctions being applied.

To minimize these setbacks, the AI Act establishes a series of coordination mechanisms, as listed below:

- Information exchange protocols between the EU and national authorities,
- Joint market surveillance initiatives, and lastly
- Provisions for the AI Office to support or intervene in national-level investigations.

These mechanisms are essential in the systemic GPAI models, where disjointed management could give the EU inevitable consequences. Though supervisors have noted the absence of a centralized enforcement structure specific to the GDPR's model, this might leave providers uncertain about which authority has the upper hand. [100] In a

[98] , *The AI Office: What is it, and how does it work? | EU Artificial Intelligence Act*, cit.

[99] G. J. – N. O. HALEEM – A. ZWITTER, *General-purpose AI regulation and the European Union AI Act*, 2024, p.

[100] J.) G. (OSKAR - HALEEM (NOMAN) - ZWITTER (ANDREJ), *General-purpose AI regulation and the European Union AI Act*, 2024consultabile su https://policyreview.info/articles/analysis/general- purpose-ai-regulation-and-ai-act.

like manner, the effectiveness of AI governance in Europe will depend on how successfully these multi-level deployers can operate as a connected regulatory ecosystem. [101]

Numerous AI systems, mainly those with a basis in machine learning and generative models, require large databases for supervision and training, many of which contain personal and sensitive information of users. With this fact being considered, these systems are placed at the intersection of two key regulatory frameworks: the EU Artificial Intelligence Act (AI Act) and the General Data Protection Regulation (GDPR). Hence, AI developers and strategists face a set of legal limitations that include the protection of individual rights and governance data.

National Data Protection Authorities (DPAs), for instance, France's CNIL or Germany's BfDI, ensure that personal data is processed lawfully, transparently, and with full respect for the rights of data owners. Meanwhile, under the AI Act, with reference to Article 10, providers of high-risk AI systems are subject to strict data governance qualifications, including mandates to ensure data quality, representativeness, and mitigation of errors. Where personal data is involved, these requirements must align with core GDPR principles such as lawfulness, data minimization, and purpose limitation.

The need for structured cooperation between AI regulators and DPAs is thus not merely procedural, it is foundational. Both sets of regulators must align their enforcement efforts to avoid regulatory duplication, conflicting interpretations, or legal uncertainty for providers. The AI Act acknowledges this coordination imperative in Recital 82, which encourages systematic cooperation and information-sharing among competent authorities.[102]

[101] , *European AI Office | Shaping Europe's digital future*, 2025consultabile su https://digital-strategy.ec.europa.eu/en/policies/ai-office.

[102] J.) V.V.AA., *General-purpose AI regulation and the European Union AI Act*, cit.

Yet, this coordination remains underdeveloped. No formal mechanism akin to the GDPR's one-stop-shop model exists for AI systems, leaving open the question of how conflicts between AI regulators and DPAs will be resolved in practice. Moreover, concerns persist regarding whether DPAs possess sufficient technical expertise to assess the risks and safety requirements unique to AI systems, particularly generative or autonomous models. This asymmetry may result in uneven enforcement or overreliance on procedural rather than substantive compliance. Consider, for example, a generative AI system deployed in education, designed to personalize learning based on student performance. Under the AI Act, such a system could be classified as high- risk due to its impact on access to education. Simultaneously, the system would fall under the GDPR due to its processing of sensitive personal data such as behavioral and demographic metrics. Ensuring lawful deployment in this context would require dual oversight: AI regulators to verify compliance with technical and human oversight requirements, and DPAs to assess legal bases for data processing and respect for data subject rights.

Without coordinated assessment protocols, providers risk being pulled in conflicting regulatory directions.

Ultimately, the intersection of the AI Act and GDPR reveals both the promise and peril of multi-framework enforcement. If properly aligned, the two regimes could mutually reinforce safety, accountability, and rights-based AI development. [103]But if left uncoordinated, they risk fragmenting compliance obligations and undermining legal clarity especially for smaller actors navigating limited resources. Future regulatory refinement may require clearer institutional mandates, formalized joint decision-making protocols, or the creation of integrated supervisory bodies capable of bridging the AI–data protection divide.

The Digital Services Act (DSA) is a component of the EU's comprehensive Digital Services Package that regulates online intermediary services and digital platforms. It

[103] , *Article 82: Compliant AI Systems Which Present a Risk | EU Artificial Intelligence Act*, [s.d.], p. 82consultabile su https://artificialintelligenceact.eu/article/82/.

places additional requirements on very large online platforms (VLOPs) and very large online search engines (VLOSEs). The legislation's main goal is to create a secure, open, and responsible digital space by addressing systemic challenges like illegal content distribution, false information, and deceptive recommendation algorithms.

The DSA establishes a tiered governance framework that combines national oversight through Digital Services Coordinators with European Union-wide coordination managed by the European Commission and the European Board for Digital Services. Major platforms must perform risk evaluations, develop risk reduction measures, and maintain transparency in their algorithms, which includes undergoing independent auditing processes as outlined in Articles 26-27 of the DSA.[104] With the increasing integration of Generative AI tools, for instance, chatbots, content generators, and automated moderation systems into platform operations, the regulatory boundaries between the DSA and AI Act are increasingly blurred. These AI-powered services may influence user experiences, amplify disinformation, or generate potentially illegal content. For example, a generative AI model deployed on a social media platform could autonomously create and disseminate manipulated political narratives on a scale.[105]

In such cases, both the AI provider and the hosting platform bear overlapping regulatory responsibilities: the former under the AI Act's provisions for high-risk or general-purpose AI systems, and the latter under the DSA's obligations for systemic risk management and content governance. This creates a shared enforcement space, requiring cooperation between AI regulators and DSA authorities.

Effective coordination is vital to avoid fragmented or duplicative enforcement. Without it, overlapping mandates could lead to regulatory uncertainty or gaps in oversight, particularly in response to cross-border harms originating from AI-driven

[104] QUINTAIS J. P. - S. F. SCHWEMER, The Interplay between the Digital Services Act and Sector Regulation: How Special Is Copyright? | European Journal of Risk Regulation, *Cambridge core*, [s.d.].

[105] , *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS*, 2021.

platform activities. [106] The AI Act and DSA embody complementary logics: the former is technology-focused, classifying systems based on their risk level; the latter is platform-centric, targeting the influence of digital intermediaries on public discourse and individual rights.

Together, these frameworks have the potential to create a comprehensive and adaptive oversight model but only if they are operationalized through joint risk assessments, shared enforcement strategies, and consistent transparency standards. Formal cooperation mechanisms, such as inter-agency working groups or integrated audits, may become increasingly necessary as Generative AI becomes central to platform governance.

CONCLUSION: TOWARD COORDINATED AND EFFECTIVE AI GOVERNANCE

The European Union's artificial intelligence governance is organized around a multi- level, multi-actor regulatory ecosystem that reflects the cross-sectoral reach and diversity of AI technology. The EU AI Office, which serves as the primary moderator at the Union level, national AI competent authorities, which are in charge of localized supervision and enforcement, Data Protection Authorities (DPAs), which are in charge of upholding the privacy protections of the GDPR, and Digital Services Act (DSA) regulators, who are tasked with lowering systemic risks associated with online platforms and search engines, form the foundation of this framework.

These institutions operate together under a collection of connecting legal instruments, including the AI Act, GDPR, DSA, and the capability of the AI Liability Directive (AILD) and Product Liability Directive (PLD), together forming the backbone of the EU’s AI governance outlook.

[106] Cit.

Nonetheless, legal architecture alone is insufficient. Achieving effective, rights- respecting, and Innovation-supportive AI governance inevitably depends on how well these institutions coordinate their mandates, interpret shared roles, and execute aligned oversight procedures.

The AI Act's tried restrictions regime, voluntary codes of practice, regulatory sandboxes, and joint enforcement mechanisms have a common goal of creating this cohesion. But the efficient test lies in operating these tools in a fragmented regulatory environment, complying with the oversight of Generative AI systems, whose rapid advancement and transnational deployment stretch the limits of traditional compliance and enforcement structures.

Coordinating challenges are usually insignificant where the legal mandates interconnect, for instance, between AI regulators and DPAs, or between the AI Office and DSA regulators. Lack of structured cooperation will lead to fabricated investigations, conflicts in compliance demands, and exposure of regulatory gaps, inevitably around algorithmic accountability and AI-generated content. The AI Act's call for cooperation, expressed in the mechanisms of numerous procedures, shared databases, and coordinated monitoring efforts, is an essential first step, though its success will depend on the political will, technical capacity, and legal clarity, all embracing inter-agency collaboration.

Three priorities are mandatory going forward. First, the harmonization of enforcement practices across Member States will be essential to ensure legal certainty for providers and prevent regulatory arbitrage. Second, capacity building, especially for national authorities and DPAs, for instance, technical training, access to AI auditing tools, and financial resourcing. Third, clear liability rules and mechanisms must be finalized through compliance initiatives, for instance, the AILD and PLD, ensuring meaningful accountability for the harm that AI systems might cause.

Inevitably, the long-term effectiveness of the EU's AI regulatory model depends not only on the potential of its rules but also on the institutional union and the integration procedures for its enforcement bodies. Mitigating the governance challenges as a result of using Generative AI and other transformative technologies will require adaptive management strategies and a shared commitment to democratic values regarding technological responsibility.

This governance perspective sets the stage for the next chapter, which shifts the focus from institutional coordination to practical compliance strategies for businesses. Chapter 2 examines how generative AI is being used in real-world operations, the permitted and prohibited practices with reference to the AI Act, and the tools and frameworks companies should adopt to meet the Regulation's requirements while maintaining their innovation.

CHAPTER 2 Using Generative AI in Business Activity - Limitations and Compliance Requirements

Building on the legal framework and formal obligations introduced in Chapter 1, this chapter critically examines how the EU AI Act's risk classification system functions when applied by firms in real-world decision-making contexts. While the Act's structure identifies high-risk AI as a regulatory priority, businesses must interpret and implement this categorization within the constraints of their internal resources, organizational size, and sectoral realities. This chapter explores how these practical limitations create friction between regulatory intent and actual compliance behavior.

2.1 PERMITTED AND PROHIBITED PRACTICES

2.1.1 INTERPRETING THE AI ACT FROM A BUSINESS PERSPECTIVE: APPLYING THE RISK CLASSIFICATION SYSTEM IN COMPLIANCE POLICIES

From a business compliance perspective, the EU Artificial Intelligence Act's risk classification system functions as a structural anchor for assigning regulatory obligations. It requires companies to classify their AI systems as prohibited, high-risk, limited-risk, or minimal-risk based on their intended purpose and context of use. However, despite its conceptual clarity, the classification framework poses significant

implementation challenges, particularly when applied within dynamic technological and organizational settings.

At the conceptual level, the risk-based approach appears rational: the higher the potential harm posed by an AI system, the more stringent the regulatory requirements. This model draws inspiration from product safety regulation, but it is poorly adapted to the mutable and context-sensitive nature of AI systems. Many modern AI technologies, especially generative and adaptive models exhibit emergent or downstream effects that are difficult to anticipate or measure in advance. This undermines the core assumption that risks can be defined ex ante and managed through static classification. The historical application of risk-based frameworks to stable, physical products does not seamlessly translate to AI, where behavior often evolves post-deployment and in interaction with complex environments. [107]

Although the AI Act presents itself as technologically neutral, its structure reveals selective regulatory priorities. Certain applications, such as real-time biometric identification or emotion recognition, are either explicitly prohibited or subject to heightened regulatory control. This creates asymmetries in compliance incentives: companies are steered toward developing low-risk applications, not necessarily because they are more beneficial or ethically sound, but because they are easier and less costly to bring to market. As such, claims of neutrality conceal a regulatory posture that may inadvertently suppress innovation in high-impact sectors such as healthcare, education, or adaptive user-facing technologies areas where both risks and benefits are significant but difficult to quantify in advance.

Moreover, the AI Act applies uniformly across organizations regardless of size, assuming a baseline capacity for compliance that many firms, particularly SMEs do not possess. Risk assessments, audit trails, and documentation obligations impose disproportionate burdens on firms with limited legal or technical infrastructure. In

[107] B. M. CABRERA et al., *The Artificial Intelligence Act: Insights Regarding Its Application and Implications*, in *Procedia Computer Science*, CENTERIS - International Conference on ENTERprise Information Systems / ProjMAN - International Conference on Project MANagement / HCist - International Conference on Health and Social Care Information Systems and Technologies, vol. 256, gennaio 2025, pp. 230–237.

practice, this has led some smaller companies to delay product launches, avoid high- risk categories altogether, or exit the EU market. Uniform legal obligations thus produce unequal economic outcomes, raising questions of structural fairness. Without flexibility based on organizational capacity or risk exposure, the regulation risks creating barriers to entry and chilling effects on smaller market players.

Part of the issue lies in the horizontal structure of the regulation itself. Designed to be cross-sectoral, the Act uses generic and often ambiguous risk criteria to apply across diverse domains. For example, the high-risk designation hinges on inclusion in Annex III, which identifies sensitive sectors such as employment, education, and critical infrastructure but it does not always clearly define functionalities or deployment contexts. [108]This ambiguity opens the door to both overinclusion of benign systems and underinclusion of genuinely hazardous ones. In particular, data-intensive applications like algorithmic advertising or personalized recommender systems may escape classification even when their societal impacts are substantial. This broad and imprecise approach undermines legal certainty and complicates business decision- making.

Compounding the ambiguity is the vagueness of key definitions within the regulation. The criteria used to classify AI systems often lack technical specificity, making it difficult for organizations to know with confidence whether they fall under the regulation's scope. In some cases, this vagueness has led to overcompliance, where companies implement burdensome controls out of caution, or undercompliance, where systems with significant societal impact fall through regulatory gaps.[109] Particularly in sectors like digital marketing, where AI applications do not easily map onto predefined risk categories, organizations face a paradox: act too cautiously and risk inefficiency, or interpret narrowly and risk future penalties.

[108] EUROPEAN COMMISSION, *Proposal for a Regulation Laying down Harmonised Rules on Artificial Intelligence*, Bruxelles, 2025, p.

[109] EUROPEAN COMMISSION, *Proposal for a Regulation Laying down Harmonised Rules on Artificial Intelligence*, Bruxelles, 2025, p.

Given these shortcomings, guidance alone will likely be insufficient to close the gap between legal design and organizational practice. [110] What is needed is a broader regulatory reconfiguration. One proposal involves shifting away from generic annexes and toward sector-specific risk assessment frameworks. [111]These would enable regulators and firms to better align classification with the real-world use cases, technological affordances, and data ecosystems of each industry. A more tailored approach would reduce interpretive ambiguity and allow for meaningful calibration of compliance efforts.[112]

In addition to tailored frameworks, the promotion of regulatory sandboxes presents another viable path forward. Sandboxes allow companies particularly SMEs to test AI systems under controlled conditions with supervisory support, reducing the immediate risk of liability while facilitating regulatory learning. This not only aids compliance but also improves the quality of AI governance by exposing systems to scrutiny earlier in their lifecycle. Moreover, it helps address resource asymmetries by offering smaller firms a pathway to safe experimentation and iterative risk management.

Beyond technical risk assessments, a complementary evaluative lens based on societal impact could offer a more holistic regulatory approach. Rather than focusing solely on the probability and severity of harm, impact-based metrics would account for broader ethical considerations, including social benefit, user empowerment, and distributive justice. Such metrics would help ensure that AI systems with high social value despite potential risk are not automatically excluded from the market due to rigid classification criteria.[113] This would also incentivize firms to design systems not only to avoid harm but to promote societal good.

Another structural limitation in the current framework concerns liability. While the Act emphasizes ex ante obligations such as documentation, risk management, and

[110] Ibid

[111] Ibid

[112] D. KRAUSE, *Implications of the EU AI Act for U.S. Regulatory Strategy and Corporate Risk Management*, SSRN Scholarly Paper 5247258, Social Science Research Network, novembre 2024, p. 25.

[113] Ibid

transparency, it is less clear about the consequences of non-compliance and the extent to which good-faith efforts mitigate liability exposure.[114] The lack of an explicit safe harbor mechanism leaves companies in a legal grey zone: even full compliance may not insulate them from responsibility in the event of harm. This uncertainty can discourage firms from taking proactive steps to embed ethical AI principles or experiment with new governance models. [115]By contrast, offering liability relief to firms that demonstrably comply with key obligations could encourage investment in robust internal compliance infrastructures and foster a culture of anticipatory governance.

In summary, the AI Act's risk classification model introduces a necessary regulatory scaffold, but its operational limitations hinder effective implementation particularly for smaller firms and emergent technologies. Ambiguities in risk categories, uneven compliance burdens, and gaps in sectoral applicability highlight the need for a more adaptive and context-sensitive approach. Sector-specific risk frameworks, sandbox environments, impact-based evaluation, and liability clarity are promising avenues for improving regulatory precision and fairness. Without such reforms, the current structure risks entrenching compliance asymmetries and stifling innovation where it may be most needed.

Evaluating Rights and Privacy Protections: Comparative Analysis and Corporate Implications

Risk-based evaluation procedures are incorporated into both the GDPR and the AI Act to protect basic rights in the context of data-driven technology. Data Protection Impact Assessments (DPIAs) are required under Article 35 GDPR for processing procedures that are "likely to result in a high risk" to the liberties and rights of natural persons. Concurrently, the AI Act mandates that companies that use high-risk AI systems as specified in Article 6 and Annex III conduct Fundamental Rights Impact Assessments

[114]J. S. BUTT, *Analytical Study of the World's First EU Artificial Intelligence (AI) Act, 2024*, in *International Journal of Research Publication and Reviews*, 5(3) (2024), pp. 7343–7364.

[115] P. HACKER, *The European AI Liability Directives – Critique of a Half-Hearted Approach and Lessons for the Future*, in *Computer Law & Security Review*, 51 (novembre 2023), art. 105871.

(FRIAs); Recital 42 emphasizes the importance of this procedure. Although both tools have an ex ante, preventive focus, their scopes are different: FRIAs are system- and rights-centric, while DPIAs are data-centric. The question of whether these responsibilities are complimentary or redundant, as well as the implications for companies using AI technologies, is brought up by their coexistence.

Article 35 GDPR mandates a DPIA whenever processing is likely to create high risks, such as large-scale monitoring, use of special category data, or automated decision- making falling under Article 22. A DPIA requires controllers to describe the processing, assess its necessity and proportionality, identify risks to rights and freedoms, and define mitigation measures. It is designed to ensure that data protection safeguards are embedded into system design before deployment. [116]

The AI Act's FRIA builds on this model but extends beyond data protection. Deployers of high-risk AI must assess risks to fundamental rights broadly, including equality, non-discrimination, and societal impacts of AI systems. Article 27 specifies that the FRIA should identify affected groups, governance arrangements, and mitigation strategies. While DPIAs focus on data minimization, legal bases, and consent, FRIAs scrutinize system-level risks such as bias, explainability, or systemic discrimination. Article 27(4) AI Act explicitly allows reuse of DPIA results for FRIA purposes, signaling a potential path to coordination.

Scholars emphasize both the overlap and divergence between DPIAs and FRIAs. Beltrán (2025) frames them as connected assessments: DPIAs map data protection risks, while FRIAs broaden the lens to systemic harms. Together, they offer a fuller picture of risks, but their simultaneous application increases compliance burdens in a multi-layered regulatory environment (GDPR, AI Act, DSA, CRA).[117]

---

[116] , *(PDF) The General Data Protection Regulation of 2016 (GDPR) Meets its Sibling the Artificial Intelligence Act of 2024: A Power Couple, or a Clash of Titans?*, su *ResearchGate*, [s.d.]consultabile su https://www.researchgate.net/publication/384682777_The_General_Data_Protection_Regulation_of_2 016_GDPR_Meets_its_Sibling_the_Artificial_Intelligence_Act_of_2024_A_Power_Couple_or_a _Cla sh_of_Titans.

[117] , *(PDF) Regulatory and Compliance Requirements for SMEs Operating AI Systems through Data Centers in the EU, with a Focus on Data Protection Challenges in Germany*, [s.d.]consultabile su https://www.researchgate.net/publication/389263846_Regulatory_and_Compliance_Requirements

_for

In a similar vein, Pakuhinezhad and Afsham (2025) contend that FRIAs and DPIAs interlock rather than duplicate. They consider FRIA as complimentary because it captures broader dangers to basic rights, and they characterize DPIAs as developing into "Algorithmic Impact Assessments" by incorporating prejudice and fairness. According to their findings, compliance can be reframed as a tactical instrument to increase competitiveness and trust.

Rintamäki et al. (2025) document severe fragmentation in DPIA practices: [118] across the EU, 106 different national conditions exist, creating legal uncertainty and inconsistent triggers. They highlight that most Annex III high-risk AI categories under the AI Act also involve personal data, requiring both a DPIA and a FRIA. To avoid duplication, they advocate harmonisation, where DPIAs feed into FRIA obligations.

Rintamäki and his co-authors (2025) analyse the overlap between the GDPR's Data Protection Impact Assessment (Article 35) and the AI Act's Fundamental Rights Impact Assessment (Article 27) [119]. Their central claim is that these two obligations cannot be understood separately, because most high-risk AI systems in Annex III of the AI Act also process personal data, automatically triggering a DPIA under the GDPR.

The authors explain that the GDPR is data-centric, assessing risks from the collection and processing of personal data. The AI Act is system-centric, examining whether the design and deployment of an AI system creates risks to equality, non-discrimination, due process, or other fundamental rights. Together, they impose a dual obligation on businesses

Their analysis does not rest on one litigated case but on regulatory practice. They document 106 different national conditions for DPIAs across the EU and EEA. This fragmented landscape shows how national authorities have expanded GDPR duties,

---

_SMEs_Operating_AI_Systems_through_Data_Centers_in_the_EU_with_a_Focus_on_Data_Protectio n_Challenges_in_Germany.

[118] RINTAMÄKI T., GOLPAYEGANI D., LEWIS D., CELESTE E., PANDIT H. J., *Impact Assessment*
Requirements in the GDPR vs the AI Act: Overlaps, Divergence, and Implications, 19 maggio 2025, p. 12.

[119] Ibid

leading to inconsistent triggers. A form of biometric monitoring or credit scoring may always require a DPIA in one Member State but not in another. This "gold-plating" creates legal uncertainty for cross-border AI deployment

The problem intensifies when layered with the AI Act. Annex III classifies credit scoring, biometric identification, and recruitment as high-risk, requiring a FRIA under Article 27. Since these activities almost always involve personal data, businesses must perform both a DPIA and a FRIA.[120] Article **22** GDPR on automated decision-making reinforces this overlap, as the same activities trigger obligations under all three provisions.

The authors argue that duplication is not inevitable. Article 27(4) AI Act allows DPIA results to be reused for FRIA purposes. They call for coordination between the European Data Protection Board and the AI Office to harmonise methodologies. Without such guidance, firms face fragmented obligations, duplication of effort, and forum shopping. With harmonisation, businesses could integrate the two assessments, lowering costs while meeting both data protection and fundamental rights standards. Grafenstein (2022) conceptualises DPIAs as regulatory coordination tools that integrate legal, organisational, and technical safeguards. He argues that DPIAs should not be siloed from FRIAs; rather, DPIA findings on privacy and lawful basis should flow into FRIA assessments on bias, discrimination, and systemic impacts. [121]This would transform compliance from a purely legal risk management exercise into a strategic governance mechanism.

Finally, Pandit and Rintamäki (2024) focus on practical solutions, proposing automated FRIA tools that reuse DPIA outputs. They argue this could reduce duplication, streamline compliance for SMEs, and make assessments scalable. Their approach demonstrates how technical innovation in compliance processes can address regulatory burdens.[122]

---

[120] *The General Data Protection Regulation of 2016 (GDPR) Meets its Sibling the Artificial Intelligence Act of 2024: A Power Couple, or a Clash of Titans,* cit.

[121] Ibid

[122] , *Artificial Intelligence in Business Law: Navigating Regulation, Ethics, and Governance - Journals*

- *Master Educational Services, Vasant Vihar, Delhi,* [s.d.]consultabile su

For businesses deploying AI, the coexistence of DPIA and FRIA obligations has significant implications. On one hand, duplication of assessments increases costs, requires expertise, and risks inconsistent obligations across Member States. SMEs are particularly affected by these burdens. Fragmentation in DPIA practice adds further uncertainty, creating the possibility of forum shopping and regulatory arbitrage.[123]

On the other hand, synergies exist. Experience with DPIAs under the GDPR provides a foundation for FRIAs, and the AI Act explicitly permits reuse of DPIA results. Firms that integrate compliance into design processes can transform these obligations into a trust-building mechanism, gaining market access and competitive advantage. Examples such as Microsoft's federated learning or Apple's on-device processing illustrate how privacy- and ethics-by-design approaches can turn regulatory compliance into a strategic differentiator.

DPIAs under Article 35 GDPR and FRIAs under Article 27 AI Act represent parallel but connected accountability tools. Both are grounded in ex ante, risk-based governance, but diverge in scope: [124] DPIAs focus on personal data risks, while FRIAs capture systemic fundamental rights impacts. The literature shows agreement that harmonisation is necessary to avoid duplication and fragmentation. Without it, businesses face high compliance costs and legal uncertainty. With it, integrated assessments could streamline obligations and strengthen governance.

For businesses, especially those deploying generative AI in decision-making, these obligations are both burdensome and strategic.[125] They increase upfront costs but can also be leveraged to build trust, secure contracts, and sustain innovation in the EU market.

---

https://www.nationaleducationservices.org/artificial-intelligence-in-business-law-navigat ing- regulation-ethics-and-governance/pid-2228133310.

[123] J.) V.V.AA., *General-purpose AI regulation and the European Union AI Act*, cit.

[124] IJSR - International Journal of Scientific Research, *GDPR And AI-Driven Business Models: Navigating Legal Risks Through A Legal Analysis Framework*, IJSR, n.d., accessed September 13, 2025, https://www.worldwidejournals.com/article/gdpr-and-ai-driven-business-models

[125] Ibid.

2.1.2. LEGAL UNCERTAINTY AND RISK-AVERSE BEHAVIOR

Despite the EU Artificial Intelligence Act's goal of harmonizing AI governance, the legislation has introduced legal ambiguities that challenge businesses' ability to accurately classify and manage risk. Central to this uncertainty is the requirement for providers to self-categorize AI systems across four tiers prohibited, high-risk, limited- risk, and minimal-risk often without sufficient sectoral examples, definitions, or interpretive guidance. In practice, many organizations, especially small and medium- sized enterprises (SMEs), respond to this lack of clarity with defensive overcompliance, classifying their systems as high-risk even when this designation is not strictly required.

This cautious behavior stems from the Act's structural design. It imposes a lifecycle compliance obligation that requires continuous risk assessment and mitigation from design through deployment to post-market monitoring. For many companies, particularly SMEs, the technical and legal demands of anticipating potential harms to health, safety, and fundamental rights can be prohibitive. The difficulty intensifies when dealing with general-purpose AI (GPAI) systems, whose modular and cross- sectoral deployment resists clear-cut regulatory classification. Given the absence of adaptive tools or sectoral guidance, companies are often deterred from innovating in ambiguous or sensitive domains. This contributes to a tendency toward regulatory overreach: firms voluntarily adopt burdensome compliance strategies, postpone product launches, or avoid certain markets altogether.

Such precautionary strategies impose measurable costs. Many firms resort to ISO-aligned compliance models, scenario-based simulations, and structured documentation regimes, which demand considerable technical expertise and time. [126]These efforts

[126] J. S. BUTT, *Analytical Study of the World's First EU Artificial Intelligence (AI) Act, 2024*, in *International Journal of Research Publication and Reviews*, 5(3) (2024), pp. 7343–7364.

disproportionately affect SMEs, which often operate without in-house legal teams or regulatory experts. Uniform obligations across all provider types exacerbate these burdens, placing small firms at a competitive disadvantage due to limited risk absorption capacity. In high-stakes sectors such as healthcare or education, the result is frequently reduced participation by smaller providers.[127]

The AI Act's provider-led classification system also creates internal tensions. Technical teams often perform system assessments, yet legal accountability remains centralized within corporate leadership. This diffusion of responsibility can slow internal decision-making, complicate classification outcomes, and introduce friction across compliance, legal, and product teams. In many organizations, disagreements over classification thresholds result in delays and heightened strategic caution.

The lack of regulatory precision may also foster a procedural approach to compliance where checklists and documentation substitute for contextual analysis or ethical deliberation. Over time, this "tick-box" mindset risks diminishing the broader goals of the AI Act, which include safeguarding fundamental rights and promoting trust. Without clarity on classification boundaries, the distinction between regulatory formality and substantive risk mitigation becomes blurred. [128]This can weaken both compliance effectiveness and public trust in AI governance.[129]

In sum, the legal ambiguity embedded in the AI Act encourages risk-averse behavior, especially among resource-constrained firms. While large organizations may absorb the costs of overcompliance, SMEs are more likely to limit market engagement, consolidate operations, or avoid high-risk applications. Without clearer interpretive guidance, flexible exemptions, or mechanisms such as regulatory sandboxes, these dynamics may entrench existing asymmetries in AI innovation and discourage the development of socially beneficial systems.

[127] Ibid

[128] Ibid

[129] J. S. BUTT, *Analytical Study of the World's First EU Artificial Intelligence (AI) Act, 2024*, in *International Journal of Research Publication and Reviews*, 5(3) (2024), pp. 7343–7364.

Conflicts Between the GDPR and the AI Act: Legal Uncertainty and Business Implications

The General Data Protection Regulation (GDPR) and the Artificial Intelligence Act (AI Act) are the central pillars of the EU's digital regulatory framework. Both aim to safeguard fundamental rights in the use of data-driven technologies, but they do so in different ways. [130]

The GDPR, particularly Article 22, restricts automated decision-making, including profiling, where such decisions have legal or similarly significant effects. [131] It grants safeguards such as the right to human intervention, to express a viewpoint, and to contest decisions.

The AI Act, by contrast, introduces a sector-specific, risk-based governance model for artificial intelligence. It focuses on high-risk systems in fields such as credit, employment, and healthcare. Its provisions require conformity assessments, transparency duties, and under Article 86, an explicit right to explanation for high-risk applications.

A broad baseline is established by GDPR Article 22. Unless certain requirements are met, such as express approval, contractual necessity, or legal authorization, it forbids making judgments that are entirely automated but have substantial consequences. Controllers must put protections in place to protect individual rights even in these situations.

Case law has reaffirmed this vast reach. Because banks relied on credit ratings nearly exclusively, SCHUFA (CJEU, 2023) classified credit scoring as a decision under Article 22. As demonstrated in the cases of Uber and Ola, Dutch courts have also expanded the protections of Article 22 to gig economy platforms. These decisions forced businesses to disclose how algorithms assign tasks or end agreements. The dangers of opacity and mistake are further demonstrated by the Dutch childcare fraud

[130] , *(PDF) The General Data Protection Regulation of 2016 (GDPR) Meets its Sibling the Artificial Intelligence Act of 2024: A Power Couple, or a Clash of Titans?*, cit.
[131] Ibid

incident. Due to faulty automated assessments, families were falsely accused of fraud, illustrating the serious repercussions of insufficient safeguards.[132]

The AI Act narrows its focus to high-risk AI systems defined in Annex III. It requires fundamental rights impact assessments (FRIAs), human oversight, and documentation obligations. Article 86 introduces an explicit right to explanation but limits it to high- risk use cases. Unlike the GDPR, which applies broadly to personal data processing, the AI Act regulates only systems that meet its risk classification thresholds, leaving gaps where other AI applications may escape designation.

Scholars disagree on whether the two regimes form a coherent system or create fragmentation. Butt (2024) describes GDPR and the AI Act as "siblings" [133] that may either complement or clash. While both adopt a risk-based approach and reinforce rights, duplication of compliance instruments, such as the GDPR's Data Protection Impact Assessment (DPIA) and the AI Act's FRIA, risks inefficiency and confusion Rintamäki et al. (2025) emphasize that harmonization between these instruments is essential, otherwise businesses face duplicated costs and fragmented enforcement.

Others, such as Pakuhinezad and Afsham (2025), view the GDPR not as a barrier but as a minimum ethical baseline and even a strategic advantage. From this perspective, Article 22 safeguards and privacy-by-design obligations enhance trust and can be leveraged competitively in business practice. [134]Beltrán (2025) situates GDPR and the AI Act within a wider "digital acquis" alongside the Digital Services Act (DSA) and Cyber Resilience Act (CRA), arguing that their integration is necessary to avoid inconsistencies in multi-layered obligations.

Moreover, there is uncertainty. Saving (2025) underlines that both instruments rely on ex ante, risk-based compliance, shifting disputes away from private contractual allocation to mandatory regulatory conformity. This creates strategic ambiguity: firms

---

[132] J.) V.V.AA., *General-purpose AI regulation and the European Union AI Act*, cit.

[133] , *Scores as Decisions? Article 22 GDPR and the Judgment of the CJEU in SCHUFA Holding (Scoring) in the Labour Context | Industrial Law Journal | Oxford Academic*, [s.d.]consultabile su https://academic.oup.com/ilj/article/53/4/840/7745471.

[134] , *(PDF) The General Data Protection Regulation of 2016 (GDPR) Meets its Sibling the Artificial Intelligence Act of 2024: A Power Couple, or a Clash of Titans?*, cit.

cannot always predict whether datasets or models will be lawful until regulators or courts intervene. Metikoš and Ausloos (2025) highlight fragmentation in the right to explanation: GDPR case law has expanded this safeguard, while the AI Act codifies it more narrowly, risking loopholes but also ensuring convergence over time.[135]

Case law shows the practical consequences of these overlaps. In *SCHUFA*, the Court's broad interpretation of Article 22 imposed obligations not only on the banks using credit scores but also on the scoring agency itself. In the *Uber* litigation, courts extended Article 22 safeguards to gig workers, obliging platforms to provide transparency in algorithmic management. The Dutch childcare fraud case illustrates the severe harms that result from inadequate oversight. These cases show the GDPR's expansive force in shaping AI governance even before the AI Act enters into force. At the same time, businesses contracting for AI services face limits: as Savin notes, contractual clauses cannot exclude overriding EU compliance duties, echoing earlier disputes such as *Schrems II* on data transfers.[136]

For businesses deploying generative AI, these overlapping regimes create both compliance burdens and strategic opportunities. Duplication of assessments (DPIA and FRIA) increases costs, especially for SMEs. Fragmented enforcement across data protection authorities and AI regulators exacerbates uncertainty. At the same time, firms that embrace compliance as a trust-building mechanism may gain competitive advantage, as seen in industries where contractual partners demand GDPR and AI Act compliance as prerequisites. The shift toward ex ante, risk-based duties means businesses must integrate compliance into product design and corporate strategy from the outset.

The interaction of the GDPR and the AI Act creates both alignment and conflict. Article 22 GDPR provides broad, individual-focused safeguards, while the AI Act

[135] P. HACKER, *The European AI Liability Directives – Critique of a Half-Hearted Approach and Lessons for the Future*, in *Computer Law & Security Review*, 51 (novembre 2023), art. 105871.
[136] S. WACHTER et al., *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation*, in *International Data Privacy Law*, 7(2) (2017), pp. 76–99.

introduces sectoral, risk-based obligations.[137] Their overlap generates legal uncertainty through duplication, fragmented enforcement, and evolving interpretations. Cases such as *SCHUFA* and *Uber* illustrate how courts extend GDPR protections, setting precedents for AI Act application. For businesses, the result is a complex compliance environment: burdensome yet unavoidable, but also capable of fostering trust and competitive advantage if integrated strategically into governance.

Deepening the Analysis of SCHUFA and Uber

The SCHUFA and Uber judgments mark a significant expansion of GDPR Article 22, turning it into a central tool for regulating algorithmic decision-making in business contexts. Both cases show how courts are unwilling to accept corporate arguments that automated scores or flags are "just data" [138] rather than binding decisions.

In SCHUFA, the CJEU held that credit scores must be treated as "decisions" under Article 22 when banks rely almost exclusively on them (paras 30–33, Case C-634/21). This closed a loophole that would have allowed responsibility to rest only with banks, leaving credit agencies outside the law (Caruana 2025). [139]

Informational rights under Articles 13–15 GDPR, such as the right to an explanation of logic, therefore apply to scoring itself, not only the final lending decision. This reframes Article 22 as a proactive accountability mechanism, reinforcing Recital 71 GDPR's warning about opacity and discrimination (Aza 2024).[140]

The implications are wide. Credit agencies and employers must treat score generation as a regulated act. Human oversight, contestation rights, and explanation duties must be built in. The Advocate General stressed that trade secrets cannot trump fundamental

---

[137] , *(PDF) The General Data Protection Regulation of 2016 (GDPR) Meets its Sibling the Artificial Intelligence Act of 2024: A Power Couple, or a Clash of Titans?*, cit.

[138] , *Scores as Decisions? Article 22 GDPR and the Judgment of the CJEU in SCHUFA Holding (Scoring) in the Labour Context | Industrial Law Journal | Oxford Academic*, cit.

[139] Ibid

[140] , *A Sandbox Approach to Regulating High-Risk Artificial Intelligence Applications | European Journal of Risk Regulation | Cambridge Core*, [s.d.]consultabile su https://www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/sandbox-approach-to-regulating-highrisk-artificial-intelligence-applications/C350EADFB379465E7F4A95B973A4977D.

rights: individuals must at least be told the main factors and their weightings (Aza 2024). The ruling also reaches labor markets. A generative AI system producing suitability scores for job candidates, if relied upon exclusively, would count as a decision under Article 22 and trigger safeguards.[141]

Uber litigation extends this reasoning. Dutch courts found that automated driver deactivations triggered by fraud-detection algorithms fall within Article 22(1), as they directly affect work and income. Minimal human checks did not satisfy the safeguard requirement; only genuine oversight suffices (Davis & Schwemer 2023). Like SCHUFA, the case shows that courts reject attempts to fragment accountability by labelling algorithmic outputs as neutral data points.[142]

The business consequences are serious. Uber had to provide drivers with explanations under Articles 13–15 GDPR and reinstate accounts where

"robo-firing" breached Article 22 (Li & Toh 2022). These rights gave workers tools to contest algorithmic opacity. But enforcement was uneven: platforms could provide limited data formats, weakening portability rights, and the burden of proof often fell on workers.

The link to labour rights is crucial. By treating deactivation as an Article 22 decision and reclassifying drivers as employees under Swiss law, courts bridged data protection with labour protections (Pidoux, Dehaye & Gursky 2023). This mirrors SCHUFA's insistence that scoring determines access to opportunities.

Together, the cases show that Article 22 protects not only privacy but also participation in economic life.

The AI Act compounds these obligations. Annex III lists credit scoring and employment-related AI as high-risk. Providers and deployers must comply with risk management (Article 9), data governance (Article 10), and human oversight (Article 14), plus conformity assessments (Articles 43–51). Thus, GDPR gives individuals ex-

[141] , *Scores as Decisions? Article 22 GDPR and the Judgment of the CJEU in SCHUFA Holding (Scoring) in the Labour Context | Industrial Law Journal | Oxford Academic*, cit.
[142] Ibid

post rights to contest decisions, while the AI Act imposes ex-ante duties to manage risks (Caruana 2025; Davis & Schwemer 2023).[143]

This dual regime both reinforces and complicates compliance. It closes accountability gaps but increases costs and uncertainty, especially for cross-border firms. Rintamäki notes how fragmented DPIA triggers already burden businesses; SCHUFA confirms that even preparatory scoring falls under Article 22, while the AI Act adds a FRIA for the same systems (Aza 2024).

In sum, SCHUFA and Uber expand Article 22 to cover not only final outcomes but also intermediate algorithmic outputs with decisive effects. They also expose enforcement gaps, especially around explanations and portability. For businesses using generative AI, the message is clear: algorithmic outputs that determine access to credit, work, or services must be treated as regulated decisions.

Combined with the AI Act, this creates a demanding but unavoidable compliance environment one that embeds transparency, oversight, and accountability into the core of AI governance.

2.1.3 INTERNAL BUSINESS DECISION-MAKING

The implications of legal uncertainty under the AI Act extend beyond market behavior to shape the internal governance and decision-making structures within AI-developing firms. Under the Act's lifecycle-based framework, risk management becomes an embedded organizational process, requiring continuous evaluation and response throughout the development and deployment cycle. This represents a fundamental shift: compliance is no longer an isolated legal function, but a strategic priority with implications for design, resource allocation, and long-term planning.[144]

---

[143] , *Data Subject Rights as a Tool for Platform Worker Resistance: Lessons from the Uber/Ola Judgments by Wenlong Li, Jill Toh :: SSRN*, [s.d.]consultabile su https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4306868.

[144]B. M. CABRERA et al., *The Artificial Intelligence Act: Insights Regarding Its Application and Implications*, in *Procedia Computer Science*, CENTERIS - International Conference on ENTERprise Information Systems / ProjMAN - International Conference on Project MANagement / HCist - International Conference on Health and Social Care Information Systems and Technologies, 256 (gennaio 2025), pp. 230–237.

The compliance process must begin during the early stages of design and continue through deployment, monitoring, and eventual system retirement. This temporal integration of compliance obligations compels firms to develop forward-looking architectures that anticipate and manage legal risks proactively. High-risk systems, in particular, must meet requirements for human oversight, documentation, and data governance obligations that directly influence how AI systems are architected and tested.

Internally, these obligations cut across departments. Legal teams, compliance officers, engineers, and product managers must coordinate to ensure systems are properly classified and adequately safeguarded. In larger organizations, this coordination is often formalized through dedicated governance bodies, such as AI ethics boards or cross-functional compliance committees. However, even within such structures, legal accountability under the AI Act remains centralized in the designated "provider," which may be a corporate entity or specific legal representative.[145]

To facilitate compliance and support classification decisions, many firms employ structured risk assessment tools. ISO 31000-aligned methods are used to model risk probability and severity, while scenario modeling frameworks some inspired by environmental risk analysis—allow organizations to test systems under edge-case assumptions. Rights-balancing tools are also used to assess proportionality, particularly where competing interests (such as fairness and safety) intersect. Visual aids such as risk matrices help structure these evaluations and support decision-making. Larger firms may partially automate these tasks through compliance software or workflow integration platforms, though these require considerable investment in tooling and personnel.[146]

Strategic decisions around product launch and market targeting are often informed by internal assessments of regulatory exposure. When faced with classification ambiguity, companies may delay release, reduce functionality, or avoid the EU market altogether. SMEs, which typically lack the capacity to sustain parallel development paths for

[145] Ibid

[146] Ibid

different regulatory regimes, are particularly affected. The resulting trade-off between compliance and competitiveness may lead firms to deprioritize innovation in high-risk domains despite potential societal benefit.[147]

Regulatory sandboxes offer a promising countermeasure to these constraints. These supervised environments allow companies to test high-risk AI systems while receiving feedback from regulators, reducing the legal exposure typically associated with pre- market experimentation. Pilot programs in jurisdictions such as the UK and South Korea demonstrate that sandboxes can accelerate both innovation and compliance learning. The inclusion of accessible sandbox schemes in the EU context especially for SMEs could help close the capacity gap and foster more inclusive AI development.

Still, reliance on internal resources and private governance tools cannot fully address the systemic imbalance between large and small actors. [148] The current compliance model presumes a level of technical and legal sophistication that many SMEs do not possess. Uniform legal obligations when not coupled with differentiated guidance or state-supported capacity-building risk reinforcing industry concentration by sidelining smaller, potentially more innovative players.[149]

Ultimately, internal compliance structures under the AI Act reveal a pattern of institutional adaptation shaped by resource asymmetry. While larger firms may develop sophisticated compliance ecosystems to manage complexity, others struggle to maintain a foothold in regulated markets. [150]Without flexible implementation pathways, collaborative regulatory mechanisms, or state-supported compliance infrastructure, the Act may privilege procedural conformity over meaningful accountability, undermining both its effectiveness and its legitimacy.

2.2 BUILDING AI COMPLIANCE INTO BUSINESS OPERATIONS

[147] , *A Sandbox Approach to Regulating High-Risk Artificial Intelligence Applications | European Journal of Risk Regulation | Cambridge Core*, cit.

[148] , *(PDF) Regulatory and Compliance Requirements for SMEs Operating AI Systems through Data Centers in the EU, with a Focus on Data Protection Challenges in Germany*, cit.

[149] C. NOVELLI et al., *AI Risk Assessment: A Scenario-Based, Proportional Methodology for the AI Act*, in *Digital Society*, 3(1) (2024), pp. 1–29.

[150] Ibid

2.2.1 STRUCTURING AI COMPLIANCE INSIDE ORGANIZATIONS

The successful implementation of AI compliance within organizations requires the establishment of effective governance structures tailored to the unique characteristics, resources, and operational complexities of each entity. While previous discussions in Chapter 1 outlined the regulatory framework and compliance obligations under the EU AI Act, this section focuses on the organizational dimension: how companies, particularly varying by size and sector, can internalize and operationalize these legal requirements. [151]This focus is critical because regulatory mandates alone do not guarantee compliance; rather, embedding compliance into the organizational fabric is essential for sustainable adherence and risk mitigation. To understand how organizations can operationalize compliance, it is first essential to examine the structural and managerial underpinnings that support these efforts.

Governance and Accountability in AI Compliance

[152]At the core of effective AI compliance is a clear governance framework that delineates roles, responsibilities, and accountability mechanisms.[153] Organizations must establish defined leadership roles specifically tasked with overseeing AI compliance efforts.[154] These roles ensure that AI governance is not siloed but integrated with the company's overall strategic and operational objectives. Accountability extends beyond leadership to include all stakeholders involved in the AI lifecycle from development to deployment and post-market monitoring.

To maintain accountability, it is essential to develop and implement performance metrics that objectively evaluate compliance effectiveness. Regular audits and assessments further reinforce accountability by identifying gaps and facilitating corrective actions. Transparency in reporting compliance status to internal and external stakeholders fosters trust and aligns with ethical standards underpinning the regulatory

[151]J. WALTERS et al., *Complying with the EU AI Act*, 2024, p.
[152] Ibid
[153] Ibid
[154] Ibid

framework. Ongoing training for those responsible for compliance ensures that knowledge remains current amid the rapidly evolving AI regulatory landscape.[155] Governance structures should also facilitate collaboration across departments, including legal, risk management, operations, IT, and AI development teams. Cross- functional committees or working groups serve as effective platforms for coordinating compliance activities, sharing knowledge, and resolving regulatory ambiguities. Such collaborative governance reduces fragmentation, enhances communication, and supports a unified organizational approach to compliance.[156]
Beyond structural governance, leadership plays a pivotal role in shaping how compliance practices are implemented and sustained across teams.

Leadership Styles and Their Impact on AI Compliance

Leadership style significantly shapes the culture and effectiveness of AI compliance within organizations. Different leadership approaches influence how compliance initiatives are prioritized, how innovation is balanced with risk management, and how teams are motivated to uphold regulatory standards. [157]
Visionary and transformational leadership styles tend to foster innovation and proactive compliance cultures by inspiring commitment and aligning compliance goals with the organization's broader mission. Transactional leadership emphasizes structured processes and performance targets, which can help enforce discipline and consistency in compliance activities. Participative leadership encourages involvement and input from various stakeholders, promoting a shared sense of responsibility and collaborative problem-solving.[158]
Adapting leadership styles to the organization's maturity and complexity can enhance compliance outcomes. [159]For example, in highly regulated industries, transactional

[155] H.-W. MICKLITZ, G. SARTOR, *Compliance and Enforcement in the AIA through AI*, in *Yearbook of European Law*, 43 (agosto 2024), pp. 297–341.

[156] J.) V.V.AA., *General-purpose AI regulation and the European Union AI Act*, cit.
[157] MICKLITZ - SARTOR, *Compliance and enforcement in the AIA through AI*, cit.
[158] Ibid
[159] MICKLITZ - SARTOR, *Compliance and enforcement in the AIA through AI*, cit.

leadership may ensure adherence to rigid standards, whereas in innovative AI development units, visionary leadership can stimulate ethical and responsible AI practices.[160]

While leadership and governance set the tone, the real test lies in embedding these structures within the operational fabric of day-to-day teams.

Embedding AI Compliance Within Existing Teams

A critical challenge in structuring AI compliance is embedding these requirements into the workflows of existing legal, risk, and operational teams. While compliance frameworks and regulatory obligations provide a blueprint, their practical implementation depends on how well organizations integrate AI compliance with existing processes.

Embedding AI compliance necessitates tailored training programs that equip relevant teams with up-to-date knowledge of AI regulations and operational implications. These programs should be accessible and role-specific, addressing the needs of legal counsel, risk managers, data scientists, and operational staff alike.

Another essential component of embedding compliance is cross-functional cooperation. The risk of isolated decision-making is decreased and compliance obligations are managed holistically by forming interdisciplinary teams with representatives from legal, risk, IT, and AI departments. By avoiding duplication of labor and utilizing organizational experience, AI compliance frameworks that are in line with current legal and operational procedures increase efficiency.

Organizations are able to adjust to new risks and regulatory changes through ongoing monitoring through frequent audits and compliance assessments. This constant watchfulness fosters a dynamic rather than static culture of compliance. However, organizational size and internal competencies have a significant impact on the ability to execute these governance techniques.

Influence of Organizational Size on AI Compliance

[160] Ibid

Organizational size plays a pivotal role in shaping the capacity and approach to AI compliance. Larger organizations generally possess greater financial and human resources, including dedicated legal and compliance departments. These resources facilitate the development of sophisticated compliance programs, capable of addressing complex regulatory requirements and operational intricacies.

In contrast, smaller organizations often face significant constraints in budget, expertise, and personnel. These limitations challenge their ability to fully understand, interpret, and implement the multifaceted obligations imposed by the AI Act. Moreover, SMEs frequently depend on external consultants and compliance tools to bridge gaps in knowledge and capability.

The operational complexity of larger organizations often involves multiple departments and geographic locations, requiring comprehensive coordination and harmonization of compliance efforts. Smaller organizations typically have simpler structures but lack regulatory expertise and sustainable compliance processes, which can increase vulnerability to non-compliance risks.

Demands for compliance are also influenced by the industry in which a company works. Because of the greater risk profiles of their AI applications, many industries are subject to more stringent regulatory monitoring. In these industries, compliance initiatives must be customized for both big and small businesses.

Strategies for Overcoming Size-Related Compliance Challenges

To mitigate size-related disparities in AI compliance capability, organizations can adopt several strategic approaches: [161]

- Leverage External Expertise: Smaller organizations can access specialized consultants, legal advisors, and compliance professionals who bring focused knowledge of AI regulations, helping to design and implement effective compliance programs without maintaining large in-house teams.
- Compliance Management Software: The use of automated compliance platforms supports tracking regulatory changes, managing documentation, and

[161] MICKLITZ - SARTOR, *Compliance and enforcement in the AIA through AI*, cit.

monitoring compliance status. These tools reduce manual workloads and help maintain an audit trail, crucial for demonstrating compliance during inspections.

- Risk-Based Compliance Prioritization: Given limited resources, organizations benefit from prioritizing compliance efforts based on risk assessments. High-risk AI applications or processes receive focused attention, ensuring resource optimization.
- Incremental Implementation: Phasing in compliance measures over time allows organizations to manage costs and complexity more effectively. Gradual adoption supports learning and process refinement.
- Peer Collaboration and Industry Networks: Participation in industry consortia or regulatory forums enables knowledge sharing, benchmarking, and collective problem-solving, enhancing compliance readiness.
- Continuous Training and Awareness: Regular updates and accessible training modules ensure that employees remain informed about evolving AI regulatory requirements and compliance best practices.

Tools and Platforms Supporting AI Compliance

Several categories of tools support organizations in embedding and managing AI compliance:

- Compliance Platforms provide end-to-end management of compliance workflows, regulatory change tracking, and documentation control.
- AI Governance Platforms offer specialized solutions for monitoring AI models, assessing fairness, and ensuring transparency.
- Risk Management Software helps identify, evaluate, and mitigate compliance risks associated with AI applications.
- Document Management Systems facilitate secure storage and retrieval of compliance records, ensuring audit readiness.
- Training Platforms deliver tailored educational content to build organizational compliance competence.

Even as organizations adopt various strategies and tools to navigate AI compliance, the academic and regulatory literature has yet to fully address one crucial dimension.

While these tools and strategies support implementation, they also expose the limits of existing literature in capturing the operational realities faced by diverse organizations.

Recognizing the Gap in Literature and Practice

Despite these identified practices and tools, there remains a notable gap in the literature regarding the specific operational integration of AI compliance within organizations of varying sizes and structures. Existing research predominantly addresses general frameworks, regulatory requirements, or compliance strategies at a conceptual level, without detailed exploration of how organizations customize and embed these requirements based on their internal capabilities and resources.
This gap underscores the need for further empirical studies and practical guidance that illuminate effective models for AI compliance governance tailored to organizational diversity. Understanding how companies operationalize compliance across different contexts is vital to bridging the divide between regulatory intent and actual implementation, ultimately enhancing compliance outcomes and promoting trustworthy AI deployment. [162]

2.2.2 TRANSLATING LAW INTO TECHNICAL AND ORGANIZATIONAL PROCESSES

[163]A central challenge companies face under the EU Artificial Intelligence Act (AI

Act) is not simply knowing what the law requires, but how to operationalize those duties across diverse AI systems and organizational contexts. The Act outlines legal obligations such as transparency, risk management, and human oversight but offers minimal guidance on how firms should implement these in practice. This disconnect between legal theory and business application has prompted many organizations to adopt what is often referred to as *compliance-by-design*—a structured approach in which legal and ethical requirements are built directly into the technical architecture

[162] J.) V.V.AA., *General-purpose AI regulation and the European Union AI Act*, cit.
[163] H. MUSTROPH, S. RINDERLE-MA, *Design of a Quality Management System Based on the EU Artificial Intelligence Act*, arXiv:2408.04689, preprint, arXiv, 12 novembre 2024, p.

and operational workflows of AI systems from the earliest development stages, rather than reviewed or applied retroactively.

The logic behind compliance-by-design is to ensure that systems are auditable, accountable, and adaptable throughout their lifecycle. Rather than treating compliance as an external constraint, it becomes an embedded property of the system. For example, when transparency is a legal requirement, this must be reflected not only in user documentation but also in explainability tools within the AI system itself.[164] Companies increasingly adopt tools such as performance metrics, saliency maps, and natural language summaries to help users understand how outputs are generated. While technically valuable, these tools may not fully meet the expectations of non-expert users or regulators without supplementary user-facing disclosures.

These disclosures often take the form of readable instructions, statements of limitations, and clear system behavior descriptions. Some companies are standardizing this process through tools like *AI cards* or *use case cards*.[165] which summarize the system's purpose, input-output behavior, and foreseeable risks. These tools also serve as documentation artifacts that facilitate communication between engineers, compliance teams, and stakeholders during audits or system updates. However, adoption remains uneven, and firms often lack sector-specific templates that would make these disclosures more actionable.[166]

Beyond transparency, risk management must also be implemented technically and procedurally. Risk mitigation activities now include *scenario modeling*, *stress testing*, and documentation of potential failure modes. Rather than limiting this to a single design phase, companies are encouraged to structure risk management across three stages: planning (ex-ante), ongoing operation, and post-deployment adjustment. These phases ensure that risks are monitored and updated as systems evolve in real-world conditions. To support this, many firms build structured documentation systems that

[164] Ibid

[165]D. DEY, D. BHAUMIK, *APPRAISE: A Governance Framework for Innovation with AI Systems*, arXiv:2309.14876, preprint, arXiv, 11 dicembre 2023, p.

[166] Ibid

record known risks, their likelihood and severity, and corresponding mitigation strategies. These repositories serve as internal audit trails and support external conformity assessments.

On the technical side, companies are increasingly using modular architectures to align with compliance workflows. Microservices separate components within a system handle functions like data logging, human oversight, or model versioning independently. [167]This approach allows companies to update or replace compliance components without rebuilding the entire system. It also enhances traceability, as each module can be documented and audited separately. Some organizations use *strategy patterns* a software design technique that enables switching between different compliance strategies depending on the AI use case to maintain flexibility without sacrificing legal conformity.

A particularly demanding area is human oversight. Technically, this may involve interface controls for pausing or reversing system decisions, especially in high-risk contexts. Organizationally, it requires defining who is responsible for monitoring the system and under what conditions human review is triggered. Many firms implement *manual approval gates*—checkpoints where a human must approve the output before it is used or actioned. While these gates help meet oversight obligations, they can introduce friction into system performance and must be balanced with operational needs.

In order to translate legal requirements, data governance is also essential. The AI Act expects providers to use high-quality, representative, and documented datasets throughout the training, validation, and testing phases. Companies address this through centralized data management systems that record data sources, sizes, types, and evidence of bias mitigation. These systems increasingly feature automated compliance checks that flag issues such as incomplete metadata or inconsistencies between training and operational environments. Yet, effective data governance requires not only

[167] Ibid

technical tools but also clear accountability structures within organizations an area where many firms still struggle.

To maintain ongoing compliance, companies are investing in *compliance health checks* internal review mechanisms that periodically evaluate whether an AI system remains aligned with legal expectations. These checks often occur at key stages in the product lifecycle or after substantial system modifications. They are supported by documentation tools that integrate inputs from legal, product, and engineering teams. Some organizations embed these reviews into their broader quality management systems, ensuring that compliance becomes part of routine project governance rather than an afterthought.

Businesses are adapting their internal organizational procedures to accommodate new technological solutions. To manage AI initiatives, cross-functional teams are estab- lished, combining technical, legal, and risk skills. Workflows for approval are set up to guarantee sign-off prior to deployment. In more established companies, procurement processes, version control systems, and sprint cycles all incorporate compliance check- points. Many small and medium-sized businesses (SMEs), however, lack the funding necessary to develop such organized processes. They frequently use generic tools or outside consultants, which might not adequately account for sector-specific compliance requirements.

Despite this progress, key limitations remain. Some firms struggle to determine when a model modification is "substantial" enough to require full documentation updates. Others report that automated compliance tools are incomplete and require manual overrides. Technical constraints such as the computational cost of model analysis can also limit the ability to implement continuous monitoring. These practical issues highlight the need for better guidance and clearer benchmarks for compliance translation.

There is also a risk that current practices devolve into checkbox compliance: producing documentation without meaningful oversight or adaptation. [168]Without standardized

[168] M. MÄNTYMÄKI et al., *Putting AI Ethics into Practice: The Hourglass Model of Organizational AI Governance*, arXiv:2206.00335, preprint, arXiv, 31 gennaio 2023, p.

templates, interoperable documentation formats, or centralized support mechanisms, translation practices will remain fragmented. SMEs are especially vulnerable, as they face disproportionate compliance burdens and limited access to legal-tech infrastructure.

In conclusion, integrating the legal requirements of the AI Act into real-world corporate operations is a complex process that calls for both organizational discipline and technical expertise. [169] To fulfill compliance requirements, businesses are creating governance frameworks, lifecycle documentation systems, and modular architectures. This terrain is still resource-intensive and irregular, though. [170]Although it requires consistent commitment and internal resources, compliance-by-design has potential as a unifying technique. It will take better guidance, standardized tools, and more explicit enforcement requirements to close this gap; these tasks will probably fall to the newly established EU AI Office and other standards organizations. [171]They will play a vital role in making sure that legal aspirations are turned into operational realities at every level of the market.

2.3 STRATEGIC BUSINESS RESPONSES TO REGULATION

2.3.1 ADAPTIVE STRATEGIES ACROSS BUSINESS SIZES

While the AI Act presents a uniform set of regulatory obligations, firms are not uniform in how they respond.[172] Their strategies for implementing compliance depend significantly on internal resources, operational complexity, and organizational size. However, existing literature largely emphasizes overarching frameworks, audit protocols, and legal interpretations of the AI Act without detailing how organizations of different sizes tailor these requirements to fit their specific capacities. Direct empirical studies differentiating compliance strategies by firm size remain scarce.[173]

---

[169] Ibid

[170]Ibid

[171] MÄNTYMÄKI M. V.V.AA., *Putting AI Ethics into Practice: The Hourglass Model of Organizational AI Governance*, 2023.

[172]C. NOVELLI et al., *Automating Business Process Compliance for the EU AI Act*, IOS Press Ebooks, 2024, p. 25.

[173] Ibid

To address this gap, this section draws on related findings from AI law compliance literature, general regulatory compliance practices, organizational theory, and analogies from GDPR implementation to infer how large firms and SMEs (small and medium-sized enterprises) may diverge in their strategic responses to the AI Act.

Internal Resource Constraints and Strategic Adaptation

Organizational capacity is one of the most significant variables in determining a firm's ability to meet AI regulatory demands. Larger firms are more likely to possess dedicated legal and technical teams, internal audit functions, and formalized compliance departments. These structures allow for the development of comprehensive AI governance programs that incorporate continuous monitoring, internal controls, employee training regimes, and dedicated compliance officers. [174]Such firms tend to engage in proactive compliance planning, regularly updating their internal protocols to stay aligned with evolving legal interpretations of the AI Act. Many develop internal audit routines that combine quality checks, model behavior reviews, and risk documentation processes to satisfy conformity assessments and post-market monitoring duties under the Act.[175]

In contrast, SMEs typically operate with leaner structures and constrained budgets, which shape their compliance approach differently. Without in-house legal or AI engineering teams, these firms often rely on external consultants, legal technology tools, or standardized compliance templates to interpret their obligations and execute documentation requirements. Their strategy leans on outsourcing and agility: instead of building permanent compliance departments, SMEs often designate existing personnel to act as compliance leads, adapting broader policies into operational terms within their resource limits. Some SMEs adopt pre-built AI lifecycle tools or contract management platforms to document supplier obligations, maintain version control, and

[174] NOVELLI C. - G. GOVERNATORI - A. ROTOLO, *IOS Press Ebooks - Automating Business Process Compliance for the EU AI Act*, [s.l.], [s.d.].

[175] , *(PDF) Regulatory and Compliance Requirements for SMEs Operating AI Systems through Data Centers in the EU, with a Focus on Data Protection Challenges in Germany*, cit.

track vendor transparency claims. This allows them to meet baseline transparency and accountability requirements without internal overhauls.

[176]Automation and Technological Leverage

Regardless of firm size, automation is increasingly viewed as a key enabler of scalable compliance. Yet the way firms integrate automation diverges. Large firms tend to develop or customize automated compliance pipelines that integrate AI risk classification, documentation generation, and internal reporting into their broader IT and audit systems. This may include logging frameworks that document data lineage, user interactions, or model updates in real-time feeding into regulatory dashboards used by legal and risk teams. [177]Larger firms may also embed compliance automation into procurement workflows, enabling flagging of high-risk third-party tools or triggering mandatory conformity checks before deployment.

For SMEs, however, automation typically comes in the form of plug-and-play legaltech tools. These solutions may include guided assessments, vendor risk scoring tools, or pre-configured DPIA generators. Automation in this context serves more as a compliance shortcut helping firms interpret, rather than architect, complex obligations. While these tools may lack deep integration into internal IT systems, they offer cost- effective alternatives for mapping AI usage, tracking risks, and generating transparency documentation. The affordability and low-friction setup of such tools often make them indispensable for SMEs navigating high-risk AI use without dedicated compliance capacity.

Organizational Design and Governance Models

Organizational structure further shapes compliance execution. Larger firms are increasingly institutionalizing governance bodies AI ethics boards, compliance task

[176] NOVELLI V.V.AA., *IOS Press Ebooks - Automating Business Process Compliance for the EU AI Act*, cit.

[177] MÄNTYMÄKI V.V.AA., *Putting AI Ethics into Practice: The Hourglass Model of Organizational AI Governance*, cit.

forces, or model review committees tasked with overseeing legal and ethical risks. These entities bring together legal, technical, operational, and ethical expertise to standardize practices, manage AI inventories, and evaluate high-risk use cases. Compliance becomes embedded in broader enterprise risk frameworks, aligning with existing governance mechanisms under GDPR, ISO 27001, or ESG reporting.

SMEs, on the other hand, often avoid duplicating formal governance bodies. Instead, they rely on existing managerial hierarchies or cross-functional teams to oversee AI risk. Where possible, SMEs align AI Act obligations with roles already familiar from GDPR implementation for example, assigning AI compliance tasks to the Data Protection Officer, IT manager, or operations lead. This consolidation minimizes overhead while maintaining traceability and internal accountability. Informal governance is thus a strategic adaptation relying more on flexible structures and individual discretion than codified oversight mechanisms.

Vendor and Supply Chain Compliance

AI Act compliance is not limited to in-house systems; it extends to AI tools procured externally. [178] This dimension becomes particularly important for SMEs, which often depend on third-party vendors for AI functionality. [179]Large firms tend to formalize this process due to diligence protocols during procurement quiring vendors to provide audit trails, transparency documentation, and risk classification data. [180]They embed AI-specific clauses in contracts, including warranties of compliance, right-to-audit provisions, and liabilities for non-compliance. These measures reflect the firm's bargaining power and capacity to enforce contractual discipline across its AI supply chain.

SMEs, by contrast, may lack the leverage or legal sophistication to enforce such terms. Their approach to vendor compliance often depends on trust-based relationships,

[178] J.) V.V.AA., *General-purpose AI regulation and the European Union AI Act*, cit.
[179] NOVELLI V.V.AA., *IOS Press Ebooks - Automating Business Process Compliance for the EU AI Act*, cit.
[180] Ibid

publicly available risk assessments, or vendor certifications. Some use procurement guides or sectoral checklists developed by industry associations to ensure that third- party tools align with the AI Act. Where contract customization is unfeasible, SMEs might favor vendors that proactively offer documentation, third-party audits, or sandbox participation to demonstrate regulatory alignment.

Cultural and Strategic Orientation Toward Compliance

Firm culture and leadership also play critical roles in shaping compliance behavior. In large firms, compliance is often viewed as part of the company's strategic risk profile integrated into reputational management, investor relations, and public trust strategies. These firms may view AI governance as a competitive differentiator, investing in early compliance to enhance credibility with regulators and customers. Internal training programs, ethics awareness campaigns, and board-level oversight mechanisms support a culture of proactive risk management.

In SMEs, the orientation is often more reactive and pragmatic. Compliance is typically pursued not as a branding asset but as a barrier to avoid something to meet efficiently without disrupting product timelines or draining limited resources. Nonetheless, some SMEs are beginning to recognize the strategic value of compliance signaling using transparency reports, certifications, or sandbox participation to appeal to clients, funders, or public procurement frameworks. In niche sectors, this signaling can level the playing field, helping smaller players gain credibility despite lacking the visibility or legacy of larger competitors.

Resource-Based Perspectives on Compliance Strategy

The resource-based view (RBV) [181] of the firm helps explain why size-based strategic divergence occurs. Larger firms, endowed with deeper financial, legal, and technical resources, develop bespoke compliance infrastructures and formal governance

[181] , *Proposal for a Regulation laying down harmonised rules on artificial intelligence | Shaping Europe's digital future*, cit.

mechanisms.[182] Their strategies emphasize procedural completeness and reputational risk avoidance. SMEs, by contrast, must deploy resources more selectively leveraging agility, niche expertise, and external partnerships to stay compliant. They prioritize tactical effectiveness over bureaucratic depth and often repurpose existing roles and workflows to meet legal expectations.[183]

Crucially, firm size does not merely influence how much can be done—it shapes how compliance is approached. SMEs may innovate faster, adopting modular tooling and lightweight training programs, while larger firms may institutionalize change more slowly but at greater depth. [184]These differences underscore the need for size-sensitive regulatory support. One-size-fits-all frameworks risk reinforcing structural inequalities, where large players formalize compliance with ease while smaller firms struggle to navigate ambiguity and cost.

The AI Act sets a common standard, but businesses approach that standard through different strategic lenses shaped by size, resources, and organizational maturity.[185] While large enterprises often formalize compliance within deep governance structures and expansive risk frameworks, SMEs opt for agile, cost-sensitive adaptations that rely on outsourcing, standardization, and selective integration.[186] These strategies reflect broader organizational behavior and regulatory adaptation theories, emphasizing the role of internal capabilities in shaping legal alignment. As compliance becomes a determinant of trust and competitiveness, supporting a diversity of adaptive strategies especially among resource-constrained firms will be essential to ensuring equitable and effective AI governance.

---

[182] NOVELLI V.V.AA., *IOS Press Ebooks - Automating Business Process Compliance for the EU AI Act*, cit.

[183] , *Artificial Intelligence in Business Law: Navigating Regulation, Ethics, and Governance - Journals*

- Master Educational Services, Vasant Vihar, Delhi,, cit.

[184] A. Hayward et al., "Meeting the Global Challenge through a Collaborative Business Strategy for Small and Medium-Sized Enterprises," *2006 IEEE International Conference on Management of Innovation and Technology* 1 (June 2006): 11–15, https://doi.org/10.1109/ICMIT.2006.262271.

[185] NOVELLI V.V.AA., *IOS Press Ebooks - Automating Business Process Compliance for the EU AI Act*, cit.

[186] Ibid

2.3.2 HOW FIRMS HAVE RESPONDED TO AI ACT AND GDPR PRESSURES.

Despite the AI Act's one-size-fits-all approach to regulatory obligations, its implementation across firms of different sizes reveals substantial divergence in strategy, resource allocation, and capacity to internalize legal norms. While comprehensive, the AI Act's operational complexity risks reproducing the same asymmetries seen under the General Data Protection Regulation (GDPR), where small and medium-sized enterprises (SMEs) were disproportionately burdened by requirements designed with large entities in mind.[187] The absence of empirical AI-specific literature on differential implementation across firm sizes necessitates turning to GDPR compliance studies, which offer useful analogies particularly regarding how firms align (or fail to align) compliance with their internal resources, staffing structures, and governance maturity.

Structural Asymmetries and Resourcing Gaps

A recurring theme across GDPR research is that SMEs face far greater implementation challenges than large firms due to structural and resource-based constraints.[188]

Small organizations often lack the legal expertise, technical capacity, and dedicated personnel needed to internalize complex regulatory requirements. Under GDPR, many SMEs underestimated the scope of the regulation or misunderstood their obligations, leading to widespread instances of superficial or incorrect compliance practices.[189] Similarly, the AI Act requires high levels of interpretive judgment particularly in classifying AI systems under the tiered risk framework and determining the appropriate technical and organizational safeguards. These tasks resemble the GDPR's demand for data protection impact assessments (DPIAs), privacy documentation, and vendor contracts, which SMEs struggled to complete or even identify as legally necessary.

---

[187] , *Scores as Decisions? Article 22 GDPR and the Judgment of the CJEU in SCHUFA Holding (Scoring) in the Labour Context | Industrial Law Journal | Oxford Academic*, cit.

[188] NOVELLI V.V.AA., *IOS Press Ebooks - Automating Business Process Compliance for the EU AI Act*, cit.

[189] NOVELLI V.V.AA., *IOS Press Ebooks - Automating Business Process Compliance for the EU AI Act*, cit.

[190]The AI Act's requirements around transparency, data governance, and human oversight may appear similarly abstract and open-ended to resource-constrained firms, pushing them to adopt defensive or overcautious compliance strategies or disengage from high-risk AI use altogether.

Supplier Contracts and Legal Delegation

One of the most difficult GDPR compliance tasks for SMEs involved establishing written agreements with all suppliers who handle personal data. Studies show that many small firms lacked the legal literacy or administrative infrastructure to draft, manage, or enforce these contracts. A similar dynamic is emerging under the AI Act, which demands contractual clarity over risk allocation, transparency access, and documentation rights between AI providers and deployers.

Larger firms are generally equipped to manage these expectations through formal procurement teams, legal departments, and automated contract management systems. In contrast, SMEs tend to rely on standard templates, informal supplier relationships, or third-party services to bridge this legal capability gap. GDPR studies showed that when simplified contractual models were provided by industry associations, public agencies, or legal tech platforms SME compliance rates increased noticeably. The same logic applies to AI governance: simplified supplier checklists, contract templates, and external advisory services could serve as vital scaffolding for smaller firms with limited legal capacity.

Documentation as a Capacity Bottleneck

Documentation remains a central pillar of both the GDPR and the AI Act. For SMEs under the GDPR, the need to maintain comprehensive records of processing activities, privacy notices, and breach response plans proved highly burdensome. The same is true for AI compliance, where firms must maintain internal risk management systems, audit logs, and post-market monitoring reports particularly when operating high-risk systems.

[190] Ibid

Under GDPR, SMEs frequently reported difficulty identifying which records were required, how to format them, and what level of detail sufficed. Documentation was often viewed not only as administratively complex but also as legally risky, with firms fearing that missteps could increase liability. [191]To address this, various frameworks and support models were developed to automate or simplify documentation ranging from plug-and-play compliance platforms to structured, step-by-step methodologies co-developed with SMEs. [192]

These solutions proved effective by focusing on scalability and task delegation. Instead of requiring firms to independently interpret abstract legal texts, structured models offered guided compliance, often through visual mapping of data flows or pre-filled templates. Applying this insight to the AI Act, documentation tools should emphasize usability, automation, and real-time integration into daily workflows particularly for SMEs that do not have time or capacity to learn the regulation in depth.

Modular Compliance Frameworks

Several GDPR studies proposed modular compliance frameworks for SMEs that combined risk-based prioritization, task allocation, and lightweight implementation strategies. One widely cited approach began with a mapping phase identifying personal data flows followed by a policy design phase and finally an implementation phase focused on embedding new routines. These frameworks were successful not because they reduced legal obligations but because they translated them into manageable, staged activities aligned with SME workflows.

The AI Act demands a similar approach. Rather than imposing uniform conformity assessment protocols, regulatory support tools should enable firms to adapt requirements to their internal structures.[193] For example, risk assessments for AI

[191] , *(PDF) Regulatory and Compliance Requirements for SMEs Operating AI Systems through Data Centers in the EU, with a Focus on Data Protection Challenges in Germany*, cit.

[192] NOVELLI V.V.AA., *IOS Press Ebooks - Automating Business Process Compliance for the EU AI Act*, cit.

[193] , *(PDF) Regulatory and Compliance Requirements for SMEs Operating AI Systems through Data Centers in the EU, with a Focus on Data Protection Challenges in Germany*, cit.

systems could be designed to resemble DPIAs, allowing SMEs to re-use familiar methods and templates. Similarly, structured workflows could guide firms through logging requirements, vendor risk evaluations, and the classification of general-purpose AI systems offering intuitive pathways through an otherwise fragmented compliance terrain.

Flexibility vs. Formalization

One advantage SMEs exhibited during GDPR rollout was organizational agility. With fewer legacy systems and flatter hierarchies, SMEs could more quickly update workflows and reassign responsibilities when compliance needs were clearly articulated. However, this agility often came at the expense of formalization. Many SMEs lacked written policies, training programs, or designated compliance officers. This led to inconsistencies in how data protection principles were applied across teams and increased the risk of non-compliance during audits.

The AI Act presents a more challenging landscape in this regard. Whereas GDPR compliance can often be assessed through documentation alone, AI governance requires evaluation of system behavior, model training methods, and real-world use. These more technical elements demand ongoing oversight. Thus, the trade-off between flexibility and formalization becomes more acute: agile adaptation is still valuable, but it must be anchored in structures that guarantee traceability, auditability, and post- market monitoring. Regulatory sandboxes, cross-functional governance templates, and periodic internal audits could help SMEs strike this balance.

Culture, Awareness, and Sectoral Norms

Both GDPR and AI compliance are shaped not only by internal capacity but also by cultural readiness and external expectations. GDPR studies revealed that firms with leadership buy-in and a culture of transparency were significantly more successful in adopting compliant practices. SMEs that viewed GDPR as a reputational or competitive issue, rather than a legal risk, were more likely to invest in long-term solutions such as staff training, vendor screening, and regular audits.

This behavioral dimension is particularly relevant for AI compliance. [194]Unlike GDPR, which focuses primarily on data protection, the AI Act touches on ethics, bias, autonomy, and discrimination topics that require contextual judgment and moral reasoning. Firms that internalize these values as part of their organizational mission are more likely to implement robust oversight, even without formal mandates. Cultural alignment with AI principles thus becomes a strategic asset, helping smaller firms differentiate themselves in an increasingly regulated digital market.[195]

Though the AI Act introduces novel obligations, its practical implementation is likely to mirror the patterns observed during GDPR rollout particularly the resourcing and structural gaps that divide large firms from SMEs. As GDPR analogies show, SMEs need regulatory guidance that is not only legally accurate but operationally feasible. This includes modular methodologies, simplified documentation workflows, scalable tooling, and vendor management templates.[196] Without this differentiation, the AI Act may entrench compliance as a privilege of the well-resourced, sidelining agile but under-supported firms from participation in AI innovation. The challenge ahead lies in translating high-level legal principles into actionable strategies that scale across business sizes and that reward effort, not just formality.

2.3.3 COMPLIANCE AS A COMPETITIVE ADVANTAGE

Beyond the legal necessity of complying with the EU Artificial Intelligence Act (AI Act), a growing body of empirical and strategic insight reveals that compliance can serve as a lever for long-term business value creation. In an increasingly data-driven economy, regulatory conformity especially with emerging AI laws is no longer a passive defensive posture but a proactive and strategic asset that can distinguish

[194] , *Scores as Decisions? Article 22 GDPR and the Judgment of the CJEU in SCHUFA Holding (Scoring) in the Labour Context | Industrial Law Journal | Oxford Academic*, cit.
[195] , *(PDF) Regulatory and Compliance Requirements for SMEs Operating AI Systems through Data Centers in the EU, with a Focus on Data Protection Challenges in Germany*, cit.
[196] NOVELLI V.V.AA., *IOS Press Ebooks - Automating Business Process Compliance for the EU AI Act*, cit.

industry leaders from followers. Compliance, particularly when implemented thoughtfully and integrated into organizational culture, can enhance trust, drive innovation, reduce operational risk, and unlock access to premium markets and partnerships.[197]

The AI Act's focus on risk management, documentation, transparency, and post-market monitoring requires businesses to develop rigorous internal systems, which though initially resource-intensive can catalyze operational excellence. By codifying best practices in areas like data governance, model transparency, and human oversight, the compliance framework nudges organizations toward process maturity. In turn, this maturity fosters increased internal coherence, improved risk forecasting, and better- quality assurance throughout the AI system lifecycle. Firms that treat compliance as a driver of business efficiency often realize these improvements as downstream operational benefits, such as fewer costly incidents, streamlined auditing processes, and a faster route to market for new AI products.

One of the most significant competitive advantages afforded by compliance is enhanced brand trust and consumer loyalty. Companies that invest in strong data protection and ethical AI practices signal reliability to increasingly privacy-conscious consumers. Apple’s strategic marketing around privacy exemplifies how embedding compliance values into brand identity can yield measurable customer loyalty gains[2]. As trust becomes a key currency in the digital economy, organizations capable of substantiating their commitment to privacy, transparency, and accountability can strengthen user relationships and reinforce brand equity.

This trust is not limited to consumers. Compliance also positions organizations as attractive partners in highly regulated or high-stakes sectors such as healthcare, finance, and public services. [198]These industries often demand robust third-party compliance assurance as a prerequisite for procurement or partnership. In this context, organizations that can demonstrate conformity with AI governance frameworks

[197] MÄNTYMÄKI V.V.AA., *Putting AI Ethics into Practice: The Hourglass Model of Organizational AI Governance*, cit.
[198] Ibid

particularly those incorporating quality management systems, fundamental rights impact assessments, and technical documentation gain a clear edge in competitive bidding processes.

Moreover, compliance can expand market access, especially within the EU's highly regulated digital single market. The AI Act establishes conformity assessments as mandatory gateways for high-risk AI systems to enter the market.[199]Thus, compliance transforms from a bureaucratic exercise into a market-enabling condition. Firms that successfully complete these assessments gain first-mover advantages and regulatory clearance to operate across 27 member states a privilege not afforded to non-compliant competitors. In this way, compliance becomes a prerequisite for scalability and sustainable market participation.[200]

From a risk management perspective, compliance frameworks provide organizations with tools for anticipating, mitigating, and responding to legal and ethical risks in AI development. For instance, organizations that proactively implement risk assessment procedures and post-market monitoring systems as required by the AI Act not only reduce the likelihood of incurring penalties but also avoid reputational damage resulting from publicized failures or data breaches. Given the significant fines imposed under existing regulations like the GDPR, the ability to demonstrate regulatory diligence can serve as a financial safeguard and an insurance-like function against catastrophic outcomes.[201]

The advantages also apply inside. Strong compliance initiatives frequently improve employee engagement and company culture. Employees are more likely to feel committed to the company's mission when firms make ethical AI development a key priority and support it with training, transparent governance frameworks, and accountable performance metrics. Employee morale is raised and a sense of purpose is fostered, especially in technical teams entrusted with striking a balance between

[199] MÄNTYMÄKI V.V.AA., *Putting AI Ethics into Practice: The Hourglass Model of Organizational AI Governance*, cit.

[200] Ibid

[201] , GDPR And AI-Driven Business Models: Navigating Legal Risks Through A Legal Analysis Framework, [s.d.].

responsibility and innovation. This kind of alignment can help retain talent, particularly when workers place a higher value on morality when selecting organizations.

The strategic use of frameworks such as APPRAISE, which integrates elements like responsible value creation, technology audits, supplier alignment, and organizational capital, helps formalize compliance as a component of corporate governance and cross- functional coordination. This structured approach ensures that technical teams, legal departments, and business leaders are aligned not just on outputs but also on the values guiding AI system development. In practice, such frameworks create a shared language across disciplines, reducing friction and improving decision-making quality.[202]

In sectors characterized by rapid technological change, compliance also drives continuous improvement and innovation. The iterative nature of compliance monitoring, which includes refining KPIs, conducting model audits, and updating documentation in line with evolving standards, establishes feedback loops that promote learning and adaptation. Far from hindering innovation, compliance can act as a catalyst by imposing constraints that encourage creative problem-solving within ethical and legal bounds. Organizations that embrace this dynamic often outperform those that treat regulation as a ceiling rather than a floor.

Importantly, firms that establish compliance as a core competency can export their frameworks as marketable capabilities. In a globalized digital ecosystem, regulatory frameworks like the AI Act are increasingly being mirrored or referenced in other jurisdictions. Organizations that internalize EU compliance standards are well- positioned to expand globally by demonstrating alignment with international best practices. This alignment reduces friction in cross-border data flows, facilitates international contracting, and positions the firm as a globally trusted AI provider.[203] Lastly, the importance of compliance for one's reputation cannot be emphasized enough. In a climate where stakeholders and the media are more aware of problems like algorithmic bias, data exploitation, and AI opacity, reputational concerns can

[202] Cit.

[203] NOVELLI V.V.AA., *IOS Press Ebooks - Automating Business Process Compliance for the EU AI Act*, cit.

quickly result in market penalties. On the other hand, businesses can use their ethical positioning as a strategic advantage by investing in clear, verifiable compliance. [204]By promoting their commitment to high standards, companies can stand out in crowded marketplaces, draw in investment, and gain credibility with both the public and regulators.

In sum, when viewed through a strategic lens, compliance with the AI Act transcends its legal function to become a differentiating force in competitive markets. Organizations that adopt this perspective benefit not only from legal certainty and reduced risk but also from increased operational effectiveness, brand equity, stakeholder trust, and long-term market resilience. In this way, compliance is not a burden but a business enabler a cornerstone of sustainable and responsible AI innovation.

2.3.4 BALANCING INNOVATION AND CAUTION IN A SHIFTING REGULATORY LANDSCAPE

As the EU Artificial Intelligence Act continues to take shape, companies deploying or developing AI systems must operate in a regulatory environment marked by partial legal certainty, evolving guidance, and overlapping legal regimes. The Act's core objective of safeguarding fundamental rights while promoting trustworthy AI development introduces a fundamental tension: firms must innovate to remain competitive, yet do so within a compliance framework that is still crystallizing. This section explores how organizations navigate this challenge by employing strategic flexibility, internal governance systems, and proactive risk management frameworks that allow them to remain agile while preparing for the future legal landscape.

One of the defining characteristics of the EU AI Act is its risk-based approach to regulating AI systems. This structure permits differentiated compliance obligations based on the severity of risks associated with specific applications.[205] However, the

[204] Ibid

[205] , *A Sandbox Approach to Regulating High-Risk Artificial Intelligence Applications | European Journal of Risk Regulation | Cambridge Core*, cit.

Act's practical implementation relies not only on its core provisions but also on a variety of dynamic interpretative instruments, including delegated acts, implementing acts, harmonized standards, and codes of practice. These instruments are essential for ensuring the Act's adaptability to technological change and provide firms with interpretative guidance that helps clarify compliance expectations over time. As these instruments are issued incrementally, organizations must design their compliance strategies with built-in flexibility, allowing for swift adaptation to emerging regulatory specifications.

In this transitional phase, firms are leveraging the broad language of the AI Act to exercise proportional judgment in implementing safeguards. For example, transparency requirements can be tailored to the complexity of the system in question, and human oversight obligations are interpreted in relation to the level of autonomy and potential risk of the AI system. This interpretive latitude allows firms to align risk mitigation efforts with practical business considerations, ensuring that innovation is not stifled by premature or disproportionate compliance investments.

Simultaneously, many organizations are structuring internal governance systems aimed at institutionalizing compliance. These governance structures include the appointment of AI compliance officers and the establishment of cross-functional ethics committees, which oversee both technical development and legal conformance. By formalizing responsibility and embedding ethical review processes within corporate decision- making, firms reduce the likelihood of regulatory breaches while maintaining operational freedom. Moreover, multinational corporations are increasingly centralizing their AI compliance operations to address jurisdictional discrepancies across regulatory regimes. This includes developing region-specific standards and data management policies that ensure conformance with both the AI Act and complementary regulations such as the General Data Protection Regulation (GDPR). Firms are also deploying predictive analytics and other advanced monitoring tools to detect potential regulatory risks before they materialize.[206]These tools serve a dual

[206] M. EBERS, *Truly Risk-Based Regulation of Artificial Intelligence: How to Implement the EU's AI Act*, in *European Journal of Risk Regulation*, 2020, p. 50.

purpose: they support real-time error correction and bias mitigation, and they also help companies demonstrate due diligence in their compliance efforts. Proactive risk detection is particularly critical for high-risk AI applications, which are subject to strict obligations under the AI Act. For example, firms deploying AI in fields such as healthcare, recruitment, or finance must maintain comprehensive documentation, implement data governance mechanisms, and conduct ongoing system evaluations. Real-time monitoring frameworks, therefore, play a crucial role in maintaining both technical and regulatory alignment.[207]

To ensure the traceability and accountability of AI-driven decisions, many organizations are adopting robust documentation practices and model interpretability tools such as LIME (Local Interpretable Model-agnostic Explanations) and SHAP (SHapley Additive exPlanations). These tools not only enhance transparency but also support fairness and non-discrimination objectives, aligning with both ethical principles and regulatory expectations. As explainability becomes an operational requirement under Article 13 of the AI Act, such integration also helps firms prepare for more granular implementation guidance in the future.

Importantly, many organizations recognize that the AI Act operates in a complex legal ecosystem, often interacting with existing sectoral legislation and horizontal frameworks such as consumer protection, non-discrimination, and product safety law. This overlap may lead to situations of regulatory duality or conflict. Until harmonization guidelines are formally issued by the European Commission, firms are advised to maintain detailed records of their compliance efforts across multiple frameworks, documenting the rationale for each compliance choice. This strategy not only facilitates regulatory inspections but also provides legal defensibility in the event of future enforcement actions.[208]

Firms are also relying on Data Protection Impact Assessments (DPIAs) and similar internal review procedures for high-risk systems. While not a formal substitute for the

---

[207] , *Artificial Intelligence in Business Law: Navigating Regulation, Ethics, and Governance - Journals*
- Master Educational Services, Vasant Vihar, Delhi,, cit.

[208]Ibid

AI-specific conformity assessments prescribed by the Act, these processes enable organizations to develop internal expertise, simulate likely compliance demands, and build audit-ready documentation structures. In some cases, companies are developing hybrid risk management tools that satisfy both GDPR and AI Act requirements, thereby minimizing redundant efforts and streamlining their legal operations.

At a broader level, many organizations are embedding compliance principles into their innovation pipelines. For instance, AI development teams are being trained on fundamental rights impact assessments, and iterative design approaches are being adopted that integrate feedback from legal, ethical, and social stakeholders. This holistic strategy reflects an emerging best practice where compliance is not merely a legal constraint but a guiding principle of responsible innovation.

Moreover, companies are increasingly engaging in industry-led standardization and soft-law initiatives, including the development of sector-specific codes of conduct and voluntary ethical guidelines. These instruments can serve as interpretative supplements in cases where regulatory obligations remain ambiguous or underdeveloped. Participation in such initiatives also enhances organizational legitimacy and may help shape the direction of future delegated and implementing acts issued under the AI Act framework.

In anticipation of more prescriptive enforcement, organizations are preparing for third- party conformity assessments and engaging with notified bodies to understand future certification expectations. [209]Some firms are participating in early compliance pilots or regulatory sandboxes to gain firsthand experience with regulatory processes. These engagements provide practical feedback loops, helping organizations refine their internal processes while contributing to the broader interpretative development of the AI Act.

In conclusion, firms are navigating the evolving regulatory landscape of the EU AI Act by adopting a multi-layered compliance strategy that balances legal prudence with

[209] DEY D. - D. BHAUMIK, *APPRAISE: a governance framework for innovation with AI systems*, 2023.

strategic innovation. [210]This involves a mix of internal governance structures, dynamic risk management tools, ethical design integration, and anticipatory documentation practices. By embedding flexibility and accountability into their compliance frameworks, organizations are not only preparing for future enforcement but also helping to shape a sustainable regulatory culture that supports both innovation and fundamental rights.

[210] , *Artificial Intelligence in Business Law: Navigating Regulation, Ethics, and Governance - Journals*
- Master Educational Services, Vasant Vihar, Delhi,, cit.

CHAPTER 3: Ethical Concerns Regarding Use of AI in Business

3.1 ETHICAL CHALLENGES IN GENERATIVE AI

3.1.1 WHAT IS BIAS IN GENERATIVE AI?

Bias in generative artificial intelligence (GenAI) refers to the systematic and often unintended skewing of outputs due to imbalances in the training data, model architecture, or human oversight. This issue presents both ethical and operational risks. As GenAI systems become more embedded in sectors like hiring, education, finance, and healthcare, their potential to reinforce or amplify social inequalities has become a major concern. Understanding the nature, sources, and impacts of bias is crucial for developing fair and trustworthy AI systems.

Dimensions and Origins of Bias

Bias in GenAI arises primarily from two interconnected sources: the training data and the model design. Since GenAI models rely on large datasets scraped from digital environments, they inevitably reflect the historical and social prejudices embedded in those datasets. [211]These may include gender stereotypes, racial profiling, or economic disparities, often leading to outputs that perpetuate rather than challenge societal inequalities.

A common example is image or language generation tools that associate specific professions with particular genders or ethnic groups. Such patterns are not manually coded but emerge from biased correlations within the data. This phenomenon also extends to deepfakes and synthetic media, where marginalized groups may be disproportionately misrepresented. [212]As these outputs circulate, they can influence

[211] W. LIU, M. LI, *The Analysis of Technological Ethical Issues in Generative Artificial Intelligence*, 14 settembre 2024, p.

[212] Ibid

public perception, policy discourse, and even legal decisions making the societal implications of bias in AI not just abstract but deeply material.[213]

Algorithmic design can exacerbate this problem when developers fail to incorporate fairness constraints or when model performance metrics do not account for subgroup variability. In these cases, even technically accurate models may still yield discriminatory results if they disproportionately underperform for certain demographics.

3.1.2 IMPACTS AND REAL-WORLD CONSEQUENCES

Bias has particularly serious repercussions in high-stakes situations. If previous hiring disparities are reflected in the underlying data, biased GenAI algorithms may exclude competent applicants on the basis of age, gender, or ethnicity. In the financial industry, credit scoring algorithms that were educated on distorted or insufficient data may refuse loans to underprivileged populations. [214]For those with darker skin tones, facial recognition algorithms in law enforcement have demonstrated noticeably greater error rates, frequently leading to misidentification.

Bias also undermines public trust. If people perceive GenAI outputs as unjust or discriminatory, the legitimacy and adoption of these technologies are at risk. This mistrust can lead to legal challenges, regulatory scrutiny, and reputational damage for the organizations deploying such tools.

Forms of Bias

Bias in generative AI manifests in multiple forms. The most prevalent include:

- **Demographic bias**: Disproportionate error rates across race, gender, or age groups.
- **Cultural bias**: Failure to represent diverse linguistic, geographic, or social norms in global applications.
- **Socioeconomic bias**: Favoring groups with more digital presence or resources due to data imbalance.
- Annotation **bias**: Prejudice introduced during the human labeling process of training data.

Each of these forms contributes to outputs that may seem rational on the surface but, in effect, reinforce structural inequalities.

3.1.3 BIAS IN RESEARCH AND SCIENTIFIC USE OF GENAI

The problem of bias is particularly acute in academic and scientific research, where objectivity is foundational. [215]Generative AI used for literature reviews, data

[213] M. AL-KFAIRY et al., *Ethical Challenges and Solutions of Generative AI: An Interdisciplinary Perspective*, in *Informatics*, 11(3) (2024), p. 58.
[214] Ibid.
[215] AL-KFAIRY et al., *Ethical Challenges and Solutions of Generative AI*

interpretation, or research writing may unintentionally distort findings due to the replication of academic or cultural biases from its training data. Language models, for instance, may overrepresent Western perspectives, underrepresent minority voices, or reinforce gender and racial stereotypes in scientific contexts.

These risks are exacerbated by the opacity of many GenAI tools, which limits researchers' ability to trace and interrogate the origin of biased outputs. When GenAI systems lack transparency, their use in research settings may lead to biased citations, one-sided conclusions, or flawed experimental design.

Strategies to Mitigate Bias[216]

Addressing bias in GenAI is not a one-time technical correction but an ongoing, iterative process. Several mitigation strategies have emerged as best practices:

1. **Inclusive and Representative Data**: Building datasets that account for diversity in gender, ethnicity, language, and geography is foundational. Diverse datasets not only help reduce bias but also improve the model's generalizability[7].
2. **Fairness-Aware Algorithms**: Models can be adjusted to correct for demographic disparities by applying fairness constraints or using debiasing techniques during training.
3. **Bias Detection Tools**: Regular algorithmic audits help identify disparities in performance across demographic subgroups. Metrics such as disparate impact, demographic parity, or equal opportunity provide quantifiable measures of fairness[8].
4. **Transparency and Explainability**: Making the model's decision-making process accessible through tools like SHAP or LIME supports auditability, user trust, and accountability.
5. **User Feedback Loops**: Incorporating real-world feedback can expose unforeseen biases and support model retraining or refinement based on diverse user experiences.
6. **Ethical Oversight Structures**: Appointing governance bodies, such as internal ethics committees or external advisory boards, ensures independent scrutiny over the deployment of GenAI technologies.[217]

Transparency does not eliminate bias, but it is a necessary condition for identifying and mitigating it. Transparent systems allow developers, auditors, and users to understand

[216] WEIJIA – MIAOMIAO, *The Analysis of Technological Ethical Issues in Generative Artificial Intelligence*.
[217] AL-KFAIRY et al., *Ethical Challenges and Solutions of Generative AI*, cit.

how decisions are made, what data are used, and where the model might fail. Transparency enhances trust and enables informed consent in AI interactions. In practice, transparency should extend to dataset documentation, algorithm selection rationale, and post-deployment monitoring.[218]

Transparent processes also promote accountability. When developers know their systems are open to external evaluation, they are more likely to build with fairness in mind. Institutions that enforce transparent design principles are better positioned to detect risks early, respond effectively to public concerns, and align AI outputs with broader ethical norms.

Despite progress in identifying and mitigating bias, several challenges remain. First, there is no universal agreement on fairness definitions, making it difficult to implement consistent standards across applications. Second, mitigation techniques may involve trade-offs improving fairness for one group might inadvertently worsen outcomes for another. Third, many bias detection tools rely on demographic labels, which may not always be available or ethically appropriate to collect.

Additionally, while the literature addresses bias in broad terms, there is limited guidance on tailoring interventions to specific use cases. For example, mitigating bias in medical diagnosis tools requires different considerations than addressing bias in content generation platforms. Sector-specific ethical frameworks are still underdeveloped, and real-world case studies are needed to refine best practices.

Bias in generative AI is a multifaceted challenge with far-reaching implications. It originates from both data and design and manifests in ways that can entrench social inequalities if left unchecked. Addressing bias requires technical vigilance, institutional commitment, and societal dialogue. [219]While no single strategy suffices, the integration of inclusive design, transparency, ongoing auditing, and ethical oversight can collectively reduce harm and promote fairness. A responsible AI future hinges on recognizing that fairness is not a passive outcome but an active process requiring persistent attention.

To address the bias risk, Article 10 AI Act requires that training, validation, and testing datasets be relevant, representative, and managed under sound governance practices. At the same time, GDPR Article 9 strictly regulates the processing of special categories

[218] BJELOBABA et al., *Research Integrity and GenAI: A Systematic Analysis of Ethical Challenges Across Research Phases*, in arXiv, preprint, 13 dicembre 2024, p.

[219] *systemic Bias in Artificial Intelligence: Focusing on Gender, Racial, and Political Biases*, in
Journal of Artificial Intelligence Practice, 7(3) (2024), p

of personal data, such as race, ethnicity, or religion that are often necessary to detect and mitigate bias. This creates a legal tension: the AI Act demands representative datasets, but the GDPR limits the use of sensitive data. Businesses deploying generative AI must therefore navigate overlapping rules that are not always aligned.

Bias mostly violates Articles 9 and 22 of the GDPR. Processing sensitive categories of data is forbidden by Article 9 unless express agreement is obtained or there are certain exceptions. However, engineers must examine these types of data in order to test whether a generative AI system discriminates, for example, by rejecting job applications disproportionately based on ethnicity. Discriminatory results continue in the absence of such testing. In addition, Article 22 limits fully automated choices that have legal or comparable important consequences, including computerized credit rating or employment. Human intervention and the ability to challenge choices must be made available by businesses. These protections are immediately compromised by bias in generative AI outputs, as discriminatory decision-making cannot be excused as "solely automated" under the GDPR.

The AI Act tackles bias more explicitly. Article 10 sets requirements for dataset quality in high-risk AI systems, demanding that data be relevant, representative, free of errors, and complete. This provision is designed to prevent systemic bias at the source. Foundation models such as ChatGPT are increasingly treated as high-risk by default, which subjects their developers to risk management, transparency, and non- discrimination duties. Non-compliance can result in fines of up to 6% of global turnover mirroring GDPR’s sanctioning regime.

Hacker, Engel, and Mauer argue that discrimination cannot be delegated to deployers alone. Unlike other risks that users can mitigate, bias must be addressed “at the root” during data curation and model training. They propose audits for representativeness, balancing between groups, and supplementing training sets with synthetic data to counter historical inequalities.

At the same time, they highlight the compliance dilemma created by the interaction of GDPR and the AI Act. To comply with Article 10 AI Act, developers must curate datasets that are representative across sensitive categories. But Article 9 GDPR makes the processing of these very categories legally difficult. This conflict leaves developers relying on narrow bases such as explicit consent or substantial public interest, or on technical alternatives like federated learning and synthetic data.

Sanctions illustrate how regulators interpret these obligations. The Italian Data Protection Authority’s 2023 suspension of ChatGPT for insufficient transparency demonstrated that supervisory authorities are willing to suspend services altogether. The AI Act introduces even higher stakes by attaching systemic non-discrimination obligations to foundation models, exposing them to fines that parallel GDPR enforcement.

For businesses, bias in generative AI creates both risks and opportunities. The risks are legal, financial, and reputational. Companies deploying biased AI systems in high-risk sectors such as hiring or credit scoring may face liability under both GDPR Article 22 and AI Act Article 10. Enforcement can involve service suspensions, heavy fines, and reputational damage. The compliance dilemma also raises costs: developers must conduct bias audits, curate datasets, and explore lawful bases for sensitive data processing.
Yet compliance can also be a market advantage. Firms that integrate fairness and transparency into their models early may gain consumer trust and secure contracts. In highly regulated sectors, demonstrating compliance with both GDPR and AI Act safeguards may become a prerequisite for doing business in the EU. Conversely, smaller developers and open-source projects may struggle with these obligations, risking a market shift towards larger corporations with greater compliance resources. Bias is not only a technical challenge but also a legal one. GDPR Articles 9 and 22 and AI Act Article 10 form a dual regime that forces developers and deployers to address discriminatory risks in generative AI. The two instruments are not fully aligned, creating compliance dilemmas but also opportunities for innovation in privacy- preserving fairness techniques. For businesses, the lesson is clear: bias is both a liability and a strategic variable. [220]Those who treat compliance as governance and design practice may transform regulatory risk into a competitive edge.

3.1.4 PRIVACY CONCERNS RELATED TO DATA USAGE IN AI

As artificial intelligence systems become increasingly embedded in business operations, the volume and sensitivity of data they require and process has raised

[220] P. HACKER et al., *Regulating ChatGPT and Other Large Generative AI Models*, in *Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency* (New York, NY, USA), FAccT '23, Association for Computing Machinery, 12 giugno 2023, pp. 1112–1123.

complex privacy concerns. Generative AI, in particular, depends on vast datasets for training, often drawn from publicly available content, commercial databases, or internal organizational systems. These datasets frequently contain personal or sensitive information, creating a spectrum of privacy risks. These risks are not theoretical: they are already materializing in various industries, particularly those that handle detailed personal profiles such as human resources and education.

1. General Privacy Risks in AI Systems

The main privacy issue with AI is the possibility of personal data being misused, leaked, or collected in excess. In order to produce forecasts, suggestions, or automatic outputs, AI models frequently consume vast amounts of data, such as names, demographics, work histories, and even medical records. On the other hand, improper management may result in unapproved access, data breaches, or unintentional exposures. Model memorization the process by which models "remember" and replicate portions of their training data is one of the particular dangers connected to generative AI. This implies that outputs produced by an AI system trained on sensitive or unfiltered content may inadvertently reveal personal information.

Further, data collection practices are not always transparent. Individuals may not know that their information has been used to train or operate AI models, particularly when data is scraped from the internet or collected indirectly. [221]When anonymization techniques are weak or absent, there is also the risk of re-identification, where individuals can be matched with supposedly anonymous data through inference attacks.

2. Privacy in Practice: Human Resources and Education

These general risks take on specific, tangible forms in business settings. In the human resources (HR) domain, generative AI is increasingly used to streamline recruitment, assess employee performance, and support workforce planning. These systems often rely on employee profiles, application documents, or behavioral data. If this information is processed without adequate safeguards, it can result in major privacy violations including exposing salary histories, health records, or internal evaluations[3]. Worse, employees may not be aware of the extent to which their data is being used, especially if consent mechanisms are unclear or bundled into general terms of employment.

Similarly, in education, AI-enhanced platforms personalize learning experiences and assess student progress. These functions rely heavily on continuous data collection from test scores to behavioral analytics and participation metrics. In this setting, the privacy risk is heightened by the fact that many users are minors or lack full digital

[221] P. ZLATEVA, D. VELEV, *Generative AI Privacy Issues*, IOS Press Ebooks, [s.d.], p.

literacy. Even well-intentioned systems may inadvertently breach student privacy if data is reused for secondary purposes, shared with third parties, or stored indefinitely without proper review.

In both cases, the ethical challenge is not just the collection of data, but its long-term storage, lack of user awareness, and the difficulty of withdrawing consent. [222]Once data has been used to train a model, it is technically challenging if not impossible to extract it, which means the risks extend far beyond the original moment of data capture.

3. Technical Safeguards: Understanding the Tools

To mitigate privacy risks, several privacy-preserving technologies have been developed. While they are often presented as technical solutions, they can and should be understood by business professionals, as they have direct implications for compliance, trust, and operational design.

Differential privacy is one of the most widely adopted tools. It works by adding statistical "noise" to a dataset or a model's output in a way that ensures no individual's data point significantly affects the result. In simple terms, it hides the presence or absence of a particular individual in a dataset, reducing the risk of re-identification. For example, a generative AI model trained with differential privacy techniques will be far less likely to reproduce personal data from its training set. However, this comes at a cost: the more noise is added, the less precise the model becomes. Businesses must therefore calibrate the level of privacy protection to balance utility and safety.

Homomorphic encryption allows AI systems to perform calculations on encrypted data without needing to decrypt it first. This means that sensitive data remains protected throughout the entire process even during analysis or processing. For instance, a financial services provider could use homomorphically encrypted data to assess loan risk without ever accessing the customer's raw financial records. While promising, this technique is computationally intensive and may slow down real-time applications, making it better suited for sensitive, non-urgent tasks.

Federated learning addresses the risk of centralizing sensitive data. Rather than moving all the data to a central server, federated learning allows models to be trained locally on user devices (such as phones or laptops) and only sends the learned parameters not the data itself back to a central system. This approach reduces the chance of data leaks in transit or from a central database, which is particularly useful in applications involving consumer devices or health monitoring apps.[223] The trade-

[222] I. A. ISMAIL, I. A. ISMAIL, *Protecting Privacy in AI-Enhanced Education: A Comprehensive Examination of Data Privacy Concerns and Solutions in AI-Based Learning*, capitolo, IGI Global Scientific Publishing, 1 gennaio [s.d.], p.

[223] I. A. ISMAIL – I. A. ISMAIL, *Protecting Privacy in AI-Enhanced Education*.

off, however, is in coordination and communication overhead, as well as a potential loss in model accuracy.

Secure multi-party computation (SMPC) enables multiple parties to collaboratively compute a result without sharing their individual inputs. For example, two hospitals could compare treatment outcomes using SMPC while keeping their patient records confidential. Like homomorphic encryption, this method offers high security but requires careful implementation and computational resources.[224]

Together, these tools offer businesses a robust set of options to protect personal data. However, each comes with limitations, and their effectiveness depends on context, implementation skill, and alignment with legal requirements.

4. Regulatory Frameworks and Compliance Strategies

From a legal perspective, data privacy risks are primarily addressed through frameworks such as the GDPR in the European Union and the CCPA in California. These regulations establish fundamental principles like purpose limitation, data minimization, and the requirement for lawful, transparent processing. In the context of AI, this means organizations must demonstrate that they are collecting only the data necessary for a specific, stated purpose and that they are taking adequate steps to protect it.

Importantly, these regulations require that data subjects (i.e., users, employees, students, or consumers) be informed about how their data is used, and in many cases, they must provide explicit consent. In dynamic AI systems, where data usage evolves over time, this implies an ongoing obligation to update users and re-obtain consent as necessary.

Privacy-by-design and privacy-by-default principles are also central to regulatory compliance. These mean that privacy considerations should be built into systems from the outset, rather than added after problems arise. [225]Businesses must not only apply technical measures but also establish governance structures such as data protection officers, regular audits, and transparent reporting to demonstrate compliance and accountability.

5. A Balanced Approach to Privacy and Innovation

[224] L. SINGH et al., *Ethical and Regulatory Compliance Challenges of Generative AI in Human Resources*, in *Generative Artificial Intelligence in Finance*, John Wiley & Sons, Ltd, 2025, cit.

[225] I. A. ISMAIL – I. A. ISMAIL, *Protecting Privacy in AI-Enhanced Education*, cit.

While the risks are significant, it is neither necessary nor practical to abandon the use of AI in sensitive domains. [226] The key lies in designing systems that strike a balance between data utility and individual rights. As noted in studies of administrative data usage, overly aggressive anonymization can render data useless, while lax protection endangers privacy. Businesses must therefore adopt a risk-based approach tailoring their privacy protections to the sensitivity of the data and the context of its use.

Moreover, fostering a culture of ethical awareness among developers, managers, and users is essential.[227] Privacy is not simply a technical problem, or a compliance checklist is an ongoing ethical responsibility that must be embedded in corporate practice.[228]

The ethical challenges surrounding privacy in AI are both complex and deeply practical. They manifest in everyday business functions, from hiring to education and beyond. However, they can be effectively managed through a combination of regulatory compliance, technical innovation, and organizational accountability. [229]By understanding the specific ways in which privacy risks emerge and by adopting clear, accessible mitigation strategies businesses can build AI systems that are not only powerful but also trusted, lawful, and ethical.

7. Legal Framework and Business Implications

Generative AI systems process vast amounts of personal data, raising significant privacy concerns. In the EU, the GDPR establishes the baseline for protection, embedding principles of consent, minimization, accountability, and security in Articles 5, 22, 24–25, 32, and 35. Recital 39 GDPR reinforces these principles, requiring that individuals be made aware of how their data is collected, used, and accessed, and to what extent it is processed. Recital 71 adds that safeguards are necessary in automated decision-making to avoid discrimination and opacity. Recital 75 further highlights the risks of unlawful or disproportionate processing, including identity theft, discrimination, reputational damage, and financial loss.

The AI Act complements the GDPR with system-level requirements. Articles 9 and 10 impose obligations on risk management and data governance for high-risk AI systems,

[226] C.-K. TING, *Quest for the Balance of AI and Privacy [Editor's Remarks]*, in *IEEE Computational Intelligence Magazine*, 17(3) (2022), pp. 2–2.
[227] Ibid
[228] M. COMERFORD, *Examining Disclosure Risk and Data Utility: An Administrative Data Case Study*, in *International Journal of Digital Curation*, 9(1) (2014), pp. 12–24.
[229] I. A. ISMAIL – I. A. ISMAIL, *Protecting Privacy in AI-Enhanced Education*, cit.

while Articles 5 and 6 establish prohibitions and risk classification rules. Together with the Digital Services Act (DSA) and Cyber Resilience Act (CRA), these frameworks create a multi-layered but fragmented regulatory landscape for privacy in AI.

The GDPR provides concrete individual-level protections. Article 5 requires data minimization and purpose limitation, which directly constrain practices such as training generative models on indiscriminately scraped internet data.

Article 22 prohibits decisions made solely through automated processing where such decisions have legal or similarly significant effects. This safeguard is especially relevant in hiring and credit scoring. An AI system that rejects applications without human oversight creates exactly the harm Article 22 seeks to prevent. The Court confirmed this broad interpretation in *Schufa* (CJEU, C-634/21, 2023), holding that reliance on credit scores alone can constitute an Article 22 decision.

Article 35 introduces an ex ante requirement for Data Protection Impact Assessments (DPIAs) in high-risk processing operations. Controllers must assess risks and embed safeguards before deployment, ensuring that systems respect the principles of lawful, fair, and accountable processing.

The AI Act builds on GDPR safeguards but extends them to system-level governance. Articles 9 and 10 require high-risk AI providers to establish risk management procedures and data governance frameworks. Datasets used for training and testing must be relevant, representative, and free of errors.

Recital 42 highlights the need for fundamental rights impact assessments, while Recital 44 stresses that training data must be "relevant, sufficiently representative, and free of errors." High-risk AI systems are also subject to conformity assessments before being placed on the market, now codified in Articles 43–51 of the final AI Act. These provisions reinforce accountability and oversight.

The sanctions are severe: violations of data governance, transparency, or banned practices can result in fines of up to 6% of global yearly turnover, which is more than the 4% level set by the GDPR.

The way these duties are carried out is demonstrated by enforcement practice. The Italian Data Protection Authority temporarily stopped ChatGPT in April 2023 for not being sufficiently transparent about how it processed data. GDPR Articles 5(1)(a) (lawfulness, fairness, transparency), 13 (information responsibilities), and 32 (security) served as the foundation for the ruling. This example demonstrates that when privacy and transparency requirements are not fulfilled, regulators will halt AI services, converting theoretical protections into real-world commercial dangers.

Bolgouras and colleagues argue that no single regulation can fully address privacy risks in AI. GDPR remains the foundation, but fragmentation with the AI Act, NIS2, CRA, and DSA creates compliance complexity and undermines trust. They call for harmonisation to make privacy protections coherent and enforceable.

Beltrán (2025) [230] conceptualises GDPR, AI Act, DSA, and CRA as four complementary pillars. GDPR Articles 5, 22, 24–25, 32, and 35 safeguard individual rights. AI Act Articles 5, 6, 9, and 10 address systemic governance. The DSA regulates platform-level risks, and the CRA secures product vulnerabilities. Integration of these regimes into a multi-layered framework, he argues, reduces duplication and positions the EU as a global leader in trustworthy AI.

For businesses, privacy obligations are both burdensome and strategic. Non-compliance exposes firms fines up to 4% of turnover under GDPR and 6% under the AI Acts as well as reputational harm. The ChatGPT suspension illustrates that regulators will not hesitate to halt AI services where safeguards are absent. In sensitive sectors, such interventions pose immediate financial and contractual risks.

At the same time, compliance can be a competitive differentiator. Privacy- and security-by-design approaches reduce sanction exposure and foster consumer trust. Beltrán notes that compliance with CRA cybersecurity obligations can also serve as evidence of conformity under the AI Act, creating synergies across regimes.

Yet fragmentation in DPIA triggers across Member States, combined with overlapping AI Act requirements, raises transaction costs and legal uncertainty. SMEs are particularly exposed, as they lack the resources of larger firms, contributing to market concentration and competitive imbalance.

Privacy in generative AI sits at the intersection of individual rights under the GDPR and systemic obligations under the AI Act. GDPR Articles 5, 22, and 35, reinforced by Recitals 39, 71, and 75, impose strict requirements on minimization, automated decision-making, and risk assessments. AI Act Articles 9 and 10, supported by Recitals 42 and 44, extend governance to data quality and systemic risk, while conformity assessments under Articles 43–51 provide ex ante oversight.

Enforcement practice, including the ChatGPT suspension, demonstrates that regulators act decisively when transparency and privacy safeguards are absent. The literature highlights fragmentation as a persistent challenge, but also points to harmonisation as a path to coherence. For businesses, privacy is both a compliance duty and a source of legitimacy. [231]Those that embed privacy into design and governance can transform regulation from a burden into a competitive advantage.

3.1.5 TRANSPARENCY AND EXPLAINABILITY OF AI DECISIONS

[230] M. BELTRÁN, *AI Algorithms under Scrutiny: GDPR, DSA, AI Act and CRA as Pillars for Algorithmic Security and Privacy in the European Union*, in *Computers & Security*, 158 (novembre 2025), 104628.

[231] Ibid.

As artificial intelligence (AI) systems assume ever more critical roles in decision-making, transparency and explainability have become central to both technical design and organizational strategy. Without clear insight into how algorithms process data and arrive at specific outcomes, stakeholders face a "black-box" dilemma that erodes trust, hampers adoption, and raises legal and ethical risks. Here, **transparency** refers to the visibility of a model's structure and data flows, while **explainability** denotes the ability to articulate why a particular input produces a given output.[232] This distinction underpins the methods and frameworks discussed below; each aimed at ensuring that AI-driven decisions remain both intelligible and actionable.

1. Enhancing Human Decision-Making Accuracy

Explanations can materially improve human performance when interacting with AI. In a mushroom-foraging experiment, 328 participants were split evenly into two groups: one received only AI edibility classifications, while the other also received visual explanations attribution heatmaps and example-based illustrations. Those with explanations outperformed the control group, demonstrating that clear, context-rich cues significantly boost decision quality. [233]Although the immersive art-festival setting amplified engagement, it did not itself inflate accuracy, suggesting the effect stems from the explanations rather than the venue. Interestingly, however, these gains did not translate into higher self-reported trust, indicating that explainability alone may not address deeper concerns about fairness or error rates.

2. Integrating Explainability into Decision Frameworks

Rather than treating explainability as an afterthought, leading organizations weave it directly into decision-support workflows. One exemplary approach combines Explainable AI (XAI) with the Analytic Hierarchy Process (AHP): machine learning models forecast outcomes (e.g., customer support needs or product profitability), then apply feature-importance scoring and local surrogate models to reveal each prediction's drivers. These insights feed into AHP's pairwise comparison matrices, enabling stakeholders to weigh criteria based on both strategic priorities and empirical evidence of model reliance. Built-in consistency checks flag discrepancies between human judgments and algorithmic rationale, ensuring decisions balance data-driven

[232] M. T. DEY, M. T. DEY, *Explainable Artificial Intelligence (XAI): Integration, Policy Frameworks, and Applications in Critical Domains and Renewable Energy*, capitolo, IGI Global Scientific Publishing, agosto 2024, p. 20.
[233] Ibid

precision with managerial expertise. [234]The result is a transparent ranking of actions, such as reallocating support staff or reprioritizing R&D, that is both auditable and strategically coherent.

3. Techniques for Model Interpretability

XAI methods can be grouped into **global** techniques that reveal overall model behavior and **local** techniques that explain individual predictions.

Global explainability techniques clarify how an entire model behaves across all data points; [235]

- **SHAP (Shapley Additive Explanations)** ranks the most influential features for the whole model and is model agnostic, making it applicable to any algorithm.
- **Sensitivity Analysis** perturbs input data and observes resulting output changes, offering a model-agnostic way to gauge overall feature impact.
- **Counterfactual Explanations** are model-specific; they create alternative input scenarios to show how small changes would alter a model's output, giving a global view of decision boundaries.
- **Feature Importance Analysis** measures how adjusting each feature's value affects the model's outputs; although model-agnostic, it can serve both global and local purposes. **Local explainability techniques** focus on individual predictions.
- **LIME (Local Interpretable Model-Agnostic Explanations)** builds a simple surrogate model around a single instance, yields the lowest error rates for individual predictions, and balances fidelity with interpretability by minimizing a joint loss-and- complexity objective.
- **SHAP's local component** while known for global explanations, SHAP assigns contribution values to each feature for a specific case while retaining its model-agnostic property, though its per-instance accuracy is lower than LIME's.

Combining global and local methods ensures that both strategic planners and operational users understand AI outputs and know how to act on them.[236]

To bridge sector-focused insights and SME implementation, it is crucial to recognize how explainability scales from enterprise frameworks to resource-constrained contexts.

4. Operationalizing Explainability in SMEs

Small and medium-sized manufacturers can transform their learning factories into low- cost innovation labs by adding edge-computing nodes and virtualised sensor streams.

---

[234] M. T. DEY – M. T. DEY, *Explainable Artificial Intelligence (XAI)*.

[235] , *A Methodological Framework for Business Decisions with Explainable AI and the Analytic Hierarchical Process*, [s.d.]consultabile su https://www.mdpi.com/2227-9717/13/1/102.

[236] M. T. DEY – M. T. DEY, *Explainable Artificial Intelligence (XAI)*, cit.

These test-beds pair real-time IoT data with lightweight machine-learning models and overlay explainable-AI tools that reveal which signals drive each prediction. The lab setting provides a safe, scaled-down environment to pilot use-cases, such as predictive maintenance or quality-control analytics before committing to full-scale rollout. In this way, SMEs can experiment with data-driven processes, build stakeholder trust through XAI-enabled transparency, and avoid the large up-front investments a full production deployment would demand.

5. Addressing Challenges and Trade-offs

Implementing XAI brings its own costs. Generating detailed explanations can strain computational resources at scale, and overly detailed outputs may overwhelm non- technical users.[237]

Moreover, simpler models risk misrepresenting true decision logic, while sophisticated models remain opaque. To sustain transparency, organizations should build on inherently explainable or XAI-ready models and deliver concise, role-tailored explanations using techniques like saliency maps, attention visualizations, or rule paths while continuously auditing those explanations for clarity, fairness, and user trust throughout the model's life cycle.

6. Regulatory Imperatives under GDPR

Explainability and openness are enshrined as essential rights in the General Data Protection Regulation (GDPR) of the European Union. Organizations are required to give data subjects clear, understandable information regarding automated decision logic and its possible effects. Customer trust might be damaged and heavy fines imposed for noncompliance. In addition to avoiding fines, open methods reduce legal risks, promote informed consent, and set businesses apart in the data privacy stewardship market.

Ultimately, this subsection has shown how transparency and explainability transform AI from inscrutable "black boxes" into legible, trustworthy partners in human decision- making.[238] By defining key concepts, surveying empirical evidence, detailing integration techniques, and mapping regulatory requirements, we lay the groundwork for designing AI systems that stakeholders can understand, trust, and act upon.

7. Legal Framework and Business Implications

[237] Ibid

[238] , The Integration of Machine Learning and Explainable AI in Business Digitization: Unleashing the Power of Data – A Review - Institute of Cited Scientists, [s.d.].

Transparency is a cornerstone of EU data protection and AI governance. The GDPR embeds it through data subject rights and information duties in Articles 12–23, and particularly in Articles 13–15 (information on processing) and Article 22 (rights against automated decision-making). Recital 39 GDPR reinforces this, stating that individuals should be made aware of how their personal data is collected, used, and accessed, and to what extent it is processed.

The AI Act complements these duties. Article 13 requires providers of high-risk AI to ensure transparency and the provision of information. Together, these rules seek to counter algorithmic opacity and restore user trust in data-driven decision-making.

Under the GDPR, transparency goes beyond publishing privacy policies. Articles 13– 15 require controllers to provide clear and accessible information on how data is collected, processed, and used. Article 22 adds a safeguard against fully automated decisions with legal or similarly significant effects.

This safeguard is echoed in Recital 71 GDPR, which warns against decisions made solely through automated processing that could lead to discrimination or lack of transparency. An AI system that automatically rejects a loan application without explanation or recourse directly violates these protections.

The AI Act extends the GDPR framework by imposing system-level duties. Article 13 obliges high-risk AI providers to disclose information that allows users to interpret and properly use outputs. This includes ensuring users understand the system's capabilities and limitations.

Recital 47 AI Act clarifies that transparency is not limited to technical documentation but also requires providers to enable effective user control. Transparency in this sense is both a legal safeguard and a governance tool, ensuring accountability of model design and deployment.[239]

Failures to meet these obligations can trigger sanctions of up to 6% of global turnover, reflecting the EU's recognition of transparency as essential to trustworthy AI. This is not just theoretical: in April 2023, the Italian DPA temporarily banned ChatGPT for lack of transparency about data collection and lawful basis, demonstrating how regulators use transparency duties as an enforcement tool.

Grochowski and colleagues argue that transparency and explainability are essential to address both technological opacity (complex neural networks) and relational opacity (power imbalances between firms and consumers). They stress that GDPR provisions (Arts. 13–15, 22) and consumer protection law must be read together to prevent

[239] , *Algorithmic Transparency and Explainability for EU Consumer Protection: Unwrapping the Regulatory Premises by Mateusz Grochowski, Agnieszka Jabłonowska, Francesca Lagioia, Giovanni Sartor :: SSRN*, [s.d.]consultabile su https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3826415.

manipulation and inequality. Still, they acknowledge that transparency can be costly, since it may require reliance on explainable but less accurate models.
Reyes García critiques existing frameworks through the lens of "privacy fatigue." He argues that lengthy privacy notices and formalistic compliance often fail in practice, producing consumer apathy rather than empowerment. Although GDPR and AI Act transparency provisions are designed to inform, they risk becoming symbolic. He calls for ex ante rights to explanation, including disclosure of DPIAs, to restore meaningful self-determination.
By grave offers a more optimistic view. He argues that GDPR's layered transparency duties (Arts. 13–15) have the potential to empower individuals if implemented effectively. In his account, shortcomings stem less from structural flaws in the law than from poor practices in communication and design.
Transparency duties bring significant costs and risks. Compliance requires investment in clear, accessible communication and sometimes limits the use of high-performing opaque models. Firms that take a "tick-box" approach publishing dense privacy notices without clarity risk fines under GDPR or the AI Act, reputational harm, and even service suspensions, as shown by the ChatGPT ban in Italy.
Yet transparency can also be a strategic opportunity. Businesses that adopt transparency-by-design through layered explanations, interactive disclosures, or proactive communication can reduce privacy fatigue, build consumer trust, and strengthen legitimacy in the EU market. In competitive sectors, transparency is increasingly a prerequisite for market access and long-term success.
Transparency under the GDPR and the AI Act seeks to rebalance informational asymmetries in generative AI. GDPR Articles 13–15 and 22 protect individuals from opaque automated decisions, while AI Act Article 13 and Recital 47 extend these obligations to system-level design and governance.
The literature underscores both the necessity and the limits of transparency: it can empower users and foster trust, but risks becoming symbolic if poorly implemented. For businesses, transparency is both a compliance challenge and a competitive tool. [240]Firms that embed transparency into governance and communication can not only avoid sanctions but also position themselves as trustworthy actors in the EU's regulatory environment.

3.2 BUSINESS DILEMMAS: COMPLIANCE VS. PROFITABILITY

[240] R. GARCIA, J. C. [JUAN CARLOS], *EU's Transparency Obligations in the Era of AI: Is Transparency Enough to End Privacy Fatigue,* SSRN Scholarly Paper 4695423, Social Science Research Network, novembre 2024, p. 25.

3.2.1 THE IMPACT OF ETHICAL CONSIDERATIONS ON BUSINESS STRATEGIES.

Organizations are increasingly recognizing that ethical considerations must be embedded alongside financial targets at the very outset of AI strategy, transforming the traditional business-case into a multi-dimensional charter that balances profit, social impact, and environmental cost. By first codifying clear ethical guidelines such as fairness thresholds, transparency requirements, and data-privacy safeguards firms ensure that AI initiatives proceed only when they meet jointly defined standards for bias mitigation, consent management, and security. Once approved, projects advance through a staged implementation process in which data sources are vetted for sensitivity, models are tested for disparate impacts across subpopulations, and decision-explanation mechanisms are built in to support accountability. Crucially, human judgment remains central: [241]AI outputs are deployed in human-in-the-loop workflows with explicit override protocols, embedding responsibility at every decision point. Real-time monitoring dashboards then track key ethics metrics bias-incident rates, privacy-complaint volumes, and fairness scores while feedback loops drive ongoing retraining and policy updates. Furthermore, these AI systems operate within a broader socio-technical ecosystem, where data pipelines and decision-making algorithms wield significant societal influence and carry environmental consequences. By expanding strategic metrics beyond pure performance to include societal, environmental, and climate costs such as carbon emissions from large-scale model training and embedding responsible-AI frameworks as a strategic differentiator through practical tools like impact assessments, Glass Box architectures, and the Design for Values methodology, firms translate abstract moral principles into concrete system requirements. [242]Moreover, assembling multidisciplinary teams combining engineers with experts in philosophy, social science, law, and economics enables organizations to anticipate unintended harm and design more robust, equitable systems. Finally, moving beyond brute-force approaches toward causality-driven and abstraction- focused models reduces both data and compute demands, turning resource efficiency into a competitive advantage while upholding ethical standards.[243]

Organizations are increasingly reshaping their strategic priorities to embed ethical AI considerations into core decision-making processes, developing clear policies for

---

[241] , *A Methodological Framework for Business Decisions with Explainable AI and the Analytic Hierarchical Process*, [s.d.]consultabile su https://www.mdpi.com/2227-9717/13/1/102.

[242] V. DIGNUM, *Responsible Artificial Intelligence — From Principles to Practice: A Keynote at TheWebConf 2022*, in *SIGIR Forum*, 56(1) (2023), pp. 3:1–3:6.

[243] F. OSASONA et al., *Reviewing the Ethical Implications of AI in Decision Making Processes*, in *International Journal of Management & Entrepreneurship Research*, 6(2) (2024), pp. 322–335.

redress and compensation when AI systems error signaling a shift toward proactive ethical risk management and adopting robust data governance practices (comprehensive documentation, rigorous data-cleaning protocols, informed-consent mechanisms) to ensure both model integrity and regulatory compliance. Establishing permanent ethics committees provides multi-dimensional oversight, guiding trade-offs between operational efficiency and stakeholder obligations, while companies invest in staff training and accountability frameworks that assign clear responsibility for AI outcomes reinforcing transparency and trust. Although deep-learning "black boxes" pose challenges for explainability and bias detection, integrating explainable-AI tools and fairness audits during development mitigates these risks and aligns deployment with corporate values, and when ethical safeguards are treated as strategic assets rather than burdens, firms realize enhanced operational efficiency through automated yet responsible workflows, improved decision accuracy, and stronger stakeholder trust ultimately translating ethical rigor into sustainable competitive advantage. Companies often signal this commitment through formal structures dedicated AI ethics units, mandatory ethics training programs, sponsored research to safeguard reputation and preempt regulation; however, when these measures serve primarily as window dressing ("ethics washing"), they can mask profit-over-principal priorities, with some firms quietly dismantling initiatives that collide with revenue goals even terminating contracts. [244]With internal ethics researchers who raise inconvenient concerns and leveraging self-issued white papers and high-level pronouncements to shape public perception and regulatory expectations without substantially altering profit-driven development practices, making genuine ethical integration deep embedding of policies, incentives, and accountability mechanisms the only path to sustaining stakeholder trust and long-term competitiveness.

3.2.2 CASE STUDIES ILLUSTRATING CONFLICTS BETWEEN COMPLIANCE OBLIGATIONS AND PROFIT MOTIVES

There is a growing conflict between generating shareholder value and complying with regulations as artificial intelligence (AI)[245] pervades every aspect of contemporary business. Businesses must make major adjustments to their profitable business strategies, incur large financial expenditures, and delay operations in order to comply with legal and ethical requirements. On the other hand, disregarding compliance may result in short-term financial gains, but it also exposes businesses to legal repercussions, damage to their reputation, and a decline in stakeholder trust. These

[244] , *The Ethics of AI Ethics. A Constructive Critique | Philosophy & Technology*, [s.d.]consul- tabile su https://link.springer.com/article/10.1007/s13347-022-00557-9.
[245] M. RYAN et al., *An AI Ethics 'David and Goliath': Value Conflicts between Large Tech Companies and Their Employees*, in *AI & SOCIETY*, 39(2) (2022), pp. 557–572.

cases, which range from modest AI companies to multinational IT giants, highlight systemic issues and call for crucial improvements.

Facebook (Meta): Algorithmic Decisions and Whistleblower Revelations

The 2021 revelations from Frances Haugen illustrate how commercial incentives can undermine responsible technology development. Working within Facebook's team focused on platform integrity, Haugen exposed the company's practice of prioritizing engagement metrics and advertising profits over user wellbeing in their algorithmic systems. Her testimony revealed the core tension: implementing safer algorithmic approaches would reduce platform usage and subsequently decrease revenue streams, creating a direct conflict between financial objectives and user protection.

The case underscores several compliances–profit dilemmas:

- **Algorithmic profit incentives:** Facebook embedded engagement maximization into its core ranking algorithms, prioritizing revenue over platform safety and ethics.
- **Whistleblower vulnerability:** Haugen faced significant backlash, highlighting how corporate resources can silence or marginalize ethical advocacy through public disputes and reputational attacks.
- **Regulatory gaps:** The absence of mandatory external algorithmic audits allowed profit-driven algorithmic strategies to continue unchecked, emphasizing the urgent need for robust external regulatory frameworks.

Google: Internal Suppression of Ethical Critique

The controversy surrounding Google's AI ethics division, involving Dr. Timnit Gebru and Dr. Margaret Mitchell, further highlights the tension between compliance obligations and corporate profits. Google's suppression of their critical research on large language models deemed “unsuitable for publication” protected profitable AI operations from scrutiny. Despite extensive internal protests from thousands of employees, Google selectively resisted transparency demands, illustrating profit- driven conditional ethical compliance.

Key tensions from this case include:

- **Control over ethical research:** Google’s decision shielded lucrative AI-training processes, demonstrating an unwillingness to compromise profit for transparency.
- **Selective responsiveness:** Google’s previous responsiveness to employee activism on defense contracts starkly contrasts its stance on AI ethics, revealing selective compliance driven by profitability considerations.
- **Chilling effects:** The suppression sent a clear message deterring internal critique and weakening ethical oversight, underscoring the inadequacy of voluntary compliance mechanisms and the necessity for external regulatory mandates.

PerceptIn: Financial Impact of Compliance on Innovation

Smaller firms like PerceptIn illustrate compliance-driven financial pressures distinct from reputational challenges. Their deployment experiences in China, Europe, and Japan reveal that compliance obligations frequently surpassed initial profitability projections:

- **China: Regulatory uncertainty:** Lack of clear standards resulted in unplanned monthly compliance costs of $25,000, totaling $300,000 annually, significantly affecting financial planning and innovation capacity.
- **Europe: Budget overruns:** Initial compliance budgets drastically inflated from $10,000 to $200,000 due to stringent regulatory demands, severely impacting profitability and innovation resources.
- **Japan: Delayed market entry:** Compliance expenditures, including $500,000 on marketing and regulatory materials over 24 months, significantly delayed market entry, creating opportunity costs that hindered product development and competitive positioning.

These financial pressures highlight how compliance obligations can divert crucial resources away from innovation, forcing startups to choose between rapid market entry and adherence to complex regulatory frameworks.

Across these cases, recurrent themes illuminate the persistent compliance-profit conflict:

1. **Power Imbalances:** Large corporations utilize institutional resources to suppress ethical critiques, while smaller startups face debilitating financial compliance burdens.
2. **Selective Ethics Compliance:** Companies typically comply with ethical obligations when aligned with profitability, retreating otherwise, thereby undermining trust.
3. **Hidden Opportunity Costs:** Regulatory compliance often redirects valuable technical resources from innovation to compliance activities, eroding long-term competitive advantage.

1. Recommendations Towards a Sustainable Equilibrium

Addressing these systemic tensions requires robust, actionable reforms:

- **Independent Ethics Oversight Bodies:** Establish domain-specific, external oversight bodies empowered to audit algorithmic practices, enforce transparency, and adjudicate ethical disputes independently.
- **Enhanced Whistleblower Protections:** Strengthen legal protections and establish confidential reporting channels to safeguard whistleblowers, reducing corporate retaliation risks.

- **Proportional Regulatory Models:** Introduce tiered compliance standards based on company size, technological impact, and deployment context to ensure fairness and prevent excessive burdens on startups.
- **Mandatory Impact Assessments:** Require comprehensive, transparent assessments of AI systems' ethical risks prior to deployment, with enforceable accountability mechanisms.
- **Dedicated Compliance Units:** Encourage separation of compliance and innovation teams to preserve core R&D productivity and innovation capabilities.

[246]Integrating these reforms into corporate and public governance frameworks can realign compliance and profitability, enabling organizations to harness AI's transformative potential responsibly and sustainably.

3.2.3 STRATEGIES FOR INTEGRATING ETHICAL PRACTICES WITHOUT COMPROMISING COMPETITIVENESS

In my view, forward-looking companies are beginning to treat ethical AI less as a regulatory box-ticking exercise and more as a strategic lever for innovation, trust, and lasting value. [247]The real challenge is to weave meaningful safeguards into AI systems without dulling the speed, agility, or cost discipline that power competitive advantage. The discussion below sketches practical ways spanning governance, operations, technical design, and culture to strike that balance between ethics and performance.

1. Establish Dual Governance: Principles Plus Controls

Ethical AI efforts succeed when high-level principles are tightly coupled with concrete governance controls. A stepwise implementation process begins by codifying foundational values such as fairness, transparency, and accountability into a corporate charter, then operationalizes them through an ethics board and formal policies. [248]This board supervises policy development, approves high-risk projects, and enforces accountability. Importantly, governance structures should leverage existing compliance functions (e.g., legal, risk management) rather than create redundant layers, ensuring efficiency and reducing overhead.

2. Leverage Structured Frameworks for Systematic Oversight

Frameworks like the EMMA (Ethical Management of Artificial Intelligence) model

---

[246] W. WU, S. LIU, *Compliance Costs of AI Technology Commercialization: A Field Deployment Perspective*, in arXiv, preprint, 31 gennaio 2023, p.
[247] R. EITEL-PORTER, *Beyond the Promise: Implementing Ethical AI*, in *AI and Ethics*, 1(1) (2020), pp. 73–80.
[248] Ibid

provide an end-to-end roadmap, embedding ethics into strategic planning, tactical resource allocation, and day-to-day operations. Through this lens, AI initiatives are assessed not only for technical feasibility but also for social impact, environmental risk, and stakeholder alignment. An accompanying AI positioning matrix categorizes projects by self-learning complexity and potential human impact, allowing firms to apply stringent oversight where needed (e.g., autonomous decision systems) while fast- tracking lower-risk applications (e.g., basic analytics). Such targeted allocation preserves agility in core revenue streams.

3. Integrate "Red Teams" and "Fire Wardens" for Proactive Testing

Ethical gaps often surface under real-world conditions. To anticipate failure modes, organizations can deploy adversarial "Red Teams" cross-functional groups tasked with stress-testing models for bias, privacy leaks, and security vulnerabilities. Complmenting them, "Fire Wardens" continuously monitor live systems, triggering rapid incident response when anomalies arise. [249]By embedding these roles within product teams rather than as external auditors, firms maintain rapid iteration cycles while ensuring that safety checks occur in parallel with development.

4. Adopt an "AI-in-the-Loop" Mindset

Rather than pursuing full automation, an "AI-in-the-Loop" approach positions AI systems as decision-support tools under human supervision. In this model, AI flags potential risks, such as outlier transactions or discriminatory predictions while human experts exercise final judgment. [250]This division leverages AI's data-processing strengths and human contextual understanding, enabling faster decision-making without ceding accountability. Practically, workflows must specify override protocols, audit logs of human interventions, and clear escalation paths for ambiguous cases.

5. Implement Continuous Monitoring and Feedback Loops

Ethical compliance is dynamic, as data distributions shift and social norms evolve. Organizations should instrument models with monitoring dashboards that track key metrics bias scores across demographic cohorts, privacy-breach incidents, and system explainability indices. Feedback from end users and external stakeholders feed into regular model retraining, policy updates, and governance reviews. By treating ethics as

[249] , *Ethical Management of Artificial Intelligence*, [s.d.]consultabile su https://www.mdpi.com/2071-1050/13/4/1974.
[250] Ibid.

an ongoing lifecycle rather than a one-off assessment, businesses ensure enduring alignment with both regulatory standards and customer expectations.

6. Build Diverse, Multidisciplinary Teams

AI developers bring essential technical skills, but ethical implementation demands broader expertise. Incorporating professionals from social sciences, law, and domain- specific fields helps anticipate societal impacts and navigate regulatory nuance. Equally important is demographic diversity, which reduces blind spots in design and testing. Cross-disciplinary collaboration can be formalized through rotating "ethics ambassadors" embedded in project teams, ensuring that ethical perspectives inform every phase from data collection to deployment.

7. Optimize Technical Architectures for Efficiency and Responsibility

Ethical AI doesn't have to rely on massive, resource-hungry models. Leaner design choices, such as working with well-curated data sets, pruning or compressing models, and using architectures suited to the task at hand, can deliver strong results while keeping compute demands and energy use in check. These efficiencies help defray the extra effort spent on ethical safeguards, turning responsibility and competitiveness into complementary goals.

8. Quantify Ethical ROI to Secure Executive Buy-In

Framing ethics as a driver of financial value is crucial for leadership support. Firms that scale AI with structured governance report return nearly three times higher than those with ad-hoc approaches, due to reduced rework, fewer regulatory fines, and stronger reputational capital. [251]By quantifying cost-savings from prevented bias incidents, churn reductions from increased customer trust, and market premiums for certified ethical products, organizations can embed ethical metrics such as "bias- adjusted revenue" or "sustainability-weighted ROI" into executive dashboards and investment criteria.

9. Foster an Ethical Culture Through Training and Incentives

Finally, technology alone cannot guarantee ethical outcomes. Employees across functions need training on AI's capabilities, limitations, and ethical pitfalls, with regular workshops on scenario analysis, red-flag identification, and compliance protocols. Centive structures ranging from recognition programs for ethical innovation to performance evaluations tied to ethics metrics reinforce responsible behavior. Leadership must model this commitment by including ethical AI progress as a standing

[251] R. EITEL-PORTER, *Beyond the Promise: Implementing Ethical AI*, in *AI and Ethics*, 1(1) (2020), pp. 73–80.

agenda item in executive meetings. By weaving these strategies into their operating models, organizations can transform ethical AI from a compliance burden into a competitive differentiator. Robust governance frameworks ensure accountability without stifling innovation; operational tactics like Red Teams and AI-in-the-Loop preserve agility while managing risk; and technical optimizations align responsibility with efficiency.[252]

Moreover, quantifiable ethical ROI and a culture of continuous learning foster executive buy-in and stakeholder trust alike. [253]Together, these practices demonstrate that ethical excellence and market success need not be mutually exclusive but can reinforce each other to deliver sustainable business value.

CONCLUSION

This thesis has explored the legal and regulatory challenges that generative artificial intelligence presents in business decision-making. It has shown that while generative AI can greatly improve efficiency and innovation, its use raises serious concerns about accountability, transparency, and fairness. The main problem identified is the fragmented and overlapping regulatory framework within the European Union.

Chapter 1 demonstrated how the Artificial Intelligence Act represents the EU's most thorough attempt to regulate AI through a risk-based compliance framework. Providers and users of high-risk systems must meet obligations concerning risk management, data governance, transparency, and post-market monitoring, along with severe penalties for non-compliance. Chapter 2 illustrated how these obligations create real challenges for businesses. Cases like SCHUFA and Uber confirm that algorithmic scores and automated deactivations must be treated as binding decisions, which broadens the area of accountability under current law. Therefore, businesses face added compliance burdens, legal uncertainty, and rising costs, especially when they operate across borders. Chapter 3 highlighted ethical issues of bias, privacy, and lack of clarity. These problems cannot be fixed by legal frameworks alone; firms need to integrate responsibility into their governance structures.

Taken together, these findings suggest that compliance should be seen not just as a legal requirement but as a tool for governance. Companies that view compliance as a strategy rather than a limitation are more likely to build trust, ensure accountability, and secure long-term legitimacy in competitive markets. From a policy standpoint, the analysis indicates the need for harmony between the AI Act and existing regulations like the GDPR, to reduce fragmentation and provide businesses with clearer guidance.

Ultimately, the European Union faces the challenge of balancing innovation with protection. Regulating generative AI must ensure fundamental rights while allowing businesses to responsibly tap into its potential. This thesis argues that achieving this balance requires recognizing compliance as a foundation for governance and placing accountability and transparency at the core of AI-driven business decision-making.

References

BELTRÁN M., AI algorithms under scrutiny: GDPR, DSA, AI Act and CRA as pillars for algorithmic security and privacy in the European Union, *Computers & security*, 158, 2025.

BUTT J. S., Analytical Study of the World's First EU Artificial Intelligence (AI) Act, 2024, *International journal of research publication and reviews*, 5 (33), 2024.

DEY D. - D. BHAUMIK, *APPRAISE: a governance framework for innovation with AI systems*, 2023.

HAYWARD A. - A. TODD - C. REYNOLDS, *Meeting the Global Challenge through a Collaborative Business Strategy for Small and Medium-sized Enterprises*, in *2006 IEEE International Conference on Management of Innovation and Technology*, [s.l.], 2006.

[252] D. DE CREMER, D. NARAYANAN, *How AI Tools Can—and Cannot—Help Organizations Become More Ethical*, in *Frontiers*, 2020, p. 25.
[253] , *Ethical Management of Artificial Intelligence*, cit.

J.) G. (OSKAR - HALEEM (NOMAN) - ZWITTER (ANDREJ), *General-purpose AI*
regulation and the European Union AI Act, 2024consultabile su https://policyreview.info/articles/analysis/general-purpose-ai-regulation-and-ai-act.

KARATHANASIS T., Guidance on Classification and Conformity Assessments for High-Risk AI Systems under EU AI Act, [s.d.].

KUSCHE I., Possible harms of artificial intelligence and the EU AI act: fundamental rights and risk, *Journal of risk research*, 0 (00), [s.d.].

MÄNTYMÄKI M. - M. MINKKINEN - T. BIRKSTEDT - M. VILJANEN, *Putting AI Ethics into Practice: The Hourglass Model of Organizational AI Governance*, 2023.

MICKLITZ H.-W. - G. SARTOR, Compliance and enforcement in the AIA through AI, *Yearbook of european law*, 43, 2024.

NOVELLI C. - G. GOVERNATORI - A. ROTOLO, *IOS Press Ebooks - Automating Business Process Compliance for the EU AI Act*, [s.l.], [s.d.].

QUINTAIS J. P. - S. F. SCHWEMER, The Interplay between the Digital Services Act and Sector Regulation: How Special Is Copyright? | European Journal of Risk Regulation, *Cambridge core*, [s.d.].

WACHTER S., Limitations and Loopholes in the EU AI Act and AI Liability Directives: What This Means for the European Union, the United States, and Beyond, *SSRN electronic journal*, 2024.

, *A Methodological Framework for Business Decisions with Explainable AI and the Analytic Hierarchical Process*, [s.d.]consultabile su https://www.mdpi.com/2227- 9717/13/1/102.

, *A Sandbox Approach to Regulating High-Risk Artificial Intelligence Applications | European Journal of Risk Regulation | Cambridge Core*, [s.d.]consultabile su https://www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/sandbox-approach-to-regulating-highrisk-artificial-intelligence- applications/C350EADFB379465E7F4A95B973A4977D.

, *Algorithmic Transparency and Explainability for EU Consumer Protection: Unwrapping the Regulatory Premises by Mateusz Grochowski, Agnieszka Jabłonowska, Francesca Lagioia, Giovanni Sartor :: SSRN*, [s.d.]consultabile su https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3826415.

, *Article 5: Prohibited AI Practices | EU Artificial Intelligence Act*, [s.d.]consultabile su https://artificialintelligenceact.eu/article/5/.

, *Article 6: Classification Rules for High-Risk AI Systems | EU Artificial Intelligence Act*, [s.d.]consultabile su https://artificialintelligenceact.eu/article/6/.

, *Article 7: Amendments to Annex III | EU Artificial Intelligence Act*, [s.d.]consulta- bile su https://artificialintelligenceact.eu/article/7/.

, *Article 9: Risk Management System | EU Artificial Intelligence Act*, [s.d.]consulta- bile su https://artificialintelligenceact.eu/article/9/.

, *Article 10: Data and Data Governance | EU Artificial Intelligence Act*, [s.d.]consul- tabile su https://artificialintelligenceact.eu/article/10/.

, *Article 11: Technical Documentation | EU Artificial Intelligence Act*, [s.d.]consulta- bile su https://artificialintelligenceact.eu/article/11/.

, *Article 12: Record-Keeping | EU Artificial Intelligence Act*, [s.d.]consultabile su https://artificialintelligenceact.eu/article/12/.

, *Article 13: Transparency and Provision of Information to Deployers | EU Artificial Intelligence Act*, [s.d.]consultabile su https://artificialintelligenceact.eu/article/13/.

, *Article 14: Human Oversight | EU Artificial Intelligence Act*, [s.d.]consultabile su https://artificialintelligenceact.eu/article/14/.

, *Article 28: Notifying Authorities | EU Artificial Intelligence Act*, [s.d.]consultabile su https://artificialintelligenceact.eu/article/28/.

, *Article 49: Registration | EU Artificial Intelligence Act*, [s.d.]consultabile su https://artificialintelligenceact.eu/article/49/.

, *Article 61: Informed Consent to Participate in Testing in Real World Conditions Outside AI Regulatory Sandboxes | EU Artificial Intelligence Act*, [s.d.]consultabile su https://artificialintelligenceact.eu/article/61/.

, *Article 72: Post-Market Monitoring by Providers and Post-Market Monitoring Plan for High-Risk AI Systems | EU Artificial Intelligence Act*, [s.d.]consultabile su https://artificialintelligenceact.eu/article/72/.

, *Article 73: Reporting of Serious Incidents | EU Artificial Intelligence Act*, [s.d.]consultabile su https://artificialintelligenceact.eu/article/73/.

, *Article 82: Compliant AI Systems Which Present a Risk | EU Artificial Intelligence Act*, [s.d.]consultabile su https://artificialintelligenceact.eu/article/82/.

, *Article 85: Right to Lodge a Complaint with a Market Surveillance Authority | EU Artificial Intelligence Act*, [s.d.]consultabile su https://artificialintelligenceact.eu/article/85/.

, *Article 101: Fines for Providers of General-Purpose AI Models | EU Artificial Intelligence Act*, [s.d.]consultabile su https://artificialintelligenceact.eu/article/101/.

, *Artificial Intelligence in Business Law: Navigating Regulation, Ethics, and Governance - Journals - Master Educational Services, Vasant Vihar, Delhi,* [s.d.]consultabile su https://www.nationaleducationservices.org/artificial-intelligence-in-business-law-navigating-regulation-ethics-and-governance/pid-2228133310.

, *Data Subject Rights as a Tool for Platform Worker Resistance: Lessons from the Uber/Ola Judgments by Wenlong Li, Jill Toh :: SSRN*, [s.d.]consultabile su https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4306868.

, *Ethical Management of Artificial Intelligence*, [s.d.]consultabile su https://www.mdpi.com/2071-1050/13/4/1974.

, *EU AI Act: first regulation on artificial intelligence*, su *Topics | European Parlia- ment*, 2023consultabile su https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence.

, *European AI Office | Shaping Europe's digital future*, 2025consultabile su https://di- gital-strategy.ec.europa.eu/en/policies/ai-office.

, *European Commission, official website - European Commission*, 2025consultabile su https://commission.europa.eu/index_en.

, *Full article: Possible harms of artificial intelligence and the EU AI act: fundamental rights and risk*, [s.d.]consultabile su https://www.tandfonline.com/doi/full/10.1080/13669877.2024.2350720.

, GDPR And AI-Driven Business Models: Navigating Legal Risks Through A Legal Analysis Framework, [s.d.].

, *(PDF) Regulatory and Compliance Requirements for SMEs Operating AI Systems through Data Centers in the EU, with a Focus on Data Protection Challenges in Germany*, [s.d.]consultabile su https://www.researchgate.net/publication/389263846_Regulatory_and_Compliance_Requirements_for_SMEs_Operating_AI_Systems_through_Data_Centers_in_the_EU_with_a_Focus_on_Data_Protection_Challenges_in_Germany.

, *(PDF) The General Data Protection Regulation of 2016 (GDPR) Meets its Sibling the Artificial Intelligence Act of 2024: A Power Couple, or a Clash of Titans?*, su *ResearchGate*, [s.d.]consultabile su

https://www.researchgate.net/publication/384682777_The_General_Data_Protection_
Regulation_of_2016_GDPR_Meets_its_Sibling_the_Artificial_Intelligence_Act_of_ 2024_A_Power_Couple_or_a_Clash_of_Titans.

, *Proposal for a Regulation laying down harmonised rules on artificial intelligence | Shaping Europe's digital future*, [s.d.]consultabile su https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules- artificial-intelligence.

, *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS*, 2021.

, *Recital 60 | EU Artificial Intelligence Act*, [s.d.]consultabile su https://artificialintel- ligenceact.eu/recital/60/.

, *Scores as Decisions? Article 22 GDPR and the Judgment of the CJEU in SCHUFA Holding (Scoring) in the Labour Context | Industrial Law Journal | Oxford Academic*, [s.d.]consultabile su https://academic.oup.com/ilj/article/53/4/840/7745471.

, *The AI Office: What is it, and how does it work? | EU Artificial Intelligence Act*, [s.d.]consultabile su https://artificialintelligenceact.eu/the-ai-office-summary/.

, *The Ethics of AI Ethics. A Constructive Critique | Philosophy & Technology*, [s.d.]consultabile su https://link.springer.com/article/10.1007/s13347-022-00557-9.

, The Integration of Machine Learning and Explainable AI in Business Digitization: Unleashing the Power of Data – A Review - Institute of Cited Scientists, [s.d.].

BELTRÁN M., AI algorithms under scrutiny: GDPR, DSA, AI Act and CRA as pillars for algorithmic security and privacy in the European Union, *Computers & security*, 158, 2025.

BUTT J. S., Analytical Study of the World's First EU Artificial Intelligence (AI) Act, 2024, *International journal of research publication and reviews*, 5 (33), 2024.

DEY D. - D. BHAUMIK, *APPRAISE: a governance framework for innovation with AI systems*, 2023.

HAYWARD A. - A. TODD - C. REYNOLDS, *Meeting the Global Challenge through a Collaborative Business Strategy for Small and Medium-sized Enterprises*, in *2006 IEEE International Conference on Management of Innovation and Technology*, [s.l.], 2006.

J.) G. (OSKAR - HALEEM (NOMAN) - ZWITTER (ANDREJ), *General-purpose AI
regulation and the European Union AI Act*, 2024consultabile su https://policyreview.info/articles/analysis/general-purpose-ai-regulation-and-ai-act.

KARATHANASIS T., Guidance on Classification and Conformity Assessments for High-Risk AI Systems under EU AI Act, [s.d.].

KUSCHE I., Possible harms of artificial intelligence and the EU AI act: fundamental rights and risk, *Journal of risk research*, 0 (00), [s.d.].

MÄNTYMÄKI M. - M. MINKKINEN - T. BIRKSTEDT - M. VILJANEN, *Putting AI Ethics into Practice: The Hourglass Model of Organizational AI Governance*, 2023.

MICKLITZ H.-W. - G. SARTOR, Compliance and enforcement in the AIA through AI, *Yearbook of european law*, 43, 2024.

NOVELLI C. - G. GOVERNATORI - A. ROTOLO, *IOS Press Ebooks - Automating Business Process Compliance for the EU AI Act*, [s.l.], [s.d.].

QUINTAIS J. P. - S. F. SCHWEMER, The Interplay between the Digital Services Act and Sector Regulation: How Special Is Copyright? | European Journal of Risk Regulation, *Cambridge core*, [s.d.].

WACHTER S., Limitations and Loopholes in the EU AI Act and AI Liability Directives: What This Means for the European Union, the United States, and Beyond, *SSRN electronic journal*, 2024.

, *A Methodological Framework for Business Decisions with Explainable AI and the Analytic Hierarchical Process*, [s.d.]consultabile su https://www.mdpi.com/2227- 9717/13/1/102.

, *A Sandbox Approach to Regulating High-Risk Artificial Intelligence Applications | European Journal of Risk Regulation | Cambridge Core*, [s.d.]consultabile su https://www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/sandbox-approach-to-regulating-highrisk-artificial-intelligence- applications/C350EADFB379465E7F4A95B973A4977D.

, *Algorithmic Transparency and Explainability for EU Consumer Protection: Unwrapping the Regulatory Premises by Mateusz Grochowski, Agnieszka*

Jabłonowska, Francesca Lagioia, Giovanni Sartor :: SSRN, [s.d.]consultabile su https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3826415.

, *Article 5: Prohibited AI Practices | EU Artificial Intelligence Act*, [s.d.]consultabile su https://artificialintelligenceact.eu/article/5/.

, *Article 6: Classification Rules for High-Risk AI Systems | EU Artificial Intelligence Act*, [s.d.]consultabile su https://artificialintelligenceact.eu/article/6/.

, *Article 7: Amendments to Annex III | EU Artificial Intelligence Act*, [s.d.]consulta- bile su https://artificialintelligenceact.eu/article/7/.

, *Article 9: Risk Management System | EU Artificial Intelligence Act*, [s.d.]consulta- bile su https://artificialintelligenceact.eu/article/9/.

, *Article 10: Data and Data Governance | EU Artificial Intelligence Act*, [s.d.]consul- tabile su https://artificialintelligenceact.eu/article/10/.

, *Article 11: Technical Documentation | EU Artificial Intelligence Act*, [s.d.]consulta- bile su https://artificialintelligenceact.eu/article/11/.

, *Article 12: Record-Keeping | EU Artificial Intelligence Act*, [s.d.]consultabile su https://artificialintelligenceact.eu/article/12/.

, *Article 13: Transparency and Provision of Information to Deployers | EU Artificial Intelligence Act*, [s.d.]consultabile su https://artificialintelligenceact.eu/article/13/.

, *Article 14: Human Oversight | EU Artificial Intelligence Act*, [s.d.]consultabile su https://artificialintelligenceact.eu/article/14/.

, *Article 28: Notifying Authorities | EU Artificial Intelligence Act*, [s.d.]consultabile su https://artificialintelligenceact.eu/article/28/.

, *Article 49: Registration | EU Artificial Intelligence Act*, [s.d.]consultabile su https://artificialintelligenceact.eu/article/49/.

, *Article 61: Informed Consent to Participate in Testing in Real World Conditions Outside AI Regulatory Sandboxes | EU Artificial Intelligence Act*, [s.d.]consultabile su https://artificialintelligenceact.eu/article/61/.

, *Article 72: Post-Market Monitoring by Providers and Post-Market Monitoring Plan for High-Risk AI Systems | EU Artificial Intelligence Act*, [s.d.]consultabile su https://artificialintelligenceact.eu/article/72/.

, *Article 73: Reporting of Serious Incidents | EU Artificial Intelligence Act*, [s.d.]consultabile su https://artificialintelligenceact.eu/article/73/.

, *Article 82: Compliant AI Systems Which Present a Risk | EU Artificial Intelligence Act*, [s.d.]consultabile su https://artificialintelligenceact.eu/article/82/.

, *Article 85: Right to Lodge a Complaint with a Market Surveillance Authority | EU Artificial Intelligence Act*, [s.d.]consultabile su https://artificialintelligenceact.eu/article/85/.

, *Article 101: Fines for Providers of General-Purpose AI Models | EU Artificial Intelligence Act*, [s.d.]consultabile su https://artificialintelligenceact.eu/article/101/.

, *Artificial Intelligence in Business Law: Navigating Regulation, Ethics, and Governance - Journals - Master Educational Services, Vasant Vihar, Delhi,* [s.d.]consultabile su https://www.nationaleducationservices.org/artificial-intelligence-in-business-law-navigating-regulation-ethics-and-governance/pid-2228133310.

, *Data Subject Rights as a Tool for Platform Worker Resistance: Lessons from the Uber/Ola Judgments by Wenlong Li, Jill Toh :: SSRN*, [s.d.]consultabile su https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4306868.

, *Ethical Management of Artificial Intelligence*, [s.d.]consultabile su https://www.mdpi.com/2071-1050/13/4/1974.

, *EU AI Act: first regulation on artificial intelligence*, su *Topics | European Parlia- ment*, 2023consultabile su https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence.

, *European AI Office | Shaping Europe's digital future*, 2025consultabile su https://di- gital-strategy.ec.europa.eu/en/policies/ai-office.

, *European Commission, official website - European Commission*, 2025consultabile su https://commission.europa.eu/index_en.

, *Full article: Possible harms of artificial intelligence and the EU AI act: fundamental rights and risk*, [s.d.]consultabile su https://www.tandfonline.com/doi/full/10.1080/13669877.2024.2350720.

, GDPR And AI-Driven Business Models: Navigating Legal Risks Through A Legal Analysis Framework, [s.d.].

, *(PDF) Regulatory and Compliance Requirements for SMEs Operating AI Systems through Data Centers in the EU, with a Focus on Data Protection Challenges in Germany*, [s.d.]consultabile su https://www.researchgate.net/publication/389263846_Regulatory_and_Compliance_Requirements_for_SMEs_Operating_AI_Systems_through_Data_Centers_in_the_EU_with_a_Focus_on_Data_Protection_Challenges_in_Germany.

, *(PDF) The General Data Protection Regulation of 2016 (GDPR) Meets its Sibling the Artificial Intelligence Act of 2024: A Power Couple, or a Clash of Titans?*, su *ResearchGate*, [s.d.]consultabile su https://www.researchgate.net/publication/384682777_The_General_Data_Protecti on_ Regulation_of_2016_GDPR_Meets_its_Sibling_the_Artificial_Intelligence_Act_ of_ 2024_A_Power_Couple_or_a_Clash_of_Titans.

, *Proposal for a Regulation laying down harmonised rules on artificial intelligence | Shaping Europe's digital future*, [s.d.]consultabile su https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-ru les- artificial-intelligence.

, *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS*, 2021.

, *Recital 60 | EU Artificial Intelligence Act*, [s.d.]consultabile su https://artificialintel- ligenceact.eu/recital/60/.

, *Scores as Decisions? Article 22 GDPR and the Judgment of the CJEU in SCHUFA Holding (Scoring) in the Labour Context | Industrial Law Journal | Oxford Academic*, [s.d.]consultabile su https://academic.oup.com/ilj/article/53/4/840/7745471.

, *The AI Office: What is it, and how does it work? | EU Artificial Intelligence Act*, [s.d.]consultabile su https://artificialintelligenceact.eu/the-ai-office-summary/.

, *The Ethics of AI Ethics. A Constructive Critique | Philosophy & Technology*, [s.d.]consultabile su https://link.springer.com/article/10.1007/s13347-022-00557-9.

, The Integration of Machine Learning and Explainable AI in Business Digitization: Unleashing the Power of Data – A Review - Institute of Cited Scientists, [s.d.].