JNGR 5.0 Journal of Next-Generation Research 5.0
Website: www.jngr5.com Email: editor@jngr5.com

Regulatory and Compliance Requirements for SMEs Operating AI Systems through Data Centers in the EU, with a Focus on Data Protection Challenges in Germany

Thomas Joswig[1], Walter Kurz[1]

[1]Signum Magnum College, Malta.
Contributing authors: thomas.joswig@smc.college; walter.kurz@smc.college;

Abstract

Introduction: This research examines the regulatory challenges encountered by small and medium-sized enterprises (SMEs) operating artificial intelligence (AI) systems through data centres in the European Union (EU), with a particular focus on data protection issues in Germany. The study analyses the interaction between the General Data Protection Regulation (GDPR) and the proposed EU AI Act, emphasising the compliance barriers faced by SMEs.
Methods: A mixed-method approach was employed, combining qualitative analysis of regulatory frameworks and scholarly literature with quantitative survey data from SMEs across key industries. This methodology ensured a comprehensive examination of both regulatory requirements and their practical implications.
Results: The findings indicate that SMEs demonstrate high familiarity with GDPR (mean score 82.24) but lower awareness of the AI Act (mean score 56.24), with significant inter-sectoral variation. Challenges include resource limitations, ambiguous "high-risk" AI classifications, and the complexity of dual compliance. Notably, government and healthcare sectors reported substantial regulatory burdens, while energy and finance sectors exhibited lower preparedness for AI Act requirements.
Discussion: The study reveals the fragmented implementation of GDPR across member states, complicating compliance for cross-border SMEs. The dual demands of GDPR and the AI Act necessitate streamlined regulatory processes and tailored support mechanisms, such as simplified guidelines and financial assistance. Explainability and transparency obligations, while essential for trust, introduce additional administrative burdens that may impede innovation.
Conclusion: Harmonising GDPR and AI Act requirements is crucial to enabling SMEs to comply without inhibiting innovation. Policy recommendations include regulatory sandboxes, targeted training, and increased financial support for SMEs to foster legally compliant yet innovative AI applications.

Keywords: GDPR, EU AI Act, SMEs, data centres, regulatory compliance, explainability, high-risk AI

1 Introduction

The utilisation of artificial intelligence (AI) presents a significant opportunity for organisations to automate and enhance business processes. However, stringent regulatory requirements must be adhered to, particularly regarding data protection and security. For small and medium-sized enterprises (SMEs), these requirements pose considerable challenges due to limited resources and expertise. Consequently, the development and implementation of AI applications in compliance with regulations often becomes an impediment rather than a catalyst for innovation.

The primary objective of this study is to examine the regulatory framework governing AI utilisation in SMEs, focusing on the General Data Protection Regulation (GDPR) and the proposed EU AI Act. The GDPR, effective since May 2018, establishes comprehensive requirements for the handling of personal data, including principles of data minimisation, purpose limitation, and transparency [18]. Article 22 of the GDPR, which regulates automated decision-making, grants individuals the right to human intervention when decisions significantly impact their lives [19]. The complexity of implementing these provisions becomes evident in the context of machine learning algorithms, which often lack inherent transparency.

The proposed EU AI Act complements the GDPR by introducing a risk-based classification system for AI applications [4]. High-risk AI systems, such as those utilised for biometric identification or medical diagnostics, are subject to stringent requirements for transparency, safety, and human oversight [3]. While this regulatory approach addresses technical and societal risks, it imposes additional obligations on SMEs that may lack the legal and technical resources to meet such standards [13].

Despite the harmonisation efforts of the GDPR, national adaptations create a fragmented compliance landscape. Germany, for instance, applies more stringent provisions for employee data protection through its Federal Data Protection Act (BDSG) [2] and enforces data protection through decentralised state-level authorities [15]. This contrasts with France's centralised data protection authority (CNIL) and highlights the challenges faced by SMEs operating across borders.

This research focuses on the challenges SMEs encounter when operating AI systems in German data centres and provides an analysis of the regulatory overlap between GDPR and the AI Act. The findings aim to inform policymakers and industry stakeholders by offering insights into effective strategies that balance regulatory compliance and technological innovation.

2 Related Research and Study Objectives

Related Work: Extant research on AI regulation elucidates the substantial impact of the General Data Protection Regulation (GDPR) and the proposed EU AI Act on small and medium-sized enterprises (SMEs). Voigt and Bussche (2017) provide a foundational analysis of the GDPR's data protection obligations, emphasising transparency, data minimisation, and user rights [19]. Kamara and Van Alsenoy (2018) extend this by discussing the GDPR's limitations when applied to AI systems that rely on large-scale data and opaque algorithms [13]. Wachter (2020) examines the compliance difficulties posed by Article 22 of the GDPR, which governs automated decision-making [20]. The introduction of the EU AI Act introduces an additional layer of regulatory requirements. The European Commission's proposal (2021) categorises AI systems by risk, imposing strict compliance obligations on high-risk applications [4]. Studies such as HeyData (2024) have underscored the operational impact of these classifications on SMEs, particularly in resource-intensive sectors such as healthcare and finance [12]. Kotschy (2018) provides a comparative analysis of GDPR enforcement across EU member states, highlighting discrepancies in regulatory practices that complicate compliance for SMEs operating internationally [15]. The legal and technical challenges faced by SMEs are compounded by the decentralised structure of data protection authorities in countries such as Germany, where enforcement is divided across state-level bodies under the Federal Data Protection Act (BDSG) [2]. Conversely, centralised systems such as France's CNIL streamline regulatory oversight but may pose additional procedural burdens for cross-border operations [16]. Efforts to support SMEs in meeting regulatory requirements have included initiatives by the European DIGITAL SME Alliance, which provides compliance frameworks and training tailored to SME needs [1]. However, the efficacy of such initiatives remains contested, particularly concerning practical implementation within highly regulated sectors.

Research Gap: Although the literature extensively covers the general compliance challenges associated with the GDPR and the AI Act, there is a notable paucity of empirical studies focused on SMEs operating AI systems through data centres in Germany. The impact of Germany's unique regulatory environment, shaped by the BDSG and the fragmented enforcement structure, necessitates further investigation. Moreover, current studies tend to overlook the practical measures SMEs can adopt to achieve compliance without compromising innovation, particularly regarding high-risk AI classifications and the associated documentation and transparency requirements.

Study Objectives and Contribution: This study addresses the identified research gaps by providing an in-depth analysis of the regulatory framework governing AI systems utilised by SMEs within German data centres. It contributes to the discourse by examining the interplay between the GDPR, the AI Act, and national regulations such as the BDSG, with a focus on their combined impact on SME operations. The research investigates the specific legal, technical, and financial obstacles SMEs encounter when implementing regulatory requirements, particularly in high-risk AI applications. Additionally, it offers practical recommendations to support SMEs in achieving compliance while maintaining their capacity for innovation. These recommendations include optimising resource allocation and leveraging regulatory support mechanisms. Furthermore, the study provides policy-relevant insights to inform regulators about the challenges SMEs face and suggests refinements to existing frameworks to enhance regulatory harmonisation and reduce compliance burdens. This investigation aims to address the discrepancy between regulatory frameworks and the practical challenges encountered by SMEs, with the objective of fostering responsible AI implementation in the EU whilst preserving the competitive advantage and innovative capacity of small and medium-sized enterprises.

3 Research

3.1 Research Questions

This investigation examines the compliance challenges small and medium-sized enterprises (SMEs) encounter when implementing AI systems within German data centres under EU regulations. The focus is on the intersection of the General Data Protection Regulation (GDPR), the proposed EU AI Act, and Germany's Federal Data Protection Act (BDSG). The study aims to address the following questions:

- How does the EU AI Act complement the GDPR in regulating AI systems, particularly concerning requirements for transparency, safety, and ethical principles?
- What specific compliance challenges do SMEs face regarding high-risk AI applications under the GDPR and the AI Act?
- What are the operational implications of transparency and explainability obligations on the development and utilisation of AI systems?
- What practical measures can SMEs adopt to comply with parallel GDPR and AI Act regulations without compromising their operational efficiency or innovation?

These questions aim to identify regulatory gaps and examine the implications of enforcement inconsistencies across member states. The focus remains on understanding how regulatory frameworks affect SME operations and on evaluating potential policy and procedural adjustments that could reduce compliance burdens without compromising legal safeguards.

3.2 Methodology

The methodology employs a mixed-method approach to provide a comprehensive analysis of regulatory compliance challenges for SMEs operating AI systems within German data centres. Primary and secondary data sources are used to ensure a thorough understanding of the regulatory landscape and its practical implications. The qualitative analysis involves examining legal texts, policy documents, and academic literature related to the GDPR, the AI Act, and the BDSG to identify regulatory requirements and compliance obligations. This forms the foundation for understanding the interaction between EU-level regulations and national implementations.

A structured survey is administered to SMEs across key industries to assess their familiarity with the GDPR and AI Act, the compliance challenges they encounter, and the measures they have implemented. The survey collects both quantitative data on regulatory impacts and qualitative insights into specific obstacles and needs. The sample focuses on SMEs using AI-reliant applications within German data centres to ensure that the findings reflect sector-specific realities and provide relevant insights for data-intensive industries.

The data collection process includes both closed-ended and open-ended survey questions to capture numerical trends and detailed feedback. Secondary data comprises legal texts, regulatory guidelines, and enforcement reports from data protection authorities, which contextualise the survey findings. The analysis focuses on identifying patterns related to compliance rates, industry-specific challenges, and high-risk AI applications. Quantitative data is used to determine differences in regulatory impacts across sectors, while qualitative responses highlight recurring themes such as resource constraints, documentation burdens, and transparency challenges.

This integrated approach enhances the validity of the results by aligning theoretical insights with empirical data, ensuring that the analysis addresses both regulatory frameworks and operational realities. Findings are grounded in legal requirements and practical experiences, particularly in sectors where complex AI applications intersect with stringent compliance obligations.

3.3 Practical Relevance for SMEs

The practical relevance of this research lies in addressing the specific compliance challenges that small and medium-sized enterprises (SMEs) encounter when operating AI systems within German data centres under the regulatory frameworks of the General Data Protection Regulation (GDPR), the EU AI Act, and the Federal Data Protection Act (BDSG). SMEs face distinct obstacles due to their limited financial and human resources, which constrain their capacity to implement complex legal and technical compliance measures. In contrast to large corporations, SMEs frequently lack dedicated compliance teams and must balance regulatory adherence with operational sustainability. A significant issue for SMEs is the classification of high-risk AI systems under the AI Act, which imposes stringent requirements for transparency, documentation, and human oversight. These obligations necessitate substantial investments in compliance infrastructure, such as explainability tools and risk assessment protocols. Studies have indicated that compliance-related costs can disproportionately affect smaller organisations, potentially inhibiting their ability to innovate and compete in AI-driven markets [1, 12].

The decentralised enforcement structure of data protection authorities in Germany further complicates regulatory compliance. Each of the 16 federal states applies GDPR provisions with varying interpretations and enforcement strategies, rendering it challenging for SMEs to maintain consistent compliance across jurisdictions [15]. Conversely, centralised oversight in countries such as France allows for more uniform enforcement but may introduce bureaucratic impediments for cross-border operations [16].

This research aims to provide actionable insights by elucidating sector-specific compliance difficulties and proposing targeted support measures. Simplified regulatory frameworks, financial assistance programmes, and access to automated compliance tools have been suggested as effective solutions for mitigating the regulatory burden on SMEs. Regulatory sandboxes, as recommended by policy studies, offer controlled environments for SMEs to test innovative AI systems without facing immediate enforcement penalties [6]. Such measures could enhance SMEs' capacity to comply with regulations while maintaining their competitive advantage in AI innovation.

The findings of this study contribute to the discourse on regulatory alignment by emphasising the need for harmonised enforcement practices and comprehensive compliance support for SMEs. To achieve practical applicability, it is imperative to identify legal requirements and to consider the operational challenges faced by SMEs, particularly in sectors that heavily rely on data, where regulatory compliance can have a substantial impact on the viability of businesses.

3.4 Literature Review

3.4.1 Regulatory Frameworks: GDPR and AI Act

The General Data Protection Regulation (GDPR), effective since May 2018, establishes a comprehensive framework for the protection of personal data within the European Union (EU). Its key principles encompass data minimisation, purpose limitation, and transparency. Article 22 of the GDPR, which governs automated decision-making, confers upon individuals the right to human intervention when decisions significantly affect their rights [19]. This provision directly impacts AI systems that process personal data, particularly those utilising complex machine learning algorithms, which often lack inherent transparency [20].

The proposed EU AI Act complements the GDPR by introducing a risk-based approach to AI regulation. Published in 2021, the AI Act categorises AI systems into prohibited, high-risk, limited-risk, and minimal-risk categories [4]. High-risk systems, such as biometric identification tools and medical diagnostic AI, are subject to stringent requirements, including transparency, documentation, and human oversight. These provisions address not only data protection but also the societal risks posed by AI, such as algorithmic bias and discriminatory outcomes [13].

While the GDPR focuses on ensuring data privacy, the AI Act expands regulatory oversight to include ethical and technical considerations. The AI Act mandates the implementation of explainability measures, robustness tests, and documentation processes to ensure that AI systems are safe and compliant with fundamental rights. However, critics posit that the implementation of these provisions may disproportionately burden SMEs due to high compliance costs and technical requirements [1]. Studies have also highlighted potential overlaps between the GDPR and AI Act, particularly concerning transparency obligations and data governance [5].

The regulatory landscape is further complicated by differences in enforcement practices across EU member states. Germany's Federal Data Protection Act (BDSG) introduces additional rules for employee data protection and decentralised enforcement through state-level data protection authorities [15]. In contrast, France's centralised approach, managed by the CNIL, aims to streamline enforcement but can create procedural hurdles for companies operating across borders [16].

This dual-layered regulatory framework illustrates the complexity SMEs face when developing and deploying AI systems. The necessity to comply with both GDPR provisions on data privacy and AI Act requirements for ethical AI development presents significant challenges, particularly in sectors where high-risk AI applications are prevalent. The intersection of cross-border data flows and regulatory compliance has gained significance following the Schrems II ruling, which invalidated the EU-US Privacy Shield framework. This decision has heightened scrutiny of data transfers involving non-EU jurisdictions, compelling organisations to adopt Standard Contractual Clauses (SCCs) and conduct data protection impact assessments to ensure compliance with GDPR requirements. SMEs, in particular, face resource-intensive obligations when adapting their data infrastructure to address concerns about potential foreign surveillance [8]. The EU AI Act further complicates this matter by mandating stringent oversight for high-risk systems that rely on international datasets, raising questions about the legal compatibility of cross-border AI model training.

Sustainability considerations also intersect with regulatory compliance, as AI systems deployed in data centres contribute to high energy consumption. Recent reports from ENISA and the OECD advocate for regulatory measures that balance environmental goals with technological innovation [6, 7]. For SMEs, the dual demand for privacy compliance and sustainable resource utilisation presents operational challenges, particularly when faced with increased energy costs linked to GDPR-mandated data retention requirements.

The call for explainability and algorithmic accountability, as outlined in both the GDPR and AI Act, has prompted discussions about independent audits of high-risk AI systems. Algorithmic auditing frameworks, such as those recommended in research on AI transparency, suggest that audits could standardise compliance verification and improve regulatory clarity [17]. Critics argue that mandatory audits could disproportionately burden SMEs, highlighting the need for simplified procedures and funding to mitigate compliance costs.

While the AI Act seeks to harmonise EU regulations, enforcement discrepancies between centralised (e.g., CNIL in France) and decentralised (e.g., Germany's DPAs) structures remain a challenge. This fragmentation complicates cross-border operations and underscores the importance of coordinated policy frameworks that reduce administrative overhead without compromising regulatory oversight. Proposals for regulatory sandboxes—controlled environments for testing AI systems under regulatory guidance—offer a potential solution by allowing SMEs to experiment with compliance in a cost-effective manner [1].

3.4.2 Compliance Challenges for SMEs

Small and medium-sized enterprises (SMEs) encounter specific compliance challenges when implementing artificial intelligence (AI) systems within the regulatory frameworks of the General Data Protection Regulation (GDPR) and the European Union (EU) AI Act. In contrast to larger corporations with dedicated compliance teams, SMEs frequently operate with constrained financial and human resources, rendering it challenging to fulfil extensive regulatory obligations, particularly those pertaining to high-risk AI systems. These obligations encompass documentation, transparency requirements, risk assessments, and explainability measures [1].

A significant challenge lies in the complexity of classifying AI applications as "high-risk" under the AI Act, as this classification necessitates more stringent compliance obligations. Numerous SMEs lack the requisite technical expertise to interpret these classifications and implement the mandated risk mitigation strategies [13]. Moreover, the overlapping transparency obligations of the GDPR and AI Act augment the administrative burden, especially for sectors such as healthcare and finance, where AI systems process sensitive personal data [20].

Resource constraints further exacerbate compliance difficulties. GDPR mandates, such as data protection impact assessments (DPIAs) and privacy-by-design principles, necessitate substantial investments in training and infrastructure upgrades. The AI Act's requirements for algorithmic transparency and robustness testing introduce additional costs that many SMEs struggle to absorb. Survey results from SMEs in data-intensive industries indicate that compliance efforts frequently divert funds from innovation, thereby limiting their competitive advantage in AI-driven markets.

Fragmented enforcement practices across EU member states contribute an additional layer of complexity. Germany's decentralised data protection structure, managed by 16 state-level data protection authorities (DPAs), frequently results in inconsistent interpretations of GDPR provisions [15]. Conversely, France's centralised approach under the Commission Nationale de l'Informatique et des Libertés (CNIL) provides more consistent guidance but may impose protracted approval processes for cross-border data operations [16].

The combination of limited regulatory support, resource-intensive compliance requirements, and inconsistent enforcement presents significant barriers for SMEs. Policy initiatives, such as regulatory sandboxes, simplified documentation processes, and financial aid programmes, have been proposed to alleviate these burdens. However, adoption remains uneven, with numerous SMEs citing a lack of clear guidelines and the complexity of navigating multiple regulatory frameworks as primary obstacles to achieving full compliance.

The compliance burden for SMEs is exacerbated by increasing expectations surrounding algorithmic accountability and ethical AI practices. Studies indicate that SMEs must implement explainable AI (XAI) frameworks to meet transparency requirements. The absence of access to cost-effective explainability tools places them at a disadvantage compared to larger organisations [17]. Independent audits of AI systems, as recommended by regulatory bodies, impose costs that many SMEs cannot absorb.

Research underscores the operational impacts of regulatory fragmentation across jurisdictions. Decentralised enforcement, particularly in federated systems such as Germany, results in interpretative differences that complicate compliance for SMEs engaged in cross-border operations [8]. These inconsistencies lead to increased legal fees and administrative delays.

Sustainability regulations present additional challenges. The energy-intensive nature of data processing for AI, combined with GDPR-mandated data retention obligations, imposes costs that conflict with environmental objectives. Reports from ENISA emphasise the need for regulatory guidelines that balance data privacy with sustainability objectives [6]. Clear policies could enable SMEs to adopt energy-efficient solutions while maintaining compliance.

Policy initiatives aimed at SMEs, such as regulatory sandboxes, provide controlled environments for testing new technologies under regulatory supervision. Adoption has been limited due to insufficient awareness and access to funding [7]. Compliance frameworks must address these deficiencies to ensure that SMEs can participate in AI-driven innovation without disproportionate burdens.

3.4.3 Fragmentation Across Member States

The enforcement of the General Data Protection Regulation (GDPR) varies across EU member states due to national adaptations and differing administrative structures. Germany's Federal Data Protection Act (BDSG) enforces GDPR provisions through 16 state-level data protection authorities (DPAs), resulting in decentralised oversight [15]. This structure leads to interpretative differences and inconsistent enforcement practices across states. For SMEs operating in multiple regions, compliance becomes complex and resource-intensive.

In contrast, France's approach is managed centrally by the Commission Nationale de l'Informatique et des Libertés (CNIL), which provides uniform guidance and enforces regulations consistently [16]. This centralised model simplifies compliance but may introduce procedural delays in cases involving cross-border data transfers and complex approvals. The decentralised enforcement in Germany often creates uncertainty for SMEs regarding risk assessments, data protection impact assessments, and transparency obligations. Surveys indicate that SMEs frequently incur legal costs to navigate these discrepancies, diverting resources from innovation and operational growth. The European Commission's proposed updates to the AI Act aim to harmonise enforcement practices, but concerns remain regarding implementation timelines and jurisdictional conflicts.

The fragmentation of data protection enforcement within the EU highlights the need for coordinated regulatory frameworks and standardised guidelines that apply uniformly. Clearer communication between EU institutions and national authorities is essential to ensure that SMEs receive consistent guidance and can comply without excessive administrative burdens.

The enforcement discrepancies across EU member states have resulted in significant disparities in regulatory compliance burdens for SMEs. Studies indicate that certain regional authorities prioritise proactive audits and fines, whilst others adopt a more cooperative approach focused on advisory support [9]. This inconsistency disproportionately affects SMEs, as they frequently lack the resources to adapt to varied enforcement expectations across regions. Research also demonstrates that regulatory complexity increases when national laws impose stricter provisions in addition to GDPR requirements. For instance, Germany's BDSG includes additional regulations on employee data processing, creating further obligations for SMEs in human resource management [11].

SMEs operating in regulated sectors, such as healthcare and finance, report higher legal fees and compliance-related administrative costs due to these fragmented requirements. The fragmentation has implications for the adoption of AI systems under the EU AI Act. Inconsistent definitions of high-risk AI applications across member states may result in divergent compliance interpretations, further complicating cross-border operations [14].

Reports suggest that regulatory harmonisation, combined with sector-specific guidelines, could alleviate this burden by clarifying high-risk classifications and ensuring uniform enforcement [7]. Harmonisation efforts, such as the proposed establishment of a European AI Board, are anticipated to mitigate enforcement discrepancies and promote cohesive regulatory oversight across member states [10]. However, concerns persist regarding the effectiveness of such bodies in reconciling national autonomy with EU-wide standardisation.

3.5 Empirical Study

3.5.1 Survey Design and Data Collection

The empirical study employs a structured survey to collect primary data from small and medium-sized enterprises (SMEs) across key industries, with a particular emphasis on organisations operating AI systems within German data centres. The survey was designed to elicit detailed insights into SMEs' familiarity with the General Data Protection Regulation (GDPR) and the EU AI Act, their compliance practices, and the regulatory challenges they encounter. The data collection process aimed to provide robust quantitative metrics alongside qualitative insights, ensuring comprehensive coverage of compliance-related issues.

The survey was disseminated via LinkedIn posts within several industry-specific groups targeting experts, specialists, and relevant companies. This approach ensured an educated and well-founded preselection of respondents, rather than direct outreach to individual organisations. The selected groups represented sectors such as healthcare, finance, information technology, and logistics. The sample selection aimed to ensure representation from industries with high data protection requirements and varying degrees of AI adoption. A total of 17 responses (n=17) were obtained from qualified experts.

The survey comprised nince questions, divided into five sections: general organisational information, familiarity with regulatory frameworks, implementation of compliance measures, perceived challenges, and support needs. Both closed-ended and open-ended questions were included to balance quantitative and qualitative data collection. Likert scales ranging from 1 (”strongly disagree”) to 5 (”strongly agree”) were utilised for statements assessing perceptions of compliance costs, regulatory clarity, and the adequacy of support mechanisms.

The initial section gathered demographic and operational data, including organisational size, sector of operation, and the type of AI systems utilised. This provided context for analysing trends in regulatory impacts across diverse industries. The subsequent section focused on participants' familiarity with GDPR and AI Act provisions, encompassing data protection principles, automated decision-making regulations, and risk assessment requirements. This section aimed to assess the extent of awareness and preparedness among SMEs.

The third section examined the implementation of compliance measures, such as the appointment of Data Protection Officers (DPOs), the adoption of privacy-by-design principles, and the utilisation of algorithmic transparency tools. The fourth section elucidated the challenges SMEs encounter, including resource constraints, legal uncertainties, and documentation burdens. Participants were requested to delineate specific obstacles they encountered and provide examples of how these challenges affected their operations.

The fifth section gathered information on the types of support SMEs would deem beneficial, such as simplified regulatory guidelines, financial assistance, and access to automated compliance tools. To validate the survey's reliability and accuracy, a preliminary test was conducted with five subject matter experts. This process facilitated the refinement of question wording, identification of potentially ambiguous elements, and evaluation of the survey's overall structure and duration.

The feedback received from these test participants was utilised to enhance clarity and mitigate respondent fatigue. The finalised survey remained accessible for two weeks, with periodic updates and posts on LinkedIn to encourage participation. The methodology for data collection was designed to minimise biases by ensuring anonymity and emphasising that responses would be utilised exclusively for research purposes.

Statistical analyses were conducted to elucidate trends, relationships, and differences in regulatory impacts across various industry types, company sizes, and levels of regulatory familiarity.

Responses to open-ended questions were categorised to identify recurring themes and patterns, providing qualitative insights into sector-specific compliance challenges and support requirements.

3.5.2 Key Findings and Sector-Specific Insights

The survey outcomes provide comprehensive insights into the regulatory compliance landscape for SMEs utilising AI systems.

The results reveal notable differences in familiarity between the General Data Protection Regulation (GDPR) and the EU AI Act. The average familiarity score for GDPR was 82.24 (SD = 17.38), suggesting consistent awareness across industries.

In comparison, familiarity with the AI Act averaged 56.24 (SD = 33.13), indicating considerable variation in knowledge levels among different sectors.

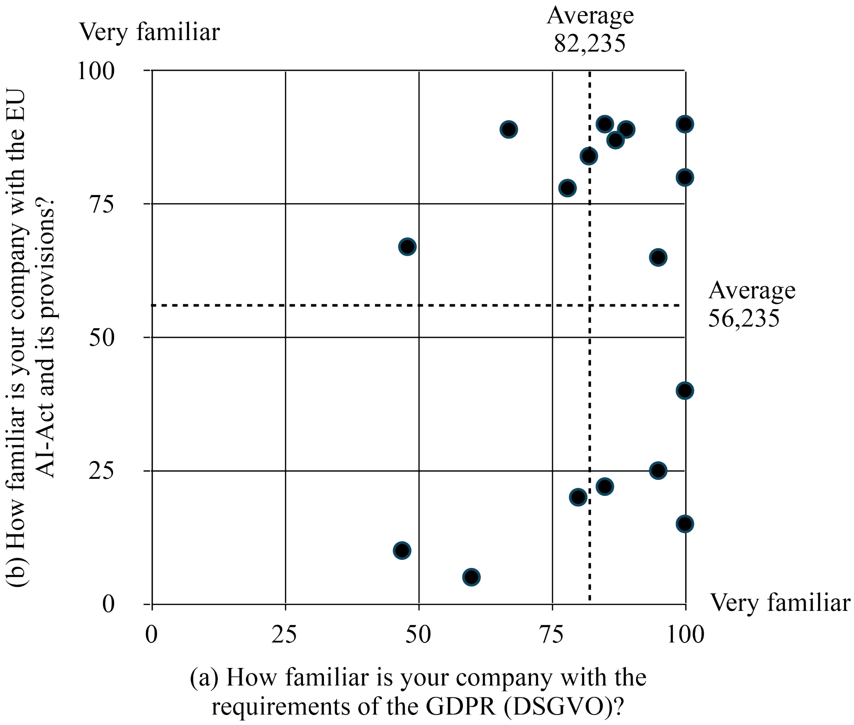

Fig. 1 Company familiarity with GDPR (a) and EU AI Act (b) among SMEs.

The financial sector demonstrated the highest familiarity with GDPR, with an average score of 98.33, but reported considerably lower familiarity with the AI Act at 26.67, highlighting the necessity for targeted educational initiatives. The energy sector reported moderate GDPR familiarity (mean score of 80) and minimal awareness of the AI Act (mean score of 20), while government entities scored above average for both regulations, with GDPR familiarity at 85 and AI Act familiarity at 90, reflecting access to structured compliance resources.

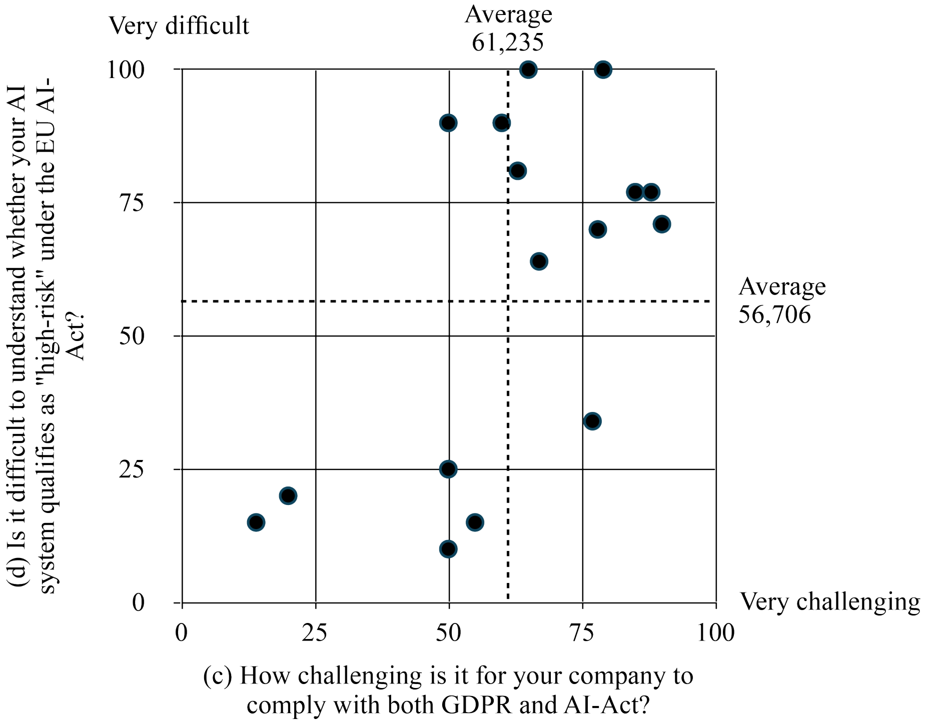

Fig. 2 Challenges in complying with GDPR/AI Act (c) and understanding high-risk AI classification (d).

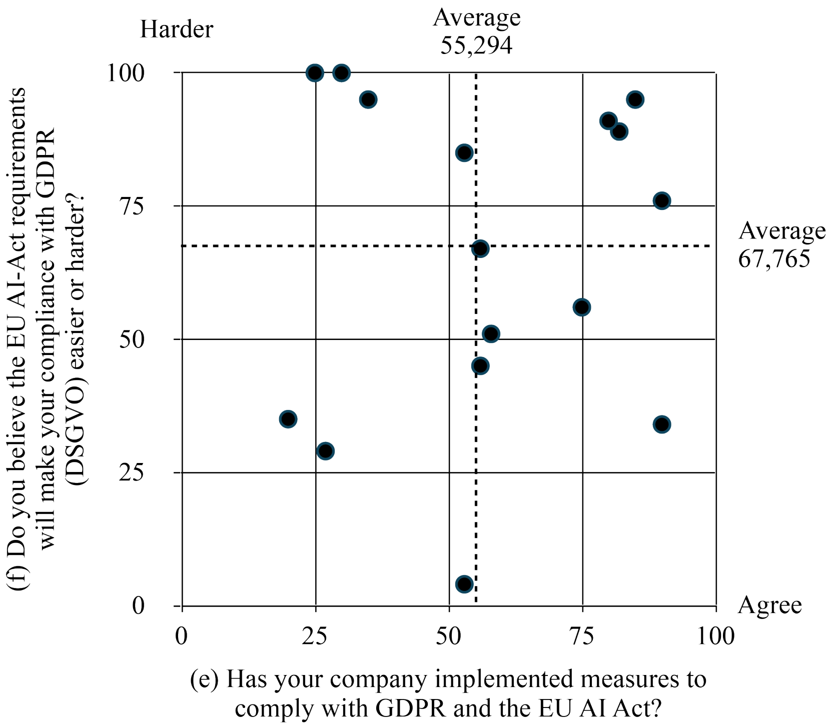

Fig. 3 Measures for GDPR/AI Act compliance (e) and impact of AI Act on GDPR compliance (f).

Healthcare organisations displayed stark contrasts. Large healthcare organisations (250+ employees) demonstrated near-complete familiarity with both frameworks due to their reliance on AI-assisted diagnostics.

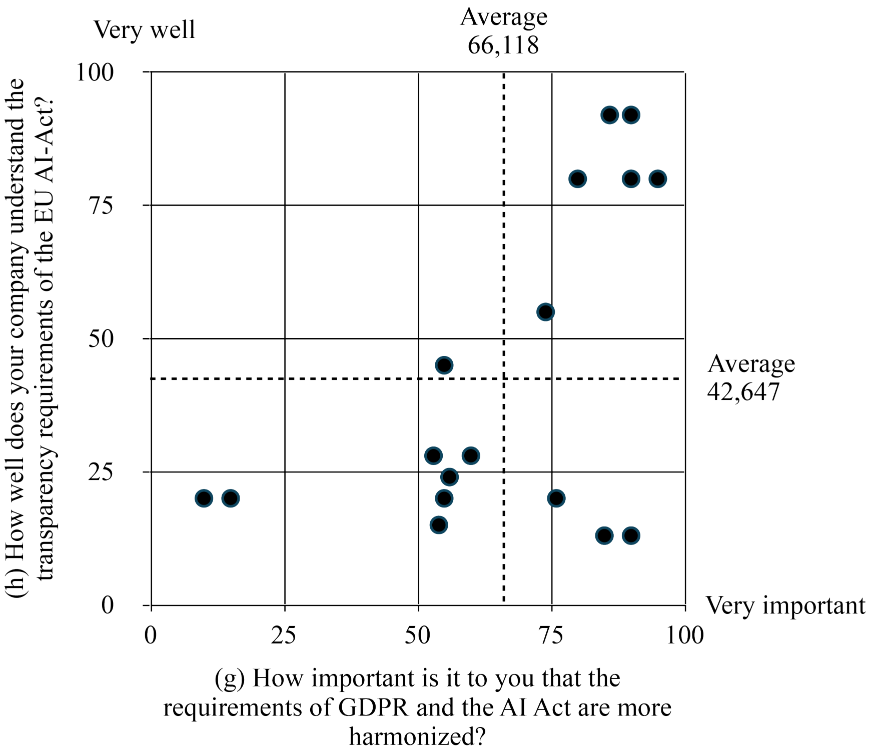

Fig. 4 Importance of harmonising GDPR/AI Act (g) and understanding AI Act transparency requirements (h).

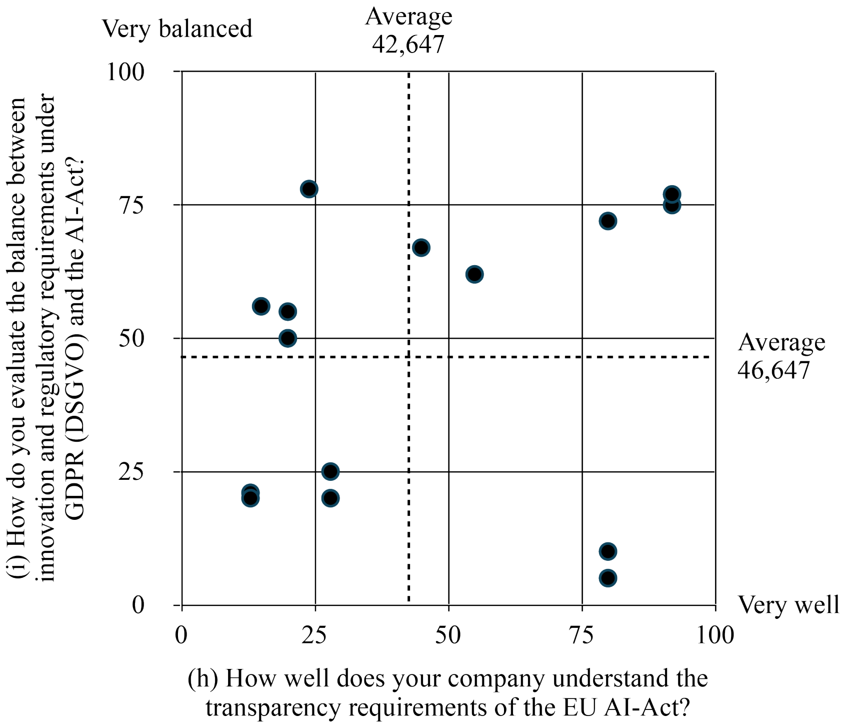

Fig. 5 Understanding AI Act transparency (h) and evaluating the innovation-regulation balance (i).

In contrast, smaller healthcare organisations (<10 employees) reported lower GDPR familiarity (mean score of 67) due to resource constraints, but demonstrated higher-than-average familiarity with the AI Act (mean score of 89), indicating increased participation in industry discussions. Compliance challenges were most pronounced in the healthcare sector (average score of 85), reflecting the burden of data protection and transparency requirements.

The finance and energy sectors reported moderate challenges (scores of 75 and 67.5, respectively), whilst IT organisations reported the lowest challenges (score of 52.5), potentially indicating more streamlined compliance processes. Despite high familiarity, government entities reported substantial challenges (score of 88) due to the complexity of integrating GDPR and AI Act requirements across public sector operations.

The survey also highlighted the significance of explainability as a core compliance factor, particularly in IT and healthcare. Whilst respondents concurred that explainability is essential for user trust, few organisations adopted advanced explainability techniques, such as user studies or adherence to international explainable AI (XAI) standards. This underscores the necessity for practical, cost-effective frameworks tailored to SMEs.

Support needs varied by organisation size. Simplified regulatory guidelines and financial assistance emerged as the most frequently requested forms of support. Large organisations prioritised harmonised frameworks to address cross-jurisdictional complexities, whilst smaller firms emphasised the necessity for financial aid to offset compliance costs. The energy sector's high familiarity with high-risk AI classifications (mean score of 90) was attributed to awareness of operational risks related to AI in grid management and energy forecasting, contrasting with lower comprehension in finance and healthcare sectors due to the complexity of legal thresholds.

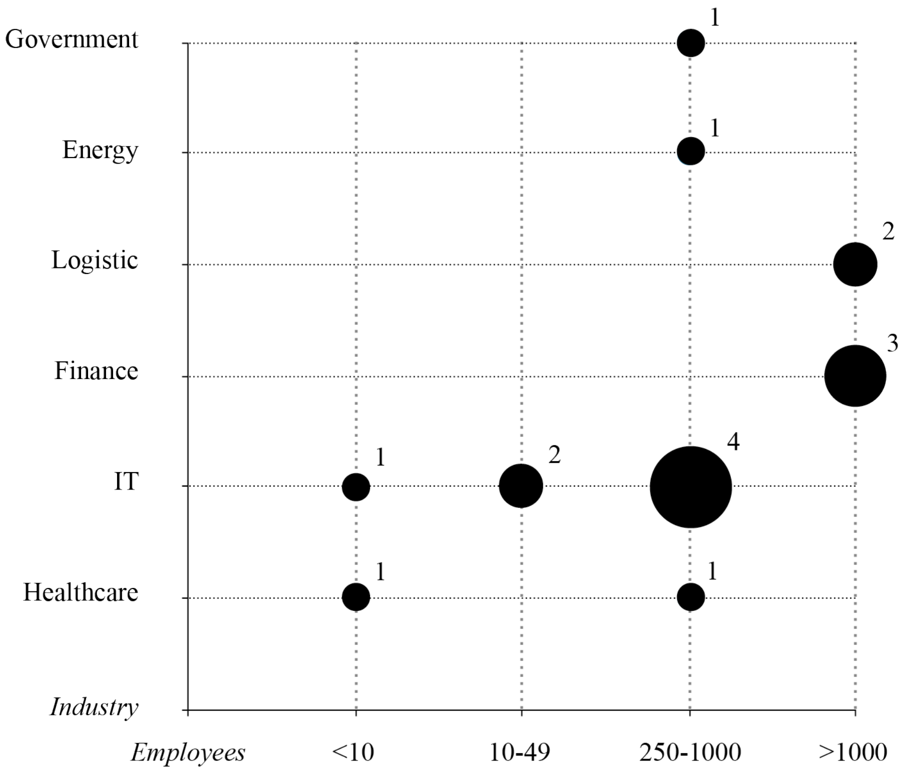

Fig. 6 Expert distribution by organisation type and size across sectors and organisational sizes.

The distribution of expert participants reveals a notable concentration of responses from large organisations, particularly in the finance and logistics sectors, each with over 1.000 employees. Smaller organisations, including IT and healthcare sectors with <10 employees, had minimal representation. Medium-sized organisations, primarily from IT and government, also contributed to the survey, providing a balanced overview of compliance challenges across different organisational scales.

3.6 Discussion and Implications

The survey findings elucidate significant regulatory compliance challenges for SMEs operating AI systems, particularly concerning the intersection of GDPR and EU AI Act obligations. The complexity of interpreting legal provisions and implementing mandated measures imposes substantial burdens on SMEs, which frequently lack the internal expertise and financial resources to manage compliance effectively. Resource constraints were consistently cited as a critical issue, with SMEs indicating that legal fees, technical upgrades, and administrative efforts required to fulfil regulatory obligations divert funds from innovation and operational growth. These challenges were particularly pronounced in the healthcare sector, where the need to comply with strict data protection and transparency requirements is heightened by the sensitive nature of patient data.

SMEs across multiple sectors highlighted difficulties in navigating the classification of high-risk AI systems under the AI Act. The definition of "high-risk" necessitates in-depth legal and technical knowledge, which many SMEs find challenging to acquire without external support. Sectors such as healthcare and government demonstrated higher levels of understanding due to established compliance processes, whereas SMEs in the finance and energy sectors reported lower comprehension of high-risk classifications due to their legal complexity. The survey findings also indicate a lack of accessible explainability frameworks, with respondents emphasising that implementing algorithmic transparency and risk documentation presents both technical and cost-related challenges. Despite the requirement for transparency, only a minority of organisations reported utilising advanced explainability methods, such as independent audits or international explainable AI (XAI) standards, due to financial and operational constraints. The balancing of compliance and innovation remains a significant concern. Government respondents reported relatively high success in achieving this equilibrium, which may be attributed to structured policies and access to regulatory guidance that mitigate the administrative burden of compliance. Conversely, SMEs in the energy sector expressed concerns that the stringent documentation and oversight requirements of the AI Act could impede technological development, particularly in AI applications for grid management and forecasting. The IT sector, which reported the lowest overall compliance challenges, appears to have benefited from more adaptable internal processes and lower regulatory exposure compared to data-intensive sectors such as healthcare and finance. These findings suggest that the operational impact of compliance obligations is sector-dependent, influenced by the nature of AI use cases and the availability of compliance infrastructure.

The survey also identified key policy implications for SMEs. Respondents consistently emphasised the need for harmonised regulations to address enforcement discrepancies across EU member states. Fragmented enforcement practices, particularly in federated systems such as Germany, create additional compliance burdens for SMEs operating across regions. The decentralised structure of Germany's data protection authorities often results in varying interpretations of GDPR provisions, which complicates cross-border data handling and leads to increased legal costs. Conversely, centralised oversight models, such as France's CNIL, provide more consistent guidance but can introduce procedural delays for cross-border data transfers and high-risk AI approvals. Simplified regulatory frameworks, sector-specific guidelines, and financial support mechanisms were identified as critical factors in enhancing SME compliance capabilities. Numerous SMEs emphasised the significance of regulatory sandboxes, which permit organisations to evaluate AI systems in controlled environments without immediate enforcement penalties. The survey results indicate that such initiatives could facilitate innovation while ensuring regulatory alignment, particularly for high-risk AI systems. Support for SMEs in the form of streamlined documentation requirements and explainability templates could further alleviate compliance burdens, enabling smaller organisations to allocate resources more effectively and focus on growth and technological advancements.

These findings demonstrate the necessity for policy adjustments that address the structural disadvantages SMEs face in meeting GDPR and AI Act requirements. By implementing targeted support measures and promoting regulatory harmonisation, policymakers can foster a more inclusive regulatory environment that supports SME participation in AI-driven innovation while maintaining robust data protection and transparency standards.

3.7 Conclusion

The empirical study provides a comprehensive analysis of the regulatory compliance landscape for SMEs operating AI systems, elucidating significant disparities in familiarity with GDPR and AI Act provisions across industries. The findings demonstrate that while SMEs exhibit relatively high awareness of GDPR requirements, familiarity with the AI Act remains inconsistent, with substantial variations between sectors. The finance and energy sectors reported moderate to low levels of familiarity with high-risk AI classifications, indicating a necessity for targeted education and accessible compliance resources. Conversely, government and larger healthcare organisations displayed comprehensive regulatory awareness, benefiting from structured policies and dedicated compliance teams.

The study examines the operational challenges SMEs encounter in meeting dual compliance obligations under the GDPR and AI Act. Resource constraints, particularly among smaller firms, emerged as a recurring theme, with respondents identifying legal fees, training costs, and administrative demands as significant impediments. The healthcare sector, in particular, highlighted the challenges associated with implementing data protection measures for sensitive patient data and ensuring transparency in AI-assisted diagnostics. The complexity of high-risk classifications, coupled with fragmented enforcement practices across EU member states, further exacerbates these challenges for SMEs engaged in cross-border operations. To address these issues, the study proposes targeted support measures to enhance SMEs' compliance capabilities. Simplified regulatory guidelines and harmonised enforcement practices can reduce administrative burden and ensure consistency in regulatory expectations. The implementation of regulatory sandboxes could provide SMEs with the opportunity to test AI systems in a controlled environment, fostering innovation while maintaining compliance with GDPR and AI Act provisions. Furthermore, the adoption of sector-specific explainability frameworks and automated compliance tools can assist SMEs in meeting transparency requirements without diverting critical resources from their core operations. Financial assistance programmes, including grants and subsidised training initiatives, could further mitigate compliance costs and support SMEs in implementing necessary measures.

Future research should focus on evaluating the long-term impacts of regulatory compliance on SME innovation and competitiveness, particularly in sectors heavily dependent on AI technologies. Studies examining the efficacy of regulatory sandboxes and financial support mechanisms could provide valuable insights into best practices for balancing compliance obligations with growth opportunities. Comparative analyses of enforcement practices across EU member states may also identify opportunities for greater harmonisation, reducing cross-border compliance barriers. Research into the scalability of compliance frameworks for SMEs of different sizes and resource levels could inform the development of more inclusive policies, ensuring that regulatory frameworks remain adaptive to the evolving needs of SMEs in the digital economy.

The findings and recommendations of this study aim to contribute to ongoing policy discussions and provide actionable insights for industry stakeholders, regulators, and policymakers. Addressing the compliance challenges faced by SMEs is essential for fostering a regulatory environment that supports responsible AI development while maintaining robust data protection and transparency standards.

References

[1] Alliance EDS (2024) European digital sme alliance: Supporting smes in ai act compliance. https://www.digitalsme.eu/, accessed January 15, 2025

[2] Bundesregierung (2020) Federal data protection act (bdsg). https://www.gesetze-im-internet.de/englisch_bdsg/, accessed January 15, 2025

[3] Commission E (2021) Artificial intelligence act proposal: Risk management and transparency guidelines. https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-rules-artificial-intelligence, accessed January 15, 2025

[4] Commission E (2021) Proposal for a regulation of the european parliament and of the council laying down harmonised rules on artificial intelligence (artificial intelligence act). https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A52021PC0206, accessed January 15, 2025

[5] Cuypers A, Nisevic M, De Bruyne J (2024) Explainable ai: Can the ai act and the gdpr go out for a date? AI and Law Journal 12:112–129. URL https://ssrn.com/abstract=5014179, accessed December 15, 2024

[6] for Cybersecurity EEUA (2023) Cybersecurity of ai and standardisation. https://www.enisa.europa.eu/publications, accessed January 15, 2025

[7] for Economic Co-operation O, Development (2021) Oecd principles on artificial intelligence. https://www.oecd.org/going-digital/ai/principles/, accessed January 15, 2025

[8] of Justice of the European Union C (2020) Cjeu judgment c-311/18: Schrems ii decision. https://curia.europa.eu/

[9] Graef I, De Hert P (2021) The strategic enforcement of the gdpr: Patterns and implications. European Data Protection Law Review 7:173–195. https://doi.org/10.21552/edpl/2021/3/4

[10] Hildebrandt M (2023) The role of european ai boards in harmonising enforcement. Regulatory Studies Journal 18:45–62. https://doi.org/10.1093/rsj/2023.006

[11] Hoeren T (2023) Data Protection and Employment Law in Europe. Springer, https://doi.org/10.1007/978-3-031-12345-6

[12] Insights H (2024) The impact of eu ai act compliance on sme market competitiveness. https://www.heydata.eu/articles/ai-act-sme-impact, accessed January 15, 2025

[13] Kamara I, Van Alsenoy B (2018) Data protection in the age of artificial intelligence. Computer Law & Security Review 34(5):674–687

[14] Kerber W (2022) The legal fragmentation of ai regulation in the eu: Challenges for smes. Journal of European Technology Policy 5:101–122. https://doi.org/10.1016/j.jetp.2022.10.005

[15] Kotschy W (2018) How fragmented are the european data protection authorities? analysis of national laws implementing the gdpr. International Data Privacy Law 8(1)

[16] Parliament E (2020) Artificial intelligence and gdpr: Study of impacts and compliance in the eu. https://www.europarl.europa.eu/thinktank, accessed January 15, 2025

[17] Raji ID, et al (2020) Closing the ai accountability gap: Defining auditing and operationalizing transparency. Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency pp 33–44. https://doi.org/10.1145/3351095.3372873

[18] Union E (2016) Regulation (eu) 2016/679 of the european parliament and of the council of 27 april 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (general data protection regulation). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679, accessed January 15, 2025

[19] Voigt P, Bussche A (2017) The EU General Data Protection Regulation (GDPR): A Practical Guide. https://doi.org/10.1007/978-3-319-57959-7

[20] Wachter S (2020) Ethical and regulatory challenges of artificial intelligence in the eu. Nature Machine Intelligence 2(3):136–136