International Journal of Social Science Research and Review

http://ijssrr.com
editor@ijssrr.com
Volume 9, Issue 3
March, 2026
Pages: 209-226

Navigating the Intersectionality of Artificial Intelligence, Data Privacy, and Strategic Consulting: A Case Study on the EU's Regulatory Framework

Harshita

Independent Researcher

Gargi College, Delhi University, India

http://dx.doi.org/10.47814/ijssrr.v9i3.3285

ABSTRACT

The integration of Artificial Intelligence (AI) has sparked a significant strategic shift within the management consulting sector creating a divide in trust. AI surely does enhance the efficiency by automating the processes such as data analysis but the lack of transparency creates a rift making the erosion of data privacy as the most important concern. Data is surely the most important asset of any business consulting firm. This risk jeopardises the client confidentiality which is the cornerstone of the consulting relationships. This makes it mandatory for the consulting firms to incorporate the specialized AI governance into their administrative operations. This study explores the intersectionality between AI, Data Privacy and Strategic Consulting with a special focus on how the European Union's regulatory framework is pushing the global firms to adapt their business models in order to attract the talent that combines AI expertise with crucial interpersonal skills thereby enhancing the role of the Hybrid Consultant. The results of the study indicate that the EU's risk based extraterritorial regulations serve as regulatory mandate. The analysis reveals that AI is not a threat of job displacement but a catalyst for role transformation, automating repetitive tasks and challenging the traditional consulting pyramid model. The firms are compelled to shift their service offering towards responsible AI advisory and governance, placing ethical compliance as the core strategic differentiator for sustaining long term market relevance and client confidence.

Keywords: *Artificial Intelligence, Data Privacy, Strategic Consulting, EU AI Act, Qualitative Analysis*

1. INTRODUCTION

In the dynamic landscape of Artificial Intelligence, Data Privacy and Strategic Consulting, the question is no longer whether AI will redefine the industry, but how firms will balance the unparalleled efficiency with its inherent ethical liabilities of artificial intelligence. The real threat is not job loss, but compromised client trust. The immediate and most critical challenge posed by the integration of AI into strategic consulting is the conflict that it creates with data privacy an d accountability. Specifically, the adoption of sophisticated Generative AI (GAI) models poses a direct and immediate challenge to legal and ethical standards because these systems possess an inherent data intensive nature that must be trained on massive and continuous streams of data, often sensitive.

Despite these liabilities, AI's role has become that of a transformative tool. The issue has never been with AI itself, but rather with its improper application. AI was designed to assist humans in enhancing their productivity, not to supplant them. We can view it similarly to how we regard computers; they were not created to take over human roles but to improve human capabilities. Ultimately, operating a computer or utilizing Excel still requires human intervention. The only shift that has occurred is that individuals must learn to leverage this technology effectively and optimally. The popular fear that AI would replace human consultants is a myth instead AI fundamentally transforms roles. Its primary function is to automate the repetitive, data-intensive tasks such as research, data analysis, and standardized framework

generation that previously consumed significant human time. This automation elevates the human role, creating the Hybrid Consultant, whose value centers on competencies AI cannot replicate.

This fundamental shift is forcing firms to modify their traditional business models, compelling them to compete for talent that possesses the crucial blend of technical AI proficiency and essential soft skills. AI is thus making the consultant's role more strategic and less administrative. This complex environment where innovation, ethics and business strategies collide, has underscored the necessity of navigating the Intersectionality of Artificial Intelligence, Data Privacy, and Strategic Consulting. To examine how legal governance is attempting to resolve this tension and redefine the future of professional services, this research analyses the EU's Regulatory Framework as a primary case study.

1.1 Conceptual Framing: Intersectionality in Sociotechnical Systems

While "intersectionality" originated in critical race theory to describe overlapping systems of discrimination (Crenshaw, 1989), this paper adapts the concept to analyse overlapping sociotechnical systems. We define intersectionality here as the examination of how multiple domains—artificial intelligence technology, data privacy regulation, and professional consulting services—interact to create emergent challenges and opportunities that cannot be understood by examining each domain in isolation.

This framing is justified because:

1. Mutual Constitution: AI capabilities shape privacy risks, privacy regulations constrain AI deployment, and consulting services mediate both—each domain constitutes the others
2. Non-Additive Effects: The challenges facing AI-enabled consulting are not simply "AI challenges" + "privacy challenges" + "consulting challenges," but rather emergent problems at their intersection.
3. Power and Governance: Like traditional intersectionality, this framework examines how regulatory power (EU AI Act), technological power (AI systems), and professional power (consulting expertise) interact

Following Leonelli (2016) and Dourish (2016), we treat these three domains as co-constitutive elements of a sociotechnical system.

Drawing from the research gaps identified above, this study addresses the following:

Research Question 1. How does the adoption of AI technologies in management consulting create specific data privacy and trust challenges that differ from other sectors?

Research Question 2. In what ways does the EU AI Act's risk-based regulatory framework reshape business models and services offerings in management consulting industry?

Research Question 3. What competencies and organisational capabilities must consult firms develop to navigate the intersection of AI deployment, data privacy compliance, and client advisory services?

By examining these questions through the lens of the EU AI Act as a critical case study, this paper contributes to understanding how regulatory framework simultaneously create compliance burdens and strategic opportunities for knowledge-intensive professional services.

2. REVIEW OF LITERATURE

Recent literature points out a gap between the rapid pace of artificial intelligence (AI) innovation and the need for strong ethical and legal frameworks. Musch et al. (2023) identify EU AI Act as the foundation to balance technological advancement and individual privacy rights. Potturi (2025) recognises specific ethical dilemmas that serve as the backdrop for this regulatory approach. Potturi argues for "responsible data use" alongside AI innovation. He addresses four systemic risks including algorithmic bias, the lack of transparency in "black box" systems, privacy concerns related to data access, and accountability questions for automated decisions. Similarly, the ICMCI Report offers a practical approach to how these ethical and regulatory frameworks manifest in professional services (International Council of

Management Consulting Institutes, 2024). This report shifts the focus towards strategic augmentation while also echoing the need for ethical safeguards specifically regarding content ownership and algorithmic fairness. The report argues that AI cannot replace human intellect. It further adds that its value lies in enhancing efficiency through automated data analysis. This allows human consultants to focus on high-level strategy and relationship management.

There arises an ethical friction while integrating Generative AI (GAI) in the business consulting industry. This has been recognised as a primary concern in the recent literature. Pattanayak (2021) identify risks regarding data privacy, algorithmic bias, and intellectual property as inherent to GAI. They argue that GAI allows improved decision-making and Natural Language Processing (NLP), it also introduces complex questions regarding neutrality, transparency, privacy, and liability. Both authors emphasize that technical implementation by firms is not enough. They must move towards "transparent and responsible practices" that simultaneously protects stakeholder equity. Similarly, Li (2024) studies AI in operations management specifically looking at the ethical challenges. He highlights the need to balance efficiency with responsibility. He refers to frameworks such as the OECD AI Principles and the EU Ethics Guidelines for a trustworthy use of AI. He also proposes a hybrid governance model that is tailored to operational contexts. A case study in the financial sector illustrates the effective use of privacy-preserving techniques such as differential privacy and federated learning to safeguard sensitive customer data. These methods demonstrably reduce unauthorized data access events by up to 30%. They also boost customer satisfaction by more than 20% and offers practical guidance for organizations to implement AI operations responsibly and in accordance with regulations.

AI integration into management consulting is driving a fundamental shift from operational support to high-value strategic and regulatory guidance. Samokhvalov (2024) traces the AI evolution since 1956 and contextualizes this transformation. He notes that AI-native firms challenge industry incumbents. He adds that human-led strategic decision-making stays highly relevant in the face of automation of routine tasks. An increasingly complex global regulatory landscape frames this transition. Samakhvalov (2024) contrasts the stringent EU AI Act with the more flexible models of the UK, the self-regulated approach of the US, and the targeted regulations of China. He forecasts a "war for talent" as firms seek professionals capable of bridging the gap between data science and business logic. In addition, the EU AI Act has been identified as a significant market catalyst that simultaneously redefines the consultant's value proposition (EY Global, 2024). Businesses face sharp penalties for non-compliance thereby creating the demand for "AI readiness". This has led firms to act as "responsible AI advisors." Consulting firms are moving beyond their traditional role as technology facilitators. They are now assembling interdisciplinary teams of legal, ethical, and technical experts and becoming essential architects of responsible AI deployment. This is helping clients to navigate an intricate ethical landscape where strategic insight remains paramount.

AI and data-driven technologies are transforming global business and management practices. They not only offer improved efficiency, innovation, and economic growth, but also raise complex ethical and governance challenges. Forradellas and Gallastegui (2021) and Edwards (2022) note that adoption of AI promises significant benefits but it is constrained by skill shortages, leadership gaps, and the need for ethical oversight. In this context, the EU AI Act emerges as a key regulatory framework. It positions consulting firms as strategic partners in AI governance. This supports compliance, risk management, ethical framework development, and workforce training. Complementing this, Nwaimo et al. (2023) demonstrate that widespread use of data analytics across sectors such as healthcare, finance, and public administration enhance decision-making and stakeholder engagement. However, this also amplifies concerns regarding privacy, bias, transparency, accountability, and consent. Their analysis underscores the importance of governance frameworks and regulations, including the General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA). These frameworks mitigate risks, safeguard individual rights, and promote responsible and ethical data innovation. These studies suggest that AI-driven digital transformation is inevitable and highly beneficial. Its long-term success, however, depends on strong governance, ethical implementation, and specialized support systems.

AI has become deeply embedded in global technological and economic systems. Its ethical use and regulatory compliance have become a critical global priority. Whittlestone et al. (2021) argues that AI offers significant societal benefits, but its development brings with it critical ethical challenges. They note growing international consensus around core ethical principles. They also highlight persistent gaps in how these principles are defined, applied in practice, balanced against competing values, and supported by empirical evidence. Mbah (2024) has explored how the intersection of AI and data privacy poses a significant challenge for international companies navigating intricate regulatory frameworks. As AI technologies increasingly rely on extensive datasets to provide insights and foster innovation, worries regarding data protection, algorithmic clarity, and adherence to privacy regulations have grown more pronounced. He underscores the complexity of navigating diverse legal frameworks such as General Data Protection Regulation (GDPR), California's Consumer Privacy Act (CCPA), and China's Personal Information Protection Law (PIPL). He further stresses the need

for clearer standards, privacy-by-design approaches, advanced data protection techniques, and cross-border collaboration. Together, these works argue that ensuring AI's societal benefit requires ethical principles, robust governance mechanisms, harmonized regulations, and proactive industry practices that safeguard privacy, reduce bias, and build public trust.

Emerging research suggests that the growing influence of AI is transforming how businesses operate and also reshaping the expectations placed on management consultants. Gupta et al. (2025) emphasize that the adoption of AI drives efficiency. It also heightens the need for robust data privacy, ethical governance, transparency and global regulatory compliance to build trust and ensure responsible use. Complementing this, Sayyadi et al. (2023) argue that the consulting business model must evolve beyond advisory roles. They add that these models must actively implement solutions, manage operational risks, and address AI-driven challenges that reflect a fundamental shift in consultants' responsibilities. Mohan (2024) further reinforces this transformation. He illustrates how AI and machine learning redefine consulting expertise, decision-making processes, and organizational structures. This creates new opportunities and demands for specialized capabilities. Together, these studies emphasize the importance of integrating technological, ethical, and strategic dimensions of AI adoption.

The management consulting sector is undergoing rapid transformation driven by digitalization and AI adoption. Mamedova et al. (2022) note that the COVID-19 pandemic exposed the vulnerabilities of a traditionally face-to-face, relationship-based industry. This accelerates the shift towards remote delivery, digital tools, and enhanced client access to analytics. Building on this, Tiwari (2025) highlights AI's potential to improve efficiency, decision-making, and value creation. He adds that this is achievable through advanced data analysis, automation, and strategic support. However, both studies emphasize that these advancements introduce regulatory, ethical, and security challenges. This necessitates robust governance, standardization, and responsible implementation of AI adoption. Similarly, Kamaruddin (2023) examines the impact of ChatGPT on consulting. He shows that using ChatGPT streamlines data analysis, enhances, client communication, and frees consultants for higher-value strategic work. This, however, also raises concerns about privacy, ethics, and workforce implications. Together, these studies indicate that digital transformation and AI can significantly strengthen consulting services. Their benefits will depend on thoughtful adaptation, strong oversight, and careful risk management.

Artificial intelligence continues to evolve. In the process, it is reshaping the structure, capabilities, and strategic direction of the management consulting industry. Across the literature, scholars highlight that AI is not replacing consultants but redefining their roles. AI is enhancing efficiency, supporting deeper analytical insights, and enabling greater value creation for clients. Axelsson and Leufvén (2025) emphasize that AI frees consultants from routine tasks, allowing them to focus on higher-value strategic work. This reinforces the importance of human skills such as trust-building, communication, and contextual judgment. Similarly, Oarue-Itseuwa (2024) suggests that AI will fundamentally transform consulting dynamics. This will intensify competition and create niche AI-focused firms. This also encourages the use of hybrid models where AI-generated insights are complemented by human creativity and empathy. Adding another dimension, Basavarju (2024) shows that AI also supports sustainability goals by improving decision-making, operational efficiency, and resource management. However, ethical, capability, and adoption challenges remain. Together, these studies suggest that the future of consulting lies in hybrid, human-AI collaboration. In such a scenario, competitive advantage and sustainable value is driven by technological capabilities, ethical responsibility, domain expertise, and emotional intelligence.

AI has a transformative influence on the management consulting sector. The EU AI Act shapes how firms must operate in this evolving environment. Wilson Sonsini (2024) explains that the Act introduces a tiered, risk-based regulatory framework. Within this framework, obligations increase with the level of AI risk. The most stringent requirements are applied to high-risk systems. The act also establishes particular regulations for GPAI models that present systemic risks. Implementation of the AI Act will occur in stages. It will begin with bans on specific harmful AI practices, followed by staged enforcement for GPAI and high-risk systems, supported by grace periods for existing technologies. The Act's broad scope extends to both EU and non-EU organizations that place AI systems on the EU market. This requires detailed risk documentation, governance structures, and alignment with existing privacy and compliance frameworks such as GDPR. The European AI Office will coordinate the oversight along with national regulators that have the power to restrict non-compliant systems. Overall, this regulation necessitates consulting firms and organizations to integrate robust AI governance, compliance readiness, and continuous monitoring into their strategic and operational approaches.

Artificial intelligence is quietly reshaping business environments. In the process, it is making ethical responsibility central to its effective adoption. Olatoye et al. (2024) assert that businesses must prioritize transparency in AI decision-making,

fairness in algorithms, and strong data privacy protections. This builds stakeholder trust and ensures alignment with societal values. At the same time, they emphasize that AI integration cannot be viewed purely as a technological advancement. It also carries broader economic and social implications, influencing employment patterns, productivity, and organizational accountability. Growing scholarly interest in AI ethics further underscores its strategic relevance for business leaders, policymakers, and researchers as they navigate digital transformation in responsible and sustainable ways (Ciobanu & Meșniță, 2021).

Overall, the literature converges on the view that AI represents an unavoidable strategic necessity. It also brings a profound governance challenge for the consulting sector. While Generative AI promises to elevate consulting practice by enhancing efficiency, strategic capability, and competitive positioning, its benefits are inseparable from the ethical, legal, and societal responsibilities that accompany data-intensive technologies (Potturi, 2025; Olatoye et al., 2024). Scholars consistently emphasize that sustainable AI adoption requires transparent systems, strong accountability frameworks, and robust privacy safeguards to balance innovation with public trust and regulatory expectations (Mbah, 2024; Nwaimo et al., 2023; Whittlestone et al., 2021). Within this context, the EU's GDPR and AI Act emerge not merely as compliance obligations but as strategic enablers that structure responsible AI integration and create new advisory opportunities for consultants (Musch et al., 2023; Wilson Sonsini, 2024; Edwards, 2022; EY Global, 2024). Thus, the future of consulting lies in the evolution of firms into ethical AI stewards. This is possible by leveraging technological advancement while embedding governance, transparency, and human- centered responsibility at the core of their strategic value proposition.

While the existing literature establishes that AI creates ethical challenges (Potturi, 2025; Pattanayak, 2021) and transforms consulting roles (Samokhvalov, 2024), a gap remains in understanding how privacy regulations specifically reshape consulting business models and skill requirements. This paper addresses this gap through detailed analysis of the EU AI Act's implications for the consulting sector.

3. RESEARCH METHODS

The goal of this research is to navigate the intersectionality between Artificial Intelligence, Data Privacy, and Strategic Consulting with a special focus on the European Union's regulatory framework. Since the study looks at the current and complex regulatory environment and its effect on business strategy, a Qualitative Research Design, specifically a Conceptual Case Study, is the best methodological approach. This method enables a detailed and complete examination of the issue by combining and reviewing a wide range of secondary sources, including academic literature, industry reports, and primary legal texts. The study will focus on a detailed case analysis of the EU AI Act and the subsequent strategic, ethical, and market responses in the strategic consulting industry. This approach offers the rich, non-numerical data needed for a deep and nuanced analysis of this emerging intersection.

3.1 RESEARCH APPROACH

This study employs a qualitative conceptual case study design using the EU AI Act as the central case. We define "conceptual case study" as an in-depth analysis of a specific phenomenon (regulatory framework) to build and refine theoretical propositions about broader patterns (AI-privacy-consulting intersections).

While the study is conceptual in nature—focusing on legal and policy analysis rather than empirical data collection—it goes beyond purely descriptive research by:

1. Analyzing the causal mechanisms through which regulation reshapes business models
2. Developing theoretical propositions about professional skill evolution (RQ3)
3. Connecting specific regulatory provisions to general principles of responsible AI governance

The EU AI Act was selected as the case because it:
(a) is the world's first comprehensive AI regulation with extraterritorial reach,
(b) explicitly addresses high-risk AI systems across sectors, and
(c) creates legally binding obligations that force organizational adaptation.

3.2. DESCRIPTIVE RESEARCH

Descriptive research aims to systematically describe a population, situation, or phenomenon. It can answer questions about what, where, when, and how, but not why. A descriptive research design can use various research methods to examine one or more variables. Unlike experimental research, the researcher does not control or manipulate the variables;

they only observe and measure them. This research paper is purely descriptive research and is based on the secondary sources like the academic research papers and the primary policy documents.

NOTE ON TERMINOLOGY: Prior descriptions of this study as "purely descriptive research" were imprecise. While we do not collect primary empirical data, our approach is analytical rather than merely descriptive. We:

1. Interpret regulatory text to identify causal mechanisms
2. Deduce implications for organizational behavior
3. Synthesize across multiple domains to generate novel propositions

This positions our work as conceptual analysis grounded in a specific case (the EU AI Act), distinct from both empirical case studies (which collect primary data) and purely theoretical papers (which may not anchor to specific cases).
This research is describing the intersectionality between artificial intelligence, data privacy and strategic consulting particularly focusing on the EU regulatory framework on AI.

The analysis will map the specific requirements of the EU AI Act to the consulting industry's operational landscape. It will also create a model showing how the risk-tiered approach, such as high-risk AI systems, requires significant changes in service offerings, internal governance, and ethical due diligence. This study will focus on the relationship between required AI system transparency, strict data privacy compliance, and the necessary strategic shift. The goal is to develop a solid and practical framework for firms dealing with this complex regulatory environment. This framework will clarify the competitive effects of compliance.

3.3. DATA COLLECTION

Secondary Data Sources

Secondary data refers to information that has already been gathered through primary sources and is made accessible for researchers to utilize in their own studies. This type of data has been collected in the past. The data that is considered secondary in one study may be viewed as primary in another. This occurs when data is reused, making it primary data for the first study and secondary data for the subsequent research in which it is utilized.

1. **Academic Research Papers -** This systematic literature review started with a thorough search across several academic databases, resulting in a collection of 50 relevant research papers. After careful screening based on clear criteria for topic relevance, research quality, and specific focus on the EU AI Act, data privacy, and strategic consulting, the selection was reduced to 35 finalized research papers, reports and online articles. This careful process ensured that the final bibliography includes the most relevant and trusted scholarly sources. These 30 papers provide the main academic basis for the conceptual case study. They offer the necessary theoretical frameworks, background information, and critical analyses needed to define the complex relationships involved in strategic adaptation after the EU AI Act. This focused set of sources is essential for maintaining the clarity and reliability of the arguments presented.

2. **Primary Policy Documents**- The study of Primary Policy Documents is crucial for the validity of this conceptual case study. This section focuses on closely examining the foundational legal text of the EU AI Act, including its official recitals, annexes, and relevant amendments. This detailed review is important because the Act itself is the main independent variable driving the need for change in the consulting industry. The analysis goes beyond the main articles to include official impact assessments and preparatory documents released by the European Commission (European Commission 2021; European Commission, 2024). These documents clarify the regulatory intent, scope, and expected effects of the legislation. This provides a solid foundation for defining the necessary relationships between AI governance, data privacy standards, and subsequent strategic changes.

3.3.1 INFORMATION SOURCES

We conducted a systematic search of the following sources:

PRIMARY SOURCES:
-EU AI Act official text (Regulation (EU) 2024/1689)
-GDPR (Regulation (EU) 2016/679)

-European Commission explanatory documents and impact assessments

SECONDARY SOURCES:
-Academic databases: Web of Science, Scopus, Google Scholar
-Professional publications: Harvard Business Review, McKinsey Insights, BCG publications -Legal databases: EUR-Lex, SSRN, Legal information resources

3.3.2 SEARCH STRATEGY
For academic and professional sources, we used the following search strings:
- AI Act, Artificial Intelligence Act, EU AI Regulation
- Consulting, Professional services, Advisory Services
- Data Privacy, GDPR, Data Protection

Additional targeted searches:
- AI in management consulting, Privacy risks
- Consulting Business model, AI Regulation
- Algorithmic Accountability

3.3.3 INCLUSION/EXCLUSION CRITERIA
INCLUDED:
-Sources published 2018-2024 (GDPR implementation to AI Act adoption)
-Focus on AI deployment in knowledge-intensive professional services
-Discussion of privacy/regulatory implications
-Peer-reviewed articles, official policy documents, major consultancy white papers

EXCLUDED:
-Sources focused solely on technical AI development without regulatory/business context
-Non-English sources (with exception of official EU documents with English translations)
-Opinion pieces without substantive analysis
-Sources addressing only consumer-facing AI (e-commerce, social media) without professional services relevance

4. RESULTS AND DISCUSSIONS

4.1 AI'S IMPACT ON DATA PRIVACY

The introduction of Artificial Intelligence has ushered in a 'cognitive industrial revolution' where now our mental processes are automated and the workplace has evolved consequently. Nevertheless, this evolution is completely dependent on the utilization of data which in today's world is as highly valued as oil. Now this automation is posing a critical dilemma regarding human data privacy and individual freedom. The primary issue is regarding the extraordinary power of AI for prediction and creation which is directly linked to its insatiable data hunger and inherent opacity. The confluence of AI and the rapidly evolving digital ecosystem has cast AI as a 'cognitive catalyst'.

AI has introduced privacy risks at a scale that the traditional security frameworks cannot address primarily through unauthorized data repurposing, targeted misuse and algorithmic bias. There is a pervasive misuse and repurposing of personal information where the malicious activities bypass the traditional security measures. The Generative AI tools are trained on our data and are used for antisocial purposes including spear phishing and AI voice cloning that later leads to impersonation and extortion. Our data such as photographs being shared under the influence of any viral trend on Instagram is being repurposed for AI training without our explicit consent and we are not even aware of it leading to civil rights implications.

The AI systems and apps often lack a clear option for deleting information that users provide. There is no information of exactly where our personal information is travelling within the AI ecosystem. This reality violated the ability of citizens to exercise their "right to erasure/ right to be forgotten." This problem is further exacerbated by the tendency of AI's "hallucinations" and inaccuracy to generate incorrect and non-factual information with full confidence becoming the basis for high stake decisions. This further erodes trust and introduces potential legal harms to individuals.

The Indian current legal structure which includes the IT Rules of 2021 faces criticism for its absence of specific and enforceable mandates. Although the rules mandate the content removal, they lack transparency regarding the timeframe

of the takedown of the non-consensual material and do not impose the same level of liability on the platforms for inaction. This places the burden of data privacy back on the victim. This highlights a significant flaw in safeguarding individual autonomy and data rights in today's digital landscape.

4.2 AI'S IMPACT ON STRATEGIC CONSULTING

The strategic consulting industry is undergoing a profound and disruptive transformation moving from a rigid and labour-intensive model to an AI augmented and expert driven system. The AI acts as a cognitive catalyst that is now restructuring the economic hierarchy of the consulting firms. The decade old structure of major consulting firms known as pyramid model is now being fundamentally challenged because now whatever tasks the junior analysts used to perform are now automated. The ability of Generative AI to instantly summarize data and create slides and do a ton of things that were earlier performed by the junior analysts. The time that was earlier required to do tasks in strategic consulting has shrunk dramatically.

According to a large-scale experiment conducted by the Harvard Business School and BCG, a strong proof of this AI augmentation amongst the highly skilled knowledge workers too is provided (Dell'Acqua et al., 2023). According to the experiment, consultants using GPT-4 were 25.1% faster in completing tasks, they completed 12.2% more tasks, they achieved over 40% higher quality in their outputs compared to the control group. Though this augmentation is not uniform, this may cause performance to drop if the consultants relied too heavily on the AI's opaque output. Successful users adopt the "Centaur" (strategic delegation) or "Cyborg" (seamless integration) practices to navigate this frontier.

As the cost of basic analytical labor approaches zero, because the rise of AI has destroyed the old business model where junior staff did tedious research forcing the industry to focus on three things that AI alone cannot provide: speed, unique information and trustworthy governance. Because the external is easily accessible to everyone, if the companies will rely on generic inputs will inevitably produce generic strategies. Here the critical differentiator is proprietary data, to generate unique insights and secure a competitive advantage for clients. AI can only support the strategic roles by acting as an interpreter, simulator or a thought partner.

A McKinsey survey (Luget et al., 2025) found that 71% of European Organizations consider their AI risk governance less than mature which signals towards the dire need of external strategic help to address this risk.

4.2.1 CONSULTING FIRMS' ROLES UNDER THE EU AI ACT

The AI Act defines several actor categories, each with distinct obligations. Consulting firms may occupy multiple roles simultaneously:

- PROVIDER (Article 3(3))
- Definition: Entity that develops an AI system or has it developed, and places it on the market or puts it into service under its own name or trademark
- Consulting Example: A firm that develops a proprietary AI-powered strategy recommendation tool and licenses it to clients
- Key Obligations: Conformity assessment, technical documentation, risk management system, post-market monitoring
- DEPLOYER (Article 3(4))
- Definition: Entity that uses an AI system under its authority, except for personal non-professional activity
- Consulting Example: A firm that uses an AI system internally for HR screening of job candidates, or for analyzing client data
- Key Obligations: Use systems according to instructions, monitor operation, report serious incidents, conduct fundamental rights impact assessments for high-risk systems
- IMPORTER (Article 3(7))
- Definition: Entity established in the EU that places on the market an AI system bearing the name/trademark of a non-EU entity
- Consulting Example: The EU subsidiary of a global consultancy that brings a US-developed AI tool to European markets
- Key Obligations: Verify provider compliance, ensure instructions/documentation are in EU languages, register in EU database
- DISTRIBUTOR (Article 3(8))
- Definition: Entity in the supply chain that makes an AI system available on the market without altering its properties

- Consulting Example: A firm that resells or recommends third-party AI tools to clients without modification
- Key Obligations: Verify CE marking, ensure provider/importer compliance, cooperate with authorities

CRITICAL INSIGHT FOR CONSULTING: Most consulting firms will be DEPLOYERS when using AI internally or in client engagements. However, firms developing proprietary AI products become PROVIDERS with significantly heavier compliance burdens.

4.2.2 RISK CLASSIFICATION OF COMMON CONSULTING AI USE CASES

The AI Act classifies AI systems into risk tiers: prohibited, high-risk, limited risk, and minimal risk. We analyze three representative consulting applications:

USE CASE 1: AI-POWERED RESUME SCREENING TOOL

Description: A consulting firm deploys an artificial intelligence (AI) system to screen job applicants' CVs, rank candidates, and generate interview shortlists for consulting roles. The system analyzes applicant data and produces recommendations to assist the HR team in decision-making.

Risk Classification: High-Risk AI System

Legal Basis: Annex III, Point 4(a) of the EU AI Act – AI systems intended to be used for recruitment or selection of natural persons are classified as high-risk.

Firm's Role: Deployer of a high-risk AI system.

Triggered Compliance Obligations:

1. Fundamental Rights Impact Assessment (Article 27)

- The firm must conduct an assessment evaluating potential impacts on privacy, non-discrimination, equality, and fairness before deploying the system.
- Identified risks must be documented along with mitigation measures.

2. Human Oversight (Article 14)

- Human HR professionals must actively review AI-generated recommendations.
- Hiring decisions cannot be fully automated without meaningful human involvement.

3. Transparency (Article 13)

- Candidates must be informed that AI is being used in the screening process.
- The firm must provide clear information regarding the logic, significance, and expected consequences of the AI processing.

4. Logging and Record-Keeping (Article 12)

- The AI system must automatically generate logs of decisions and processing activities.
- Records must be retained for an appropriate period (minimum six months or as required by regulatory standards).

5. Registration (Article 49)

- The use of the high-risk AI system must be registered in the EU database for high-risk AI systems.

Privacy Intersection (GDPR Considerations)

- **Lawful Basis:** Legitimate interest (Article 6(1)(f) GDPR), subject to balancing test.
- **Data Protection Impact Assessment (Article 35 GDPR):** Required due to systematic and automated evaluation of individuals.
- **Data Subject Rights:** Candidates have the right to request meaningful information about the logic involved, challenge decisions, and seek human review.

Business Impact

- **Upfront Costs:** Conducting impact assessments, implementing compliance frameworks, and technical integration.
- **Ongoing Costs:** Maintaining human oversight layers, logging systems, and documentation.
- **Reputational Risk:** Potential discrimination or bias could lead to legal exposure and reputational harm.

USE CASE 2: GENERATIVE AI FOR CLIENT DELIVERABLE CREATION

Description: Consultants use generative AI tools (such as ChatGPT, Claude, or proprietary large language models) to draft report sections, create presentation slides, and generate preliminary strategic insights for clients. The AI assists in content generation but does not replace professional judgment.

Risk Classification: Limited Risk or Minimal Risk AI System

Legal Basis:: If using a general-purpose AI model, obligations arise under Chapter V of the EU AI Act. The system is not inherently high-risk unless deployed for high-risk purposes (e.g., generating legally binding advice or performing regulated decision-making functions).

Firm's Role

- **Deployer** (when using third-party models such as GPT-4), or
- **Provider** (if the firm fine-tunes or significantly modifies the model to create a new AI system).

Triggered Compliance Obligations

1. Transparency (Article 50)

- AI-generated content must be clearly labeled where appropriate.
- Clients should be informed that content is AI-assisted.

2. Quality Assurance

- Human consultants must review, verify, and edit AI outputs.
- AI-generated content cannot be presented as independent expert judgment without validation.

3. Intellectual Property Compliance

- Transparency obligations may apply regarding training data (Article 53).
- There is a risk of reproducing copyrighted material verbatim, requiring careful review and safeguards.

Privacy Intersection (GDPR Considerations)

- **Processor Agreements (Article 28 GDPR):** Required if client data is input into third-party AI systems.
- **Confidentiality Safeguards:** Contracts must ensure that AI providers do not use client data for further model training.
- **Cross-Border Data Transfers:** If the AI provider is outside the EU, appropriate safeguards (e.g., adequacy decision or Standard Contractual Clauses) must be implemented.

Business Impact

- **Efficiency Gains:** Faster drafting and productivity improvements.
- **Quality Risks:** Potential AI hallucinations, factual inaccuracies, or misinterpretations.
- **Client Trust Considerations:** Transparency regarding AI use affects credibility and brand reputation.
- **Competitive Pressure:** Market expectations increasingly favor AI-augmented efficiency and cost-effectiveness.

4.2.3 CROSS-CUTTING IMPLICATIONS FOR CONSULTING BUSINESS MODELS

Comparing these use cases reveals several patterns:

1. ROLE COMPLEXITY: Consulting firms increasingly occupy multiple AI Act roles simultaneously (deployer for internal tools, provider for proprietary products, distributor for third-party solutions). This creates compliance fragmentation and requires sophisticated legal/technical capabilities.

2. HIGH-RISK CONCENTRATION: Common consulting activities (HR, client advisory affecting individuals) frequently trigger high-risk classification, subjecting firms to the Act's most stringent requirements.

3. COST-BENEFIT CALCULUS: The compliance burden for proprietary AI development may exceed ROI for all but the largest firms, accelerating market consolidation.

4. GDPR COMPOUNDING: AI Act obligations layer atop existing GDPR duties, creating compound compliance complexity. For example, Use Case 1 triggers both an AI Act fundamental rights impact assessment AND a GDPR DPIA—with overlapping but not identical requirements.

5. TRANSPARENCY AS DOUBLE-EDGED SWORD: Obligations to disclose AI use (Articles 13, 50) can strengthen client trust if framed positively, but also expose competitive intelligence about methodologies.

These patterns directly inform Research Question 2: The AI Act reshapes consulting business models by making compliance a core competency, not an ancillary function.

4.3. CASE STUDY AND ANALYSIS

This Conceptual Case Study looks at how the management consulting industry is responding to the European Union's regulations, particularly the AI Act. It does this by assessing current literature and comparing it with key policy requirements. The results show that the EU AI Act is not just a compliance burden; it is a key force driving the change in consulting services toward a new area: Responsible AI Advisory.

4.3.1 THE EU AI ACT FRAMEWORK

The EU AI Act takes a risk-based approach. It sets clear, multi-layered compliance requirements. This leads to a need for specialized consulting services. These requirements drive the industry's shift, both economically and legally.

THE EU AI ACT

The European union's AI Act is strategically designed as the definitive global legal standard for AI governance. The core aim of this act is to protect the fundamental rights while providing a legal security for the businesses across the 27 member states. The main factor contributing to its success is its ability to extend its influence beyond borders, utilizing the economic strength of the European internal market to encourage worldwide adherence to its standards – this occurrence is referred to as the "Brussels Effect." The EU AI Act takes a risk-based approach. It sets clear, multi-layered compliance requirements. This leads to a need for specialized consulting services. These requirements drive the industry's shift, both economically and legally.

This case study analyses the EU AI Act as the foundational architecture and the strategic implications of the AI Act and demonstrating how the framework positions it as the essential blueprint for the nations worldwide.

• **Worldwide Framework:** According to McKinsey, the AI Act is the first comprehensive regulation for artificial intelligence globally and will function as a "test bed" and "model" for other regions (Soller et al., 2024).

• **Coordinated Oversight:** The Act works within an integrated structure alongside the General Data Protection Regulation (GDPR) and the Digital Services Act (DSA), ensuring a unified regulatory strategy for the entire digital landscape.

• **Strategic Necessity:** International organizations are viewing compliance not merely as a checklist but as a strategic advantage to foster trust and market resilience, underscoring the significance of the Act in commercial terms.

4.3.2 FOUNDATIONAL ARCHITECTURE: THE RISK-BASED GLOBAL STANDARD

The AI Act is based on the principle of proportionality, where the level of regulation corresponds to the potential risk an AI system presents to human health, safety, and fundamental rights. This risk-based approach is the central aspect being examined and replicated by other regions worldwide.

4.3.2.1 The scope

The AI Act takes a comprehensive approach by categorizing AI systems according to the potential risks they present, instead of regulating particular technologies or industries. A major element reinforcing the Act's worldwide influence is its extraterritorial clause. Both McKinsey and KPMG explain that the scope encompasses AI tools developed in other markets if their use or outcomes are experienced within the European Union (Soller et al., 2024; KPMG International, 2024). This strategic claim of jurisdiction compels international standardization.

4.3.2.2 The four-tiered classification system

The Act categorizes AI applications into four distinct groups, each with its own set of obligations that were implemented. The prohibitions began on 2 February 2025, while governance regulations for General-Purpose AI (GPAI) took effect on 2 August 2025.

1. Unacceptable Risk (Prohibited): Systems that pose a clear threat to the fundamental rights are banned. These systems include social scoring which means evaluating individuals based on behaviour or status and untargeted scraping of facial images for biometric databases.

2. High Risk: These systems, which can negatively impact safety or fundamental rights, are subjected to the most rigorous obligations. The requirements apply to the critical areas, such as:
o Employment and Worker Management: Systems are used for targeted job advertisements, recruitment screening, and evaluating candidate performance.
o Access to Essential Services: Determining creditworthiness excluding fraud detection and accessing eligibility for public assistance.
o Law Enforcement: Profiling during criminal investigations or detections.

3. Limited and Minimal Risk: Lower-risk systems such as consumer chatbots and spam filters generally only need to comply with transparency standards informing users that they are interacting with an AI or basic safety requirements.

4.3.3 STRATEGIC GLOBAL IMPACT: THE BRUSSELS EFFECT IN ACTION

The most significant effect of the EU AI Act is its ability to elevate regional law and to become the global legal benchmark. This influence arises from the Act's extraterritorial clause, which mandates compliance from any global provider whose AI system impacts the EU market. Consequently, this strategy effectively exports the ethical standards of the EU, compelling international businesses to adhere to the Act's rigorous standards for health, safety, and fundamental rights if they wish to enter the largest single market globally. Consulting firms argue that this approach converts regional regulation into a competitive benefit for those who adopt compliance early.

4.3.3.1 The EU AI Act as the Inevitable Standard

The EU AI Act's strategic claim is its intention to serve as the standard global legal framework. This idea is further supported by the centralized enforcement entity: the European AI Office. The European Commission highlights that the AI Office acts as the centre of AI expertise, responsible for executing the AI Act – particularly regarding GPAI models – and promoting the EU's approach worldwide, elevating the EU to a status of a “global reference point” (European Commission, 2025). Additionally, as detailed in the summary of the AI Office’s responsibilities, it ensures strategic alignment with the DSA and DMA, offering the global community a cohesive and thorough framework for digital regulation.

4.3.3.2 Contrasting the Global Regulatory Mosaic

The prominence of the AI Act is highlighted by the varying strategies of other major global actors:

- **United States:** According to Samp et al. (2025), the US relies predominantly on a Presidential Executive Order along with a "mosaic of federal and state laws" which results in a lack of unified federal law. This approach, which is sector-specific and based on guidance, stands in contrast to the AI Act's horizontal, legally binding structure.
- **China:** The Congressional Research Service (2025) indicates that China's regulatory framework is seen as a "vertical, technology-specific framework which is shaped by national security interests," which differs from the EU's horizontal, ethics-based focus.

The comprehensive nature and legal clarity of the EU AI Act provide a more reliable and scalable option for global enterprises, reinforcing its status as the preferred international standard.

4.3.4 IMPLEMENTATION REALITIES AND STRATEGIC RESPONSE

The EU AI Act's strategic goal to set a global standard is met with considerable challenges during its implementation process. Consulting firms such as McKinsey and KPMG uniformly describe compliance not as a simple technical upgrade but as a comprehensive transformation that spans multiple years and millions of euros, requiring ongoing investment and expertise across various functions (Soller et al., 2024; KPMG International, 2024). This section outlines the main economic and organizational challenges involved in converting the Act's overarching principles into enforceable, practical obligations, highlighting the substantial costs of compliance, widespread regulatory uncertainty, and the potential risk of market fragmentation.

4.3.4.1 The burden of compliance

The compliance obligations which include ongoing monitoring, logging, and reassessment after changes represent significant and ongoing administrative expenses.

- **Cost and Innovation Risk:** A survey conducted by ACT-Online revealed that tech startups and SMEs in the EU and UK face considerable annual losses between €94K and €453K due to regulatory compliance delays impacting AI models (Vivek, 2025). Agatic (2025) has pointed out that this intricate and expensive system is unfamiliar to many software developers, resulting in a substantial administrative burden for SMEs.
- **Clarity and Maturity Gaps:** Although deadlines are approaching, a survey by McKinsey found that merely 4% of organizations felt the AI Act's requirements were clear, and only around 29% believed their AI risk governance had attained any degree of maturity by early 2024. Respondents identified the main challenges as "unclear obligations" (81%) and "complexity" (69%) (Luget et al., 2025).

4.3.4.2 Strategic Organizational Response

Global firms are perceiving the Act as a key chance to integrate ethical practices on a worldwide scale. As stated in the EY report, the firm has committed a US$1.4 billion investment into AI transformation efforts to cultivate a culture of compliance and responsible governance, viewing the Act as a pivotal opportunity to bolster long-term business value (EY Global 2025).

KPMG highlights that for those deploying high-risk systems, responsibilities consist of conducting a fundamental rights impact assessment (FRIA) and ensuring human oversight by trained individuals (KPMG International 2024). The report on developing a strategic response further contends that organizations should adopt the AI Act as a global internal standard to facilitate compliance throughout their entire operational scope, recognizing the extraterritorial implications and the Act's relationship with other regulations such as the GDPR.

4.4 GDPR- AI ACT INTERSECTION IN CONSULTING PRACTICE

The AI Act explicitly states that it complements, rather than replaces, the GDPR (Recital 10). For consulting firms, this creates layered obligations. We identify six critical GDPR touchpoints:

- Lawful Basis for Processing (GDPR Article 6)
  - CHALLENGE: AI systems in consulting often process personal data about clients' employees, customers, or stakeholders. Firms must identify a lawful basis for this processing.
  - COMMON BASES:

1. Legitimate Interest (Article 6(1)(f)): For internal AI tools (e.g., knowledge management systems that process employee data). Requires balancing test: firm's interest vs. data subject rights.

2. Contract (Article 6(1)(b)): When AI processing is necessary to deliver contracted consulting services to the client.
3. Consent (Article 6(1)(a)): Rarely viable in B2B consulting due to imbalance of power and difficulty obtaining freely given consent.

AI ACT INTERSECTION: Article 10 of the AI Act requires training data to be "relevant, representative, and free of errors." If personal data is used for training, firms must have a lawful basis not just for the original collection, but also for the "further processing" of training the AI (GDPR Article 6(4) compatibility test).

PRACTICAL EXAMPLE: A consulting firm wants to train an AI model on past project reports (which contain client employee names, performance data). Even if the firm had a lawful basis to collect this data originally (contract with client), using it for AI training requires either:

1. A compatibility assessment under Article 6(4), OR

2. A separate lawful basis (likely legitimate interest, with appropriate safeguards)

- Data Protection Impact Assessment (GDPR Article 35)
  TRIGGER: DPIAs are mandatory for processing that is "likely to result in a high risk to rights and freedoms," including:
  - Systematic and extensive automated decision-making (Article 35(3)(a))
  - Processing on a large scale of special categories of data (Article 35(3)(b))
  - Systematic monitoring (Article 35(3)(c))

CONSULTING SCENARIOS REQUIRING DPIA:

1. AI-powered employee performance evaluation tools (automated decisions + large scale)
2. Sentiment analysis of customer feedback (potentially large scale + profiling)
3. Diversity analytics using demographic data (special categories: race, religion)

AI ACT INTERSECTION: High-risk AI systems under the AI Act require a Fundamental Rights Impact Assessment (FRIA) per Article 27. For many consulting AI applications:

1. The GDPR DPIA and AI Act FRIA cover overlapping concerns (privacy, discrimination)
2. But they have different legal requirements and scopes
3. BEST PRACTICE: Conduct integrated assessment covering both frameworks

5. COMPARATIVE PERSPECTIVE: INDIA'S IT RULES 2021

5.1 RATIONALE FOR COMPARISON

While this paper centres on the EU AI Act, a brief comparison with India's IT Rules 2021 serves three analytical purposes:

1. EXTRATERRITORIAL REACH TESTING: Many global consulting firms (McKinsey, BCG, Deloitte) operate in both the EU and India. Comparing regulatory approaches reveals whether firms face harmonious or conflicting obligations across jurisdictions.

2. REGULATORY PHILOSOPHY CONTRAST: The EU's risk-based, sector-neutral approach (AI Act) differs from India's sector-specific, intermediary-focused approach (IT Rules). This contrast illuminates the EU's strategic choices.

3.GENERALIZABILITY ASSESSMENT: If similar consulting challenges emerge under different regulatory frameworks, it strengthens the claim that AI-privacy-consulting tensions are fundamental, not EU-specific.

We focus on India rather than other jurisdictions (e.g., China, Brazil) because India represents a significant market for Western consulting firms and its regulatory approach is more comparable to EU frameworks (democratic governance, GDPR-influenced data protection law).

5.2 INDIA IT RULES 2021: KEY PROVISIONS AFFECTING AI IN CONSULTING

India's Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, regulate "significant social media intermediaries" and certain online platforms. Unlike the EU AI Act, these rules don't directly address AI systems, but they create privacy and algorithmic transparency obligations relevant to consulting.

KEY PROVISIONS FOR CONSULTING:

1. Due Diligence Obligations (Rule 3) - Intermediaries must inform users about rules/regulations, privacy policy, and user agreement - CONSULTING IMPACT: Firms operating platforms or marketplaces for AI tools must disclose terms.

2. Grievance Redressal (Rule 3(2)) - Appoint Grievance Officer to address complaints within 24 hours - CONSULTING IMPACT: Minimal for traditional consulting; relevant if offering SaaS AI products.

3. Traceability Requirement (Rule 4(2)) - Significant intermediaries must enable identification of "first originator" of information - CONSULTING IMPACT: If consulting-developed AI generates content (like Use Case 2), attribution mechanisms needed.

4. Interplay with Personal Data Protection Act (not yet in force as of Jan 2025) - India's upcoming data protection law mirrors GDPR in many respects - Expected to require DPIAs, cross-border transfer mechanisms, etc.

5.3 COMPARATIVE ANALYSIS: EU vs INDIA

COMPARISON TABLE

Source: Author's comparative analysis based on:

- European Union (2024). Regulation (EU) 2024/1689 on Artificial Intelligence (AI Act). Official Journal of the European Union.

- Government of India, Ministry of Electronics and Information Technology (2021). Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

DIMENSION RULES	EU AI ACT, 2024	INDIA IT RULES, 2021
Regulatory scope	All AI systems in specified sectors/uses (sector-neutral)	Intermediaries and certain online platforms (platform specific)
Risk classification	Explicit 4-tier system (prohibited, high, limited, minimal)	No risk tiering
Transparency obligations	Detailed requirements for high risk systems (Article:13); labelling of AI content (Article 50)	General disclosure obligations for intermediaries
Extraterritorial application	YES: applies to non-EU providers placing systems in EU market	UNCLEAR: primarily targets entities with Indian users
Enforcement mechanism	Fines up to €35M or 7% global turnover	Loss of safe harbour, potential blocking
Impact on consulting	Direct: consulting firms explicitly covered when using/ providing AI	Indirect: consulting affected mainly if operating intermediary platforms

As the comparative analysis with India demonstrates, the EU AI Act's approach is not the only possible regulatory model. However, its comprehensiveness, extraterritorial reach, and first-mover advantage position it as the de facto global standard for AI governance in professional services. This reinforces our finding (Research Question 2) that the EU regulatory framework is driving worldwide transformation of consulting business models, extending influence beyond European borders.

6. CONCLUSION

This research examined the complex and evolving intersection of artificial intelligence, data privacy, and strategic consulting through the lens of the European Union's AI regulatory framework. The findings clearly indicate that AI is not

merely a technological advancement but a structural force. It is fundamentally reshaping professional services, particularly management consulting. AI offers unprecedented efficiency, predictive capability, and analytical depth. Its data-intensive and opaque nature, however, introduces significant ethical, legal, and governance challenges. Among these, data privacy emerges as the most critical concern. This is because the misuse, repurposing, and lack of transparency surrounding personal data directly threaten individual rights, organizational trust, and long-term legitimacy.

The analysis demonstrates that the EU AI Act plays a decisive role in addressing these challenges. This Act introduces a comprehensive, risk-based regulatory framework that prioritizes fundamental rights and enables responsible innovation. The Act not just functions as a compliance burden. The Act acts as a strategic catalyst that is redefining how consulting firms design services, structure internal governance, and compete in global markets. Through its extraterritorial reach and alignment with existing regulations such as the GDPR, the EU AI Act extends its influence beyond Europe. This effectively sets a global benchmark for ethical AI governance – an effect widely referred to as the "Brussels Effect."

From a strategic consulting perspective, this study finds that AI does not signal widespread job displacement. It instead accelerates role transformation. The automation of repetitive, data-intensive tasks challenges the traditional consulting pyramid model. It also elevates the importance of higher-order human capabilities such as judgment, contextual understanding, ethical reasoning, and relationship management. This transition gives rise to the "Hybrid Consultant." A hybrid consultant is a professional who combines AI literacy with interpersonal and strategic expertise. Consequently, consulting firms are increasingly shifting toward responsible AI advisory, compliance readiness, and governance design as core value propositions.

At a broader level, the findings underscore that trust, not technology, is the ultimate strategic differentiator in the AI-driven consulting landscape. Firms that proactively embed ethical governance, transparency, and privacy-by-design into their AI practices are better positioned to sustain client confidence and long-term relevance. This study is limited by its reliance on secondary data and conceptual analysis. It still provides a strong foundation for future empirical research on firm-level implementation strategies and comparative regulatory outcomes. Overall, the research concludes that the future of strategic consulting lies not in resisting AI, but in responsibly integrating it. This integration must place human values, accountability, and trust at the center of technological progress.

REFERENCES

1. Agatic, F. (2025, February 21). *AI Act compliance made easier: Help is on its way for SMEs developing AI solutions*. European DIGITAL SME Alliance. https://www.digitalsme.eu/ai-act-compliance-made-easier-help-is-on-its-way-for-smes-developing-ai-solutions/
2. Axelsson, F., & Leufvén, J.K. (2025). Exploring AI Usage in Management Consulting Leveraging AI for Potential Benefits at the Intersection of Business and Technology [Masters Thesis, Chalmers University of Technology]. https://odr.chalmers.se/server/api/core/bitstreams/0b29c234-159c-4e33-83fa-92bb589c9a0a/content
3. Basavaraju, C. (2025). *The Role of Artificial Intelligence (AI) in Shaping Sustainable Business Practices and the Evolving Landscape of Management Consulting* [Masters Thesis, National College of Ireland]. https://norma.ncirl.ie/7787/1/chiragbasavaraju.pdf
4. Ciobanu, A. C., & Meșniță, G. (2021). AI ethics in business – A bibliometric approach. *Review of Economic and Business Studies, 14*(2), 169–202.
5. Congressional Research Service. (2025). *Regulating artificial intelligence: U.S. and international approaches and considerations for Congress*. https://crsreports.congress.gov/product/pdf/R/R48555
6. Dell'Acqua, F., Saran, A., Mcfowland, R., Krayer, L., Mollick, E., Candelon, F., Lifshitz-Assaf, H., Lakhani, K., & Kellogg, K. (2023). *Navigating the Jagged Technological Frontier: Field Experimental Evidence of the Effects of AI on Knowledge Worker Productivity and Quality*. Harvard Business School Working Paper No. 24-013. https://www.hbs.edu/ris/Publication%20Files/24-013_d9b45b68-9e74-42d6-a1c6-c72fb70c7282.pdf
7. Edwards, L. (2022). *The EU AI Act: A summary of its significance and scope*. Ada Lovelace Institute.
8. European Commission. (2021). *Proposal for a regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206
9. European Commission. (2024, March 8). *European AI Office – Shaping Europe's digital future*. https://digital-strategy.ec.europa.eu/en/policies/ai-office
10. EY Global. (2024, July 17). *Why companies must prepare now for the new EU AI Act*. EY Insights. https://www.ey.com/en_gl/insights/public-policy/why-companies-must-prepare-now-for-the-new-eu-ai-act

11. EY Global. (2025). *How EY is navigating global AI compliance: The EU AI Act and beyond*. https://www.ey.com/en_gl/insights/ai/how-ey-is-navigating-global-ai-compliance-the-eu-ai-act-and-beyond
12. Forradellas, R. F. R., & Gallastegui, L. M. G. (2021). Digital Transformation and Artificial intelligence applied to Business: legal regulations, economic impact and perspective. *Laws*, *10*(3), 70. https://doi.org/10.3390/laws10030070
13. Gupta, A., Amarnani, M., Soanki, S., & Kishore, J. (2025). AI and data privacy in business. *2025 First International Conference on Advances in Computer Science, Electrical, Electronics, and Communication Technologies (CE2CT)*, 109–114.
14. International Council of Management Consulting Institutes. (2024). *Navigating the future: A guide to AI in management consulting*. ICMCI.
15. Kamaruddin, R. I. (2023). *ChatGPT and the future of management consulting: Opportunities and challenges ahead* [Masters thesis, Massachusetts Institute of Technology].
16. KPMG International. (2024). *Decoding the EU Artificial Intelligence Act: Understanding the AI Act's impact and how you can respond*. https://home.kpmg/xx/en/home/insights/2024/02/decoding-the-eu-artificial-intelligence-act.html
17. Li, Z. (2024). AI ethics and transparency in operations management: How governance mechanisms can reduce data bias and privacy risks. *Journal of Applied Economics and Policy Studies*, *13*, 89–93.
18. Luget et al. (2025, January 9). *Insights on responsible AI from the Global AI Trust Maturity Survey*. McKinsey & Company. https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/tech-forward/insights-on-responsible-ai-from-the-global-ai-trust-maturity-survey
19. Mamedova, I. A., Savchenko-Belsky, V., & Velesco, S. (2022, February). Management consulting in digital era. In *Proceedings of the International Scientific Conference "Smart Nations: Global Trends In The Digital Economy"* (Vol. 1, pp. 430–437). Springer International Publishing.
20. Mbah, G. O. (2024). Data privacy in the era of AI: Navigating regulatory landscapes for global businesses. Int. J. Sci. Res. Anal, 13(2), 2396-2405.
21. Mohan, S. K. (2024). Management consulting in the artificial intelligence–LLM era. *Management Consulting Journal*, *7*(1), 9–24.
22. Musch, S., Borrelli, M. C., & Kerrigan, C. (2023). Balancing AI innovation with data protection: A closer look at the EU AI Act. *Journal of Data Protection & Privacy*, *6*(2), 135-152.
23. Nwaimo, C. S., Oluoha, O. M., & Oyedokun, O. (2023). Ethics and governance in data analytics: Navigating innovation and regulation. *Journal of Data Ethics and Governance*, *5*(2), 45–67.
24. Oarue-Itseuwa, E. (2024). Artificial intelligence's impact on the management consultancy sector over the next five years. *Management Consulting Journal*, *7*(1), 49–58.
25. Olatoye, F. O., Awonuga, K. F., Mhlongo, N. Z., Ibeh, C. V., Elufioye, O. A., & Ndubuisi, N. L. (2024). AI and ethics in business: A comprehensive review of responsible AI practices and corporate responsibility. *International Journal of Science and Research Archive*, *11*(1), 1433-1443.
26. Pattanayak, S. (2021). Navigating Ethical Challenges in Business Consulting with Generative AI: Balancing Innovation and Responsibility. *International Journal of Enhanced Research in Management & Computer Applications*, 10(2), 24-32.
27. Potturi, P. (2025). Ethical AI in Business Intelligence: Balancing Innovation with Responsible Data Use. *European Modern Studies Journal*. Vol. 9 No. 4.
28. Samokhvalov, K. (2024). The transformative impact of artificial intelligence on the management consultancy sector. *Management Consulting Journal*, *7*(1), 59–68.
29. Samp, T., Tobey, D., Darling, C., & Loud, T. (2025). *Ten-year moratorium on AI regulation proposed in US Congress | DLA Piper*. DLA Piper. https://www.dlapiper.com/en/insights/publications/ai-outlook/2025/ten-year-moratorium-on-ai
30. Sayyadi, M., Collina, L., & Provitera, M. J. (2023). The end of management consulting as we know it? *Management Consulting Journal*, *6*(2), 68–77.
31. Soller, H., Ohme, A., Schmitz, C., Strandell-Jansson, M., Chapman, T., & Zwiebelmann, Z. (2024, November 13). *The European Union AI Act: Time to start preparing*. McKinsey & Company. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-european-union-ai-act-time-to-start-preparing
32. Tiwari, S. P. (2025). The implications of artificial intelligence in management consulting: A risk and barrier assessment. *Multidisciplinary Reviews*, *8*(8), 2025244–2025244.
33. Vivek. (2025, March 18). *EU AI Act: Understanding compliance costs and penalties*. EU-ai. https://ai-eu-act.eu/blog/eu-ai-act-understanding-compliance-costs-and-penalties/

34. Whittlestone, J., Nyrup, R., Alexandrova, A., Dihal, K., & Cave, S. (2021). *Ethical and societal implications of algorithms, data, and AI: A guideline for responsible innovation*. Leverhulme Centre for the Future of Intelligence.
35. Wilson Sonsini. (2024). *10 things you should know about the EU Artificial Intelligence Act*. Wilson Sonsini Goodrich & Rosati.

Copyrights