Thesis Topic

GDPR in Focus: A Literature Review to Bridge Knowledge Gaps

Ankita Negi

Haaga-Helia University of Applied Sciences

Master education Leading Business transformation
Thesis

2024

Author(s)
Ankita Negi

Degree
Master of Business Administration,

Report/thesis title
GDPR in Focus: A Literature Review to Bridge Knowledge Gaps

Number of pages and appendix pages
55 + 1

The thesis explores the multi-layered compliance landscape of the GDPR to address significant research gaps on its theoretical understanding and practical implementation. This study employs an exploratory research design that combines a systematic literature review of 169 academic papers with semi-structured interviews with professionals to uncover critical gaps and develop actionable insights in the field of GDPR studies. Funnel analysis was used to synthesize findings, a process of progressively narrowing broad compliance themes down to detailed challenges and opportunities. It highlighted serious issues in regulatory complexity, interdisciplinary integration challenges, and the absence of tailored, cost-effective approaches for SMEs. The study also demonstrated the compliance hurdles of industries identified as high-risk sectors, such as those in healthcare and e-commerce, where the high reliance on sensitive data increases compliance burdens. The investigation emphasizes how AI-driven compliance tools, privacy-preserving technologies, and strong data governance frameworks are beneficial in facilitating compliance. Comparative analyses involving global regulations like the CCPA, PDPB, and PIPL depict both challenges and opportunities in the pursuit of international harmonization of data protection standards while considering unique local regulatory contexts. It also points out a number of shortfalls in the actual enforcement of consumer rights and investigates issues such as the so-called "privacy paradox," where consumer behavior does not comply with the stated level of privacy concern.

This thesis synthesizes fragmented insights from legal, technological, and organizational perspectives into a comprehensive framework for GDPR compliance. It connects theoretical discourse with practical application and lays the foundation for future research and a roadmap for organizations toward sustainable compliance. The findings underpin long-term benefits that come along with compliance, such as increased trust by consumers, operational efficiency, and competitive advantage, therefore rendering this work a vital contribution to GDPR scholarship and practice.

Keywords :- GDPR compliance, data protection, interdisciplinary framework, AI-driven compliance, global regulation comparison.

Table of contents

1. Introduction

As a dedicated exploration of the evolving impact of data protection, extensive literature on the General Data Protection Regulation (GDPR) was reviewed indiscriminately, encompassing both leading and general works. Initially, the wealth of articles and books was approached with enthusiasm, as the breadth of information offered appeared promising. However, this exploration soon resulted in a sense of overwhelm, as much of the literature reiterated similar points, creating an avalanche of redundant information.

Studies predominantly focused on highlighting issues associated with GDPR but frequently failed to propose practical alternatives(Voigt and Von dem Bussche 2017). In some cases, recommendations were offered but proved unrelated to the regulation’s most pressing challenges. Positioned at the intersection of public policy and technological innovation, GDPR has significantly influenced international practices and introduced widespread changes. Despite its vast scope, much of the existing literature appeared repetitive, marked by overlapping arguments and a lack of fresh perspectives.

The GDPR, officially known as Regulation EU 2016/679 (European Parliament 1995), established protection of the personal data of individuals from unauthorized use and breach. It was a complete data protection directive which correspondingly dealt with privacy and security issues that the earlier directives, like Directive 95/46/EC and Hungary's Act LXIII of 1992 (European Parliament 1995) could not fully control. These previous frameworks lacked the strength in regulating the heavy processing of personal data effectively. Coming during rapid technological advances, social change, and the need for a harmonized market, GDPR is an increasingly crucial safeguard of individuals' privacy rights in handling their digital data.

1.1 Objective

The objective of this thesis is to bridge the significant gaps in the existing body of research on GDPR compliance. This objective will be achieved by synthesizing fragmented findings across disciplines and sectors. Being a broad data protection framework, GDPR has wide-reaching implications for organizations across various industries. However, the current research really reflects a disconnect in both the theoretical and practical aspects of such fragmented studies that usually fail to paint a cohesive (Voigt and Von dem Bussche 2017), interdisciplinary business case of the complexities on compliance with the GDPR. The purpose of this thesis is to bridge this fragmentation through the integration of insights provided via technical, organizational and other regulations views into a comprehensive framework that could be used in understanding the GDPR.

1.2 Research Problem and Questions

Through an in-depth review of 169 research papers, this study addresses two central research questions:

To examine and assess the body of current research on GDPR

What are the significant gaps in current knowledge regarding GDPR's impact, as identified through a critical analysis of existing research?

1.3 Delimitation

This study does not purport to present a point-by-point legal analysis of the miscellaneous GDPR requirements toward compliance, nor does it attempt to give exhaustive compliance guidelines. Even paid articles, which formed part of the literature review, were excluded from this study due to budgetary constraints. This research, therefore, is intended to analyze the general implications of GDPR in many sectors and tries to reveal gaps in knowledge which further guides future research concerning the impact of this regulation and also practical problems related to its application.

1.4 Key concepts

The fundamental data protection concepts of data minimisation, accountability, and transparency form the basis of GDPR rules.These principles establish the legal basis for organizational compliance requirements.(De Hert & Papakonstantinou 2021)This paper presents a broad overview of GDPR's impact on organizations: operational shifts, compliance costs, and the integration of privacy-oriented policies into business operations(Voigt and Von dem Bussche 2017). Central to GDPR are data subject rights (European Data Protection Board 2021), including access, rectification, erasure, data portability, and the right to be forgotten, empowering individuals to control their personal information.

Organizations face several compliance challenges, from robust consent management to enhanced data security and operational changes promoting accountability(European Data Protection Board 2021). This study also compares GDPR with global data protection frameworks—the CCPA, PIPEDA, and PDPA—highlighting key differences that influence compliance strategies for multinational organizations (Shah 2021). GDPR’s role in driving technology development in areas such as artificial intelligence, big data, and the Internet of Things is explored, particularly where compliance imperatives intersect with innovation(Cao & Kretschmer 2024). Finally, this study highlights significant gaps in GDPR literature, identifying

underexplored topics that warrant future research to deepen understanding of GDPR's long-term effects and sector-specific challenges.

The layout of the thesis is designed to take the reader through a holistic analysis of the challenges and solutions alike regarding compliance with the GDPR. Starting with an Introduction that outlines the objectives, significance, and scope of the research, it follows by a Literature Review that synthesizes findings from 169 academic papers to establish existing gaps in GDPR compliance research. The Methodology section details the mixed-methods approach, including both thematic analysis of literature and insights from semi-structured interviews with GDPR professionals.

In the Findings and Discussion section, key themes are explored, such as interdisciplinary compliance needs, sector-specific challenges, and the necessity for practical compliance tools. This section also compares GDPR with other global regulations, highlighting compliance complexities for multinational organizations. The Conclusion and Recommendations offers actionable proposals for addressing the identified gaps, emphasizing the development of AI-driven tools and sector-specific frameworks to support sustainable compliance. The thesis closes with suggestions for Further Research, identifying future studies to enhance GDPR understanding and application across diverse contexts.

2. Literature review

2.1 Summary of The Analytical Models for the literature review

This study adopts a structured theoretical framework, drawing on established models and theories to analyze GDPR compliance. A pivotal model utilized is "A Framework for GDPR Compliance for Small- and Medium-Sized Enterprises" (Brodin, 2019), selected for its credibility and nuanced insights into the compliance challenges faced by SMEs. This framework served as a foundational structure for categorizing and examining GDPR compliance issues, particularly addressing the resource constraints unique to SMEs.

A mixed-method approach was employed to ensure a comprehensive understanding of GDPR compliance(Reeves 2020). Initially, themes were identified and organized based on the SME compliance framework, enabling a systematic investigation into the legal, operational, and technological dimensions of GDPR (Brodin 2019). These themes were further refined through funnel analysis, progressively narrowing the focus from broad compliance categories to specific, actionable challenges encountered by organizations.(Hoofnagle, van der Sloot & Borgesius 2019)

The findings from the literature review were subsequently consolidated through primary data collection via semi-structured interviews with professionals whose work involves or is significantly affected by GDPR compliance(Veale & Zuiderveen Borgesius 2019). This integration of frameworks, analytical models, and interview data ensures that the study's conclusions are firmly rooted in established GDPR literature (Hoofnagle, van der Sloot & Borgesius 2019) while capturing nuanced challenges and practical implications (Reeves 2020). The result is a robust, actionable exploration of GDPR compliance that bridges theoretical insights with real-world applications.

2.2 Understanding the Key Principles of GDPR

In this digitisation era, it cannot go without mention that the need to ensure data subjects' personal information is processed within the law and justly. This implies that personal data shall be processed lawfully, fairly, and in a transparent manner to the data subject (Štarchoň & Pikulík 2019). Fairness and transparency in our processing practices will equate to trust and confidence in data subjects. In addition, freely given, specific, informed, and unambiguous consent is required, and the data subject shall have the right to withdraw the said consent at any time.

2.2.1 Purpose Limitation

Data processing under the EU GDPR must adhere to the principle of purpose limitation (Bakare et al. (2024), legitimate purposes and not process it beyond these purposes. In other words, data processing activities must be tailored, proportionate, and achieve the prescribed objectives. Organizations must clearly communicate the primary goal of data processing and refrain from using personal information for unit ended or unrelated purposes. This principle is crucial to preventing data subject exploitation and safeguarding their privacy rights. Adherence to purpose limitation can be achieved through transparent and explicit disclosure practices, ensuring that each data processing request corresponds to the specified purpose and handling personal data only for the agreed-upon objectives. By strictly adhering to this principle, organizations can build trust and foster a culture of respect for the individual's privacy rights. This not only improves public perception but also helps organizations operate within legal boundaries, minimizing the risks and liabilities associated with data misuse.

2.2.2 Data Minimization

According to the General Data Protection Regulation, an organization must only gather the personal information that is absolutely required to accomplish its goals (European Parliament 1995). This principle recognizes that minimizing the gathering and storing of personal information is the most effective way to safeguard people's privacy against exploitation or abuse (Biega & Finck n.d.).

2.2.3 Accuracy

The need for enterprises to confirm the timeliness and correctness of personal data is emphasized by the GDPR (Kuner et al., 2020). It is the responsibility of companies to make every effort to ensure that the information they collect and maintain about individuals is accurate and current, as inaccurate or outdated data can lead to discriminatory or unjust decisions and harm to data subjects (Schwartz & Solove, 2021). Essentially, maintaining data accuracy under the GDPR involves continuous monitoring and validation efforts by data controllers, as required by the principle of accuracy outlined in Article 5(1)(d) of the regulation (European Data Protection Board, 2021).

Organizations should ensure that any personal information obtained, processed, and handled is accurate and current when necessary. This aligns with GDPR, as inaccurate or outdated information can lead to unfair outcomes for data subjects (Drąg & Szymura 2018). Data

controllers are expected to have stringent processes for verifying and validating the accuracy and currency of personal data regarding individuals, updating it as appropriate.

2.2.4 Storage Limitation

According to the storage limitation principle, personal information should not be kept on file for longer than is required for the reasons for which it was gathered or processed. Data controllers are required to carefully consider how long personal data should be kept on file and, when that period has elapsed, to either delete or anonymise it. Data retention beyond its useful life violates GDPR data protection regulations and poses needless privacy and security risks. (Drąg & Szymura 2018) (Biega & Finck 2021)

GDPR mandates that after a purpose is served, gathered and processed personal data must be anonymised or erased. Excessive data retention raises the possibility of security and privacy breaches and violates the regulation's data protection guidelines. (Biega & Finck 2021).

2.5.5 Integrity and Confidentiality

The GDPR key principles state that the data controllers and processors should implement technical and operational safeguards to protect personal data from unlawful accidents. Organization must insure appropriate measures to take care of the Personal data they handle to protect the fundamental rights of the data subjects, protections from data breach, data compromise and accidental loss of data. Must be ensured by the organizations. (Zichichi et al. 2022)

2.6.6 Accountability

The principle of accountability is beyond compliance of GDPR, this key principle requires organizations to demonstrate their commitment to the GDPR regulations. The data controller and processor should be able to provide evidence of their ability of compliance to the GDPR regulation this can be demonstrated with record-keeping practices, polices and appropriate procedures. (Zichichi et al. 2022) This principle underlines the importance of transparency and accountability in data protection, ensuring that the organizations can be held accountable for their handling of personal data and the measures they have taken to safeguard it.

2.3 Themes Identified from "A Framework for GDPR Compliance for Small- and Medium-Sized Enterprises" By Martin Brodin

The paper "A Framework for GDPR Compliance for Small- and Medium-Sized Enterprises" (Brodin's 2019)was chosen because it is highly structured in answering the problem of GDPR compliance. The framework presented in the paper aligns with the objectives of the thesis as it could be employed as a method of systematically dislodging the mysteries of GDPR and its impact, especially on SMEs. This paper was highly relevant for organizing and synthesizing themes in the literature review, as it provided an empirical and theoretical basis for developing compliance strategies with a focus on design science and practical evaluations. Its insights into compliance principles, sector-specific challenges, and actionable frameworks provide a good foundation for identifying and categorizing the gaps in GDPR compliance research.

Compliance Challenges	**Initial and Ongoing Costs**	**Consumer Rights**	**Technology and Innovation**	**GDPR and Other Regulation**
Complexity and Ambiguity of Regulations	Implementation Costs	Right of Access	Market Dynamics and Competition	United States
Lack of Resources and Expertise	Cost of Annual Compliance	Right to Rectification	Encouragement of Privacy-Preserving Technologies	India
Unsatisfactory Technical and Organizational Measures	Labor Costs	Right to Erasure	Impact on Data Sharing and Open Innovation	China
Non-Exercise of Data Subject Rights	Technology and Infrastructure	Right to Restrict Processing	Innovation in Data Management Practices	Thailand
Insufficient Data Processing	Professional Services and	Right to Data Portability	Regulatory Uncertainty	United Kingdom

Agreements	Legal Fees			
Challenges with International Data Transfers	Training and Awareness	Right to Object to Processing	Long-Term Benefits of Compliance	East African
Non-Uniform Application across EC Member States	Operational Changes	Consumer Enhanced Rights		Australia
High Cost of Compliance	Market Impact	Increased Transparency		Canada
Public Awareness and Understanding	Insurance Costs	Privacy Paradox		South Asian Countries
Technological Challenges		Implications for Marketing Practices		United Arab Emirates
		Consumer Trust		
		Compliance Issues		
		Global Impact		
		Consumer Engagement		
		Economic Implications		

2.4 How GDPR Compliance Themes Were Addressed in the Literature

Complexity and Ambiguity of Regulations: Literature often criticizes the complexity and ambiguity of GDPR; organizations often struggle to interpret and operationalize its provisions.

Researchers emphasize that the non-uniform application of GDPR in the various EU member states exacerbates this challenge, resulting in a lot of inconsistencies that further deter multinational organizations from achieving full compliance. Researchers like (Tikkinen-Piri et al. 2017) discuss how abstract the terms "appropriate measures" and "legitimate interests" are, which can be interpreted rather subjectively. It provides ambiguity in compliance matters. This regulatory opaqueness does not only affect SMEs but larger organizations as well, making it challenging to develop standard compliance frameworks.

Initial and Ongoing Costs: The cost of compliance has been extensively discussed in the literature (Voigt & von dem Bussche, 2017). Implementation expenses, such as updates to technological infrastructure, Data Protection Impact Assessments (DPIAs), and legal consulting fees, are widely recognized as significant barriers for organizations of all sizes. Studies highlight that SMEs and mid-sized organizations face greater challenges due to their limited budgets (Schwartz & Solove, 2021). For larger corporations, the focus often shifts to annual compliance costs, which encompass professional services, employee training, and operational adjustments (European Data Protection Board, 2022). Additionally, these financial burdens contribute to broader economic effects, such as reduced market competitiveness and the diversion of resources away from innovation and growth initiatives (Binns, 2019).

Consumer Rights :There has been an intense debate in the literature regarding the increased consumer rights introduced through the GDPR, including the rights of access, rectification, erasure, and data portability (Voigt & von dem Bussche, 2017). However, the practical implementation of these rights remains a critical challenge. Many studies highlight a disconnect between the theoretical empowerment of data subjects and the actual application of these rights in practice (Kuner et al., 2020). Scholars critique organizations for lacking the mechanisms and processes needed to handle consumer requests effectively, with challenges compounded by weak technological infrastructure and inadequate internal workflows (Schwartz & Solove, 2021). Adding to this complexity is the so-called "privacy paradox"—where consumers express concern about privacy yet continue to engage in data-sharing behaviors, often without fully understanding their rights or the implications (Acquisti et al., 2015).

Technology and Innovation: It also explores how the GDPR influences technological and innovation landscapes. Some works praise GDPR for fostering the development of privacy-preserving technologies and promoting innovative data management practices (Voigt & von dem Bussche, 2017). Conversely, others criticize the regulation for its negative impact on data sharing and open innovation, citing regulatory uncertainty as a significant factor stalling progress in fields

like artificial intelligence (AI) and machine learning, where access to large datasets is critical (Schwartz & Solove, 2021).

However, GDPR has also spurred the growth of privacy-enhancing technologies (PETs), such as differential privacy and secure multi-party computation, demonstrating how compliance can coexist with innovation (Dwork & Roth, 2014). This dual effect underscores the complex relationship between stringent data protection regulations and the evolving technological landscape.

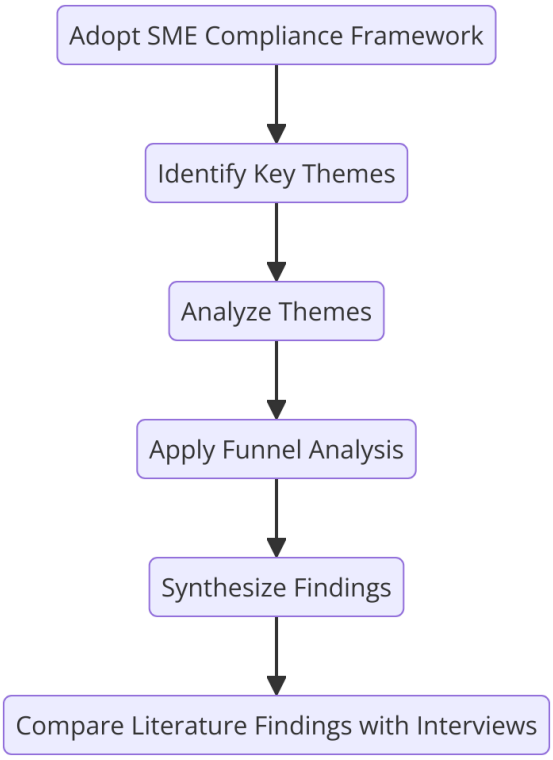
Comparison of GDPR and Other Regulations: Comparative analyses highlight how the General Data Protection Regulation (GDPR) aligns with or differs from data protection laws in countries like the United States, China, and India. For instance, GDPR's robust provisions contrast with the U.S.'s sectoral approach to data protection (Schwartz & Solove, 2021). A recurring issue is navigating international data transfers, especially post-Schrems II, which invalidated the EU-U.S. Privacy Shield and left businesses relying on complex mechanisms like Standard Contractual Clauses (SCCs) (Court of Justice of the European Union, 2020). Emerging frameworks such as India's Personal Data Protection Bill (PDPB) and Thailand's Personal Data Protection Act (PDPA), which share GDPR-like principles, further demonstrate how GDPR has become a global benchmark for data protection (Greenleaf, 2021).o analyzed for their possible influence on the evolution of global standards of data protection.

Conclusion

The identified themes of GDPR compliance—spanning regulatory complexity, financial burdens, consumer rights, technological impacts, and global comparisons—relate directly to the research questions by providing a structured lens to evaluate existing literature. These themes reveal recurring gaps, such as the insufficient integration of practical solutions for compliance, limited exploration of long-term benefits, and a lack of sector-specific studies addressing unique organizational challenges. By critically analyzing these themes, the research highlights areas where current literature falls short in capturing GDPR's comprehensive impact.

Addressing these gaps supports the primary aim of this study: to review and evaluate the existing literature to identify the significant deficiencies in understanding GDPR's implications. This thematic approach not only structures the evaluation but also bridges the theoretical discourse with practical insights, laying a foundation for future research to develop actionable strategies and fill the knowledge void in GDPR compliance.

3.Research Methods



3.1 Research Approach

The research design is exploratory in nature and integrates a systematic literature (Smith et al. 2023) review with the collection of primary data through semi-structured interviews. The objective of this work is to synthesize existing research on emerging knowledge gaps related to compliance with the GDPR and its organizational implications. Thus, a unified theoretical and practical look will be provided regarding the multi-dimensional influence of the GDPR.(Wachter, Mittelstadt, and Floridi 2017)

3.1.1 Systematic Literature Review

This study conducted a systematic review of 169 academic papers selected out of an initial pool of 185 abstracts. Papers were screened to remove repeated, paid, and irrelevant content in order to achieve a quality dataset. This diverse pool of sources-peer-reviewed articles, regulatory reports, and industry studies-enabled a truly interdisciplinary approach by combining aspects of law, technology, and organization. This ensures a sound basis for the various challenges and benefits arising out of GDPR compliance across sectors and organization types. (Smith et al. 2023)

In addition to this literature review, real-world insights were provided through semi-structured interviews with professionals involved in GDPR compliance-for example, cybersecurity consultants, software engineers, information security leads-which highlighted practical challenges faced by organizations. These balanced the findings from the literature by bridging the gap from theoretical frameworks to practical realities.

3.1.2 Structured Approach to GDPR Compliance

This research uses "A Framework for GDPR Compliance for Small- and Medium-Sized Enterprises" by (Brodin 2019), which is very useful in organizing and analyzing themes on GDPR compliance. This framework, as proposed in the paper, is particularly useful for categorizing and examining compliance issues, which should provide insight into legal, operational, and technological aspects of GDPR. It was designed to take into consideration special resource conditions of SMEs but was flexible for large organizations too.

The framework handpoints key compliance phases of analysis, design, and implementation, while giving structured grounds for the multi-faceted impact that GDPR will have. By aligning the study to this framework, the research ensures a systematic and comprehensive thematic exploration.

3.1.3 Key Themes Synthesised

Using the SME compliance framework, the following themes were synthesised.

Legal Compliance	Complexity of GDPR requirements, legal ambiguities, and international data transfers.
Operational Challenges	Training and awareness, cost of compliance, and resource constraints in SMEs.
Technological Dimensions	Adoption of AI and privacy-preserving technologies, cybersecurity measures.
Sector-Specific	Tailored solutions for healthcare, e-commerce, and tech startups.
Long-Term Benefits of GDPR	Enhanced consumer trust, better data governance, and operational efficiency.
Global and Comparative Insights	Differences in GDPR implementation vs. other data regulations (e.g., in the US, India)

3.2 Methods and implementation

3.2.1 Adopt SME Compliance Framework: This research relies on the "Framework for GDPR Compliance for Smalland Medium-Sized Enterprises"(Brodin 2019).The framework offers a systematic model for capturing and classifying GDPR compliance challenges and benefits. This framework grounds the study in manageable themes that answer legal, operational, and technological dimensions of GDPR compliance.

3.2.2 Identify Key Themes: Using the SME compliance framework (Brodin 2019), key themes such as resource constraints, technological challenges, legal ambiguities, and sector-specific compliance requirements are identified. These themes serve as the foundation for analyzing GDPR's impact on organizations, ensuring a systematic exploration of its multi-dimensional effects.

3.2.3 Analyzing Themes: After reviewing 189 research paper abstracts, 169 papers were carefully selected for this thesis, ensuring the elimination of repetitive, paid, and irrelevant content. Each selected paper was meticulously analyzed to identify and understand the themes explored in research conducted up until 2024. This rigorous process incorporated a critical review of academic works, regulatory reports, and industry studies, ensuring a robust theoretical foundation.

3.2.4 Funnel Approach and Docanalyzer AI: Once themes were established, A funnel approach was applied to progressively narrow down findings, moving from broader compliance themes to specific, actionable insights. This method allowed the study to quantify and prioritize the compliance issues by measuring their impact across various dimensions, such as financial, operational, and technological aspects.

To enhance efficiency in data management, Docanalyzer AI was used to organize, label, and store all research papers, ensuring consistency and traceability of information. Docanalyzer AI facilitated labeling and tracking of key insights from the 169 selected articles, providing structured support for the funnel analysis. This AI-assisted tool was instrumental in synthesizing information from a large dataset, making it possible to mark findings, identify patterns, and measure gaps with precision.

3.2.5 Synthesis of Findings and Identification of Knowledge Gaps: The final findings were derived by synthesizing insights from both the literature review and the semi-structured interviews. The study identified common knowledge gaps in GDPR compliance, where theoretical insights and practical experiences aligned. This synthesis enabled the project to present findings that were not merely a summary of existing literature but were enriched by real-world insights

from GDPR professionals. Key gaps in knowledge were highlighted, providing actionable insights and guidance for organizations navigating GDPR compliance challenges.

3.3 Data collection

3.3.1 Primary Data

Semi-structured interviews were used as the primary data collection tool. This format allowed for flexibility in exploring predefined themes while also enabling respondents to introduce new perspectives based on their unique experiences.

The study employed a purposeful sampling strategy to select six respondents directly involved in GDPR-related activities across diverse professional roles. This approach ensured a range of perspectives on GDPR implementation and its implications, reflecting the complexity and multidimensional nature of the regulation.

Selection Criteria:

Participants were chosen for their professional expertise in GDPR compliance.

Respondents represented various organizational roles and industries, such as technology, cybersecurity, sales, and auditing, providing a comprehensive understanding of GDPR’s impact.

Interview Categories and Questions:

Impact on Work: How does GDPR affect your professional responsibilities?

Sources of Updates: How do you stay informed about GDPR changes and updates?

Broader Impacts: What areas of life or business do you believe GDPR influences the most?

Future Outlook: What do you see as the future challenges and opportunities of GDPR?

Research Gaps: Are there any areas of GDPR-related research you believe remain underexplored?

Thematic Analysis:

Coding: Responses were systematically categorized into thematic nodes, such as "work challenges," "GDPR impacts," and "future opportunities."

Pattern Recognition: Commonalities across responses were identified, highlighting shared experiences, while differences illuminated unique professional insights.

Interpretation: Thematic clusters were synthesized into key findings, contextualized within the broader framework of GDPR compliance challenges and opportunities.

This approach ensured a balanced analysis that captured both recurring themes and nuanced perspectives, contributing to a robust understanding of GDPR's implications. Findings were cross-referenced with the theoretical framework to ensure alignment with existing literature while highlighting areas for further exploration.

Profession/Designation	Work Aspect Affected by GDPR	GDPR Updates Source	Key GDPR Impact Areas Identified
Software Engineer	Handling customer-sensitive/private data	Technology websites, newsletters	Website browsing, data handling
Cybersecurity Consultant	Collaboration with businesses for compliance	Business-related GDPR guidelines	Empowerment through data control
Assistant, Auditing and Expert	Administrative tasks, creating policies	Training and session	Data protection, processing transparency
Nordic Information Security Assurance Lead	Cybersecurity controls Privacy team updates	Privacy team updates	Challenges in cybersecurity and life domains
Sales Manager	Customer data processing	Internal training and updates	Compliance and company awareness
Analyst (Financial)	Collection and management of client data.	EUR LEX, official sites	Enhanced rights for customers to review and delete their data.

3.3.2 Secondary Data

Secondary data for this research was collected following the identification of themes derived from "A Framework for GDPR Compliance for Small- and Medium-Sized Enterprises" (Brodin, 2019). This framework provided the foundational structure for categorizing and analyzing the key

aspects of GDPR compliance. Data collection involved an extensive review of academic databases, including ResearchGate, Google scolar and IEEE, to ensure access to the most current and relevant research on GDPR compliance up to 2024.

A)Summary of the data collected from 169 research papers

a) Legal Obligations for businesses Under GDPR - General Data Protection Regulation has indeed hugely affected the processing of personal data through businesses by imposing a great deal of legal obligations on handling personal data to make such handling lawful, fair, and transparent.(Hoofnagle et al. 2019) The crux of such requirements involves principles of lawfulness, purpose limitation, data minimization, accuracy, storage limitation, integrity, and confidentiality. Businesses must extend their operations in compliance with such principles.

Therefore, any processing of personal data must have the free and informed consent of the individuals to whom the data pertains, as per the principle of lawful processing. Additionally, the processing must have a legal basis in at least one of the exceptions allowed by the law, such as consent or a legitimate interest. Additionally, the business should make sure that the data is collected for clear, defined, and lawful purposes and that any further processing aligns with these original goals (Hoofnagle et al. 2019) . Organizations should also not demand more information than may be required for the fulfillment of the pre-defined purpose. One of the other major responsibilities regards accuracy: a business will have an obligation to make the necessary corrections without any further delay. Equally, personal data must not be retained longer than was originally intended, and retention periods should be developed by a business subject with a view to further ensuring compliance with the storage limitation principle. Lastly, appropriate technical and organizational measures shall be developed to protect such personal data against unauthorized access, loss, or damage of personal data. Overall, these obligations are a sea-change in the way businesses have to treat any personal info with a full review and revision of existing data practices.(Hoofnagle et al. 2019)

i) **Breach Notification-** According to the GDPR, unless the breach is unlikely to jeopardise the rights and liberties of natural persons, an organisation must notify the appropriate supervisory body of a breach of personal data within 72 hours of learning about it. The type of breach, the categories and approximate number of impacted individuals, and the potential repercussions should all be covered in such a statement. An organization must also notify the individuals involved of the breach if it is likely to provide a significant risk to their rights and freedoms, noting. (Bakare et al. 2024)

Because violating these regulations has serious penalties and other legal ramifications, it is critical that an organisation implement effective procedures for breach detection, investigation, and notification. The GDPR's overarching goal of encouraging increased accountability and openness in data processing activities includes this component. (Heavin & Power 2019)

ii) Appointment of the data protection officer (DPO)- The GDPR stipulates that an organization has to designate a DPO in order to ensure compliance with the regulation and be a focal point of contact for the organization, data subjects, and supervisory authorities. This is notably required for the public authorities or bodies, but also for those private entities whose core activities consist either of processing on a large scale that forms part of a system of regular and systematic observation, or the processing of sensitive personal data.

In essence, core activities of the DPO are to monitor compliance of an organization with GDPR, advise on issues related to data protection impact assessments, and liaise with supervisory authorities in cases of audits or investigations. Most importantly, the DPO has to act independently and avoid conflicts of interest and is required to report to the highest management level within an organization. Because the role of DPO ensures accountability and transparency in the handling of personal data, this in essence ensures that the overall framework of GDPR is reinforced when it comes to protection of personal privacy rights. (Bryce, Lang, and Nagaroor 2024).

In addition, any organization that should designate a DPO should also ensure that the latter be well-endowed in terms of resources and access to all processing activities involving personal data, such that these would enable the proper performance of their duties. In this regard, this position also enunciates the proactive measure for data protection in relation to compliance with the increasingly dynamic landscape of privacy laws. (Cao and Kretschmer 2024)

iii) Cross-Border Data Transfers - Under the GDPR, organizations transferring personal data outside the European Union are obliged to ensure such personal data has adequate protection. This applies with respect to a transfer within a corporate group or to third-party organizations in those countries that do not have equivalent laws on protection of data. To make such transfers, organizations may use certain mechanisms provided for by GDPR, which include the Standard Contractual Clauses (SCCs) and Binding Corporate Rules.

SCCs are preapproved contractual terms that need to be inserted into the contracts between data exporter-located within the European Union-and data importer-who will be outside of the EU. The clauses provide an assurance that the transferred data is protected to a standard required by the GDPR.

Meanwhile, Binding Corporate Rules (BCRs) are internal rules adopted by multinational corporations to allow intra-group international transfers of personal data to entities outside the EU. Both mechanisms aim to ensure that individuals' data rights are respected, even when their personal data leaves the EU.

Organizations must carefully assess the legal basis for such transfers and, in the absence of an adequacy decision (i.e., when the destination country does not offer equivalent data protection), these mechanisms become essential to compliance with GDPR.(Cao and Kretschmer 2024) (Ullagaddi 2024)

iv) Privacy by Design and by Default- The basis for any legislation on data protection, and most strongly reaffirmed by GDPR, is privacy by design and by default. This means it should be implemented right at the beginning in processing activities and business practices of organizations. Inherently, taking proactive measures evokes considerations about privacy in system design and operations.

The basic framework enshrined into GDPR is Privacy by Design and Default, setting the core requirement for data controllers and processors. Pursuant to the regulation, appropriate technical and organizational measures shall be observed from the outset so that the processing will meet the principles of data protection and the protection of the rights of the data subject.(Prasad and Pérez 2020), (Cao and Kretschmer 2024) This means designing systems that are secure, holding less personal data than necessary, and only processing data for the intended purpose.

v) Compliance challenges- Whether an organization is big or small, today's data-driven landscape sees most wrestling with the complexities and ambiguities thrown up by the European Union's General Data Protection Regulation. Designed with a view to protecting the privacy and personal data of all EU citizens, the GDPR encompasses a wide range of compliance requirements-many of which, up until now, have been incomprehensible and hard for many businesses to implement.(Chander et al., 2023).

vi) Complexity and Ambiguity of Regulations- The GDPR has a wide framework aimed at enhancing the protection of data and privacy, but its complication has caused organizations to fumble with ways of complying with it. Most businesses find the ambiguous and complex nature of some of its provisions, especially when considering the extent of applicability.

While the GDPR does, for example, provide for a number of detailed requirements concerning valid consent, data protection impact assessments, and protocols for cross-border data transfer, what in practice amounts to "adequate protection" or "appropriate safeguards" is usually left open

and thus sometimes quite tricky to determine precisely what an organization needs to do to satisfy such requirements.(Hoofnagle, van der Sloot, and Zuiderveen Borgesius 2019)

Because the regulation is so convoluted, there can be ambiguity on certain requirements for compliance, particularly in instances of an organization balancing obligations that are sometimes in conflict with one another, such as data protection and business continuity. (Voigt and Von dem Bussche 2017)The outcome may involve accidental noncompliance, increasing the likelihood of a fine.

In today's data-driven landscape, organizations of all sizes are grappling with the complexities and ambiguities of the European Union's General Data Protection Regulation. The GDPR, aimed at protecting the privacy and personal data of EU citizens, has introduced a multitude of compliance requirements that have proven challenging for many businesses to fully comprehend and implement.(Smith 2019)

vii) Lack of Resources and Expertise- The lack of resources and skills inside organisations to properly implement GDPR compliance has been recognised as a widespread concern in a number of studies. Due to inadequate training and a lack of awareness of the intricate legal and technical requirements of data privacy legislation, many organizations—especially smaller ones—face serious difficulties.Companies often struggle to dedicate enough personnel and technical resources to compliance efforts. (Presthus and Sønslien 2021) As highlighted in many cases, GDPR violations stem from human error, poor training, and a general lack of competence regarding data protection obligations. The enforcement practices vary widely across European Union countries due to disparities in the resources available to national data protection authorities. (Ruohonen and Hjerppe 2022) This resource gap exacerbates compliance challenges, particularly in terms of enforcing GDPR obligations at a local level.

For example, most organizations report not investing in any training programs on the education of employees with regards to requirements set by GDPR. In turn, this lack of proper expertise negatively impacts their ability to implement adequate policies that could ensure efficient data protection, thus being exposed to violations and possible fines. (ICO 2021)

viii) Unsatisfactory technical and organizational measures - Most organizations are incurring heavy fines because of non-compliance with GDPR as a result of failure to implement security measures for their data technically and organizationally. According to different studies, insufficient information security protocols have already caused various data breaches. Such flaws often emerge because of weak IT infrastructure and poor data protection that paves the way for unauthorized access to sensitive information.

Moreover, Proceedings on Privacy Enhancing Technologies (Saemann et al. 2022) add that incapacity to apply security controls, including encryption or pseudonymization of personal data, may result in severe fines and loss of reputation for an organization. The realization of appropriate security frameworks is hence core for organizations in the process of mitigating the risks of non-compliance.

ix) Non-Exercise of Data Subject Rights - One of the core challenges that organizations grapple with in their journey to GDPR compliance is the failure to act on data subject rights, such as the right to erasure and the right to access personal data. (Presthus and Sønslien 2021) . Organizations often do not meet the requirements concerning data subject rights; this has resulted in many complaints and enforcement actions from data protection authorities. These often lead to heavy fines because the inability to respond to the requests of data subjects infringes key provisions of the GDPR, which were actually intended to give control over personal data to the individual subjects.(ICO, 2021)

x) Insufficient Data Processing Agreements - Many organizations fail to establish valid data processing agreements with their data processors, a key requirement under the GDPR (Voigt & von dem Bussche, 2017). The regulation mandates that organizations must have a written data processing agreement, which includes specific mandatory provisions such as the relationship between the data controller and processor and the exact manner in which personal data is processed to comply with GDPR requirements (Kuner et al., 2020). Failure to secure these agreements can lead to significant compliance risks, exposing organizations to penalties and fines (European Data Protection Board, 2021).

xi) Challenges with International Data Transfers - International data transfer can be described as one of the major challenges seen in the enforcement of GDPR. (Tzanou, 2015) An explanation as to how the extra-territorial enforcement of GDPR makes it really complicated when personal data is transmitted to jurisdictions outside the EU, especially since the data protection laws of those countries will be perceived as lesser in stringency than what is contained in GDPR.

Organizations are required to implement various tools to facilitate lawful data transfer, such as SCCs or BCRs. However, specific local regulations and implementation challenges often complicate compliance. This therefore means that the companies will have a big compliance burden because transfers between the EU and other regions may expose the companies to certain risks and penalties in case proper safeguards are not enacted. (Voigt and Von dem Bussche 2017)

xii) Non-Uniform Application across EC Member States - One of the biggest concerns that have reiterated on a number of occasions for every organization operating across multiple jurisdictions is discrepancies in enforcement levels across EU member states. Its inconsistent enforcement just fragmented the regime and therefore made it even more difficult for big multinational organizations to enforce such fragmented regime compliance. The enforcement authorities of different countries will apply and interpret the various provisions of GDPR differently, which results in variance in penalties and requirements for compliance with the GDPR.(Taylor & Kent 2017) This lack of harmonization results in confusion on the part of organizations, since they have to be cognizant of and comply with the particular regulatory nuances applicable in each jurisdiction. This condition complicates their compliance efforts even more.

xiii) High Cost of Compliance - The costs of GDPR compliance may be unaffordable, especially by SMEs. Many organizations have to deal with increased costs of consulting and administrative burdens in their attempt to show compliance with GDPR (Abdulah and Aseri 2020). Such a wide span of requirements, from data protection impact assessments and employment of Data Protection Officer to implementing appropriate security of data, often pose resource-intensive tasks. For SMEs, these costs may turn into a significant barrier since GDPR compliance may become an expensive burden. (Abdulah and Aseri 2020)

xiv) Public awareness and Understanding - Public awareness and awareness of the rights and obligations ensuing from the GDPR remain an issue. Most individuals seem to be at sea regarding their rights over protection, such as the right to access, rectification, and erasure of data (Ruohonen and Hjerppe 2021) This partial knowledge makes it difficult to assert the rights on maximum implementation by organizations and also leads organizations not to feel obligated enough for the application of all provisions of the GDPR due to a lack of public awareness, hence an increased risk of violations.

xv)Technological Challenges - The implication is serious tests for organizations in trying to comply with GDPR. New technologies, such as Artificial Intelligence, Blockchain, and Big Data Analytics, are evolving and further complicate the task of offering personal data protection according to the requirements of the GDPR, (Tzanou, 2015) thus forcing organizations to adjust their compliance strategies to new innovation continuously-often leading to a reconsideration of the measures adopted regarding data protection so that they meet the stricter demands laid out by the regulation. The evolution of technology is ongoing and such that even systems complying with the requirements may get obsolete over time, and vigilance, updates in data protection practices are required to be carried out on a continuous basis.

b) Initial and Ongoing Costs

i) Implementation Costs - The estimated cost of implementation by Fortune 500 companies for GDPR compliance is in the region of $16 million on average. This huge cost suggests how heavy a burden these large organizations should bear, with immense resources required to comply with the stringent data protection requirements imposed by this regulation. (Lynskey, 2022)

One estimate from a single survey was that 58% of the companies believed the cost of their GDPR-related projects to fall within a range of € 50,000 to € 250,000, while costs for compliance, auditing processes and updating technologies for data protection represent highly resource-intensive and expensive investments in compliance with the GDPR. (Reeves 2020)

ii) Cost of Annual Compliance - Annual compliance cost estimates vary significantly based upon the size and industry of an organization. Large organizations, such as Fortune 500 companies, are estimated to be spending an average of approximately $16 million annually. (Chander et al. 2021) Some industries have an even higher financial burden. Banks face annual compliance costs up to $84 million, and technology firms are expected to pay about $26 million annually to become compliant with the GDPR. These high figures underline the considerable investment needed to attain total compliance, especially for industries whose operations are basically hinged on the protection and processing of personal data.(Chander et al. 2021) SMEs, even though the costs may not go into millions, they do come as a considerably high financial burden. A lot of SMEs estimate that the cost of compliance with GDPR annually runs into the range of €50,000 to €250,000 per year, of which a lion's share may be devoted to external consultants, legal advice, investments in technology, and training of staff. These costs can be disproportionately burdensome for smaller businesses, many of which lack on-staff expertise or infrastructure to handle compliance efficiently. Accordingly, the majority of SMEs are depending on third-party services to help them through the intricacies with GDPR, thereby depressing the financial burden. (Demirer et al. 2024)

Apart from direct costs, there are indirect costs: the loss of productivity and opportunity costs from diverting employees from their normal duties to manage activities of compliance. Additionally, non-compliance with GDPR by firms attracts fines up to a level of €20 million or 4% of annual global revenue, whichever is greater, thus considerably raising the financial risk for possible non-compliance.(Smith, 2019)

iii) Labor Costs - Estimates of labor costs vary between 20% to 50% of the GDPR compliance cost, covering dedicated resources in privacy compliance and training of existing personnel. Compliance often requires specialized resources, such as DPOs and legal advisors-especially in larger organizations-to ensure that data protection measures will meet the complex requirements of the regulation. On smaller organizations where hiring is not possible or cost-effective, the task will typically fall to current personnel, in which case intensive training will be required to bring them up to date on GDPR regulations (Chander et al. 2021).

Apart from direct labor, organizations incur the cost of indirect labor as well. The opportunity cost is there for employees who are burdened with taking care of GDPR compliance assignments and duties because their time and acumen are being utilized in compliance activities rather than core business functions themselves. This leads to productivity loss, besides affecting the operational efficiency of the organization.(Demirer et al. 2024) Moreover, various training programs that are required regularly so that people can be aware of the changing landscape of privacy laws add to compliance-related labor costs.

iv) Technology and Infrastructure - Companies are required to invest in new technologies, revise policy statements regarding privacy, and audit flows for the processing of data in order to make them GDPR-compliant.(Prasad and Pérez 2020) Technological investments are usually massive investments since they involve creating mechanisms for safekeeping and storing data, mechanisms for encryption, and one for continuous monitoring. Such efforts are necessary to make the processes of data processing GDPR-compliant and any eventual breaches of data minimal.

Technology-related costs in the compliance process of GDPR are usually in the range of 12-17% of all compliance costs (Chander et al. 2021). Such examples include IT infrastructure improvement, audit flow testing, and privacy-enhancing technologies addition to systems. Changes of this nature are essentially due to the stringency of provisions for security in the GDPR under conditions of no unauthorized access or use of personal information .

v) Professional Services and Legal Fees - A significant share of GDPR compliance costs goes toward services that include consultancy and legal fees, on average at about 19% to 24% of total compliance spending. Many organizations use third-party consultants to understand the intricacies of GDPR and to assist in making their data processing operations compliant with the various stringent requirements of the regulation. This dependence has resulted in a very active market for the provision of consultancy services related to GDPR. (Chander et al. 2021)

The fear of non-compliance coupled with its associated extraordinarily high fines leads many companies to seek out lawyer consults and specialized compliance guidance to a great degree, thereby driving up costs. This is certainly true for larger organizations where the volume of their data processing activities requires frequent consultation and legal review during the course of ongoing operations.(Lynskey, 2022)

vi) Training and Awareness - Training for GDPR compliance can also be very different in cost, depending on the nature of the organization. Many companies resort to formal external training whereas others prefer informal internal training programs. "The organizations which have invested in more formal types of training programs are generally showing better compliance results, but it is truly an expensive venture for any small-scale and medium-scale organization". (Reeves 2020)

A lack of sufficient training also creates significant vulnerabilities. Lack of awareness and ineffective training programs are often among the leading causes of heightened vulnerability regarding data breaches. Without proper knowledge in respect of data protection obligations, employees may reveal sensitive information that could lead to critical financial and reputational harm for an organization. (Voigt and Von dem Bussche 2017)

vii) Operational Changes - This is also forcing organizations to change their way of consuming data, at an increased operational cost for gaining GDPR compliance. For instance, compliance with design principles-like data minimization and purpose limitation-strictly requires a company to revisit and redesign flows of data processing, which is not only time-consuming but costly changes that make marketing and data management strategies more complex, too, especially for companies whose businesses rely on large-scale data processing for personalized marketing efforts. (Prasad and Pérez 2020) Compliance with GDPR often requires businesses to collect and store less data, which in turn reduces their big data analytical capability to engage in targeted advertising and gain deep customer insights .

viii) Market Impact - GDPR has brought very significant market impacts, especially on venture capital investment and the effectiveness of online advertising. According to numerous studies, strict data protection regulations drove venture capitalists away from investing in some tech startups, especially those in which the collection and processing of data have been an essential part of their core functions. This decrease in investments is largely attributed to increased compliance costs and the fear of fines due to possible breaches of GDPR. (Campbell et al. 2020)

GDPR also negatively impacts the effectiveness of online advertising. It limits the ability of organizations to collect and utilize personal data in operating targeted promotional campaigns. In

exchange, many organizations refer to the worsening in ad performances as well as revenue losses that must be encountered due to the use of more restrictive data gathering methods (Campbell et al. 2020)

ix) Insurance Costs - With the arrival of a GDPRrelated insurance market, it brought along additional expenses for organizations willing to hedge against different kinds of risks related to data breaches. Most organizations purchase cyber insurance policies for paying fines, legal expenses, and all other liabilities arising due to GDPR infringement. One study showed that 31% of the organizations surveyed had purchased insurance covering cyber risks and that 43% of those policies explicitly covered GDPR fines and penalties. This trend doubtless reflects greater awareness of the financial risks from GDPR non-compliance, particularly for those organizations processing volumes of personal data.(Lintvedt 2022)

c) Consumer Right

i) Data Subject Rights under the General Data Protection Regulation (GDPR) - The General Data Protection Regulation (GDPR) establishes the rights of data subjects to empower individuals with greater control over their personal data (Voigt & von dem Bussche, 2017). Organizations are required to adapt their practices to comply with these regulations and ensure adequate safeguards for data protection.

ii) Right of Access (Article 15) - The Right of access allows people with the option to give consent to the data controller to process their data, by giving consent consumers may also request controller to access their data and may also get supplementary information from the controller- like purpose of data processing, what kind of personal data is involved and if any third party is involved in the data processing. This ensures transparency.(Spalević and Vićentijević 2021) (Cao and Kretschmer 2024)

iii) Right to Rectification (Article 16) - The right to rectify makes sure that the data subjects have the option to request for corrections of inaccurate or incomplete personal data that is stored by the organization. This also ensures that personal data remains reliable. Organizations must update their record upon the request of any individual. (Spalević and Vićentijević 2021) (Cao and Kretschmer 2024)

iv) Right to Erasure (Right to be Forgotten) (Article 17) -The Right to erasure, is also referenced as the right to be forgotten. This ensures people are able to request deletion of their personal data that they had previously given consent to store. This can be done under any circumstances. (Spalević and Vićentijević 2021) (Cao and Kretschmer 2024)

v) Right to Restrict Processing (Article 18) - Under right to restrict processing the data subjects can ask to limit the use of their personal data, data that is processed under specific conditions. This can be exercised in situations where the accuracy of the data is questioned or the data processing is unlawful or the organization no longer needs to process data but the individual needs it for legal claim, during the restriction period organizations can store the data but not process it. (Spalević and Vićentijević 2021) (Cao and Kretschmer 2024)

vi) Right to Data Portability (Article 20) - The rights to data portability ensures people to recivie their data in a structured, commonly used and machine readable format. This right also allows individuals to transfer their data to another controllers. It applies to data processing by automated means, The processing is based on consent or the performance of the contract. This is to make sure that individuals can switch between service providers without losing the control of their data. (Spalević and Vićentijević 2021) (Cao and Kretschmer 2024)

vii) Right to Object to Processing (Article 21) - The Right to Object allows individuals to object to the processing of their personal data under certain conditions. This includes cases where the data is processed for direct marketing purposes or based on legitimate interests. Organizations must cease processing the data unless they can demonstrate compelling legitimate grounds that override the individual's rights and freedoms, or if the data is required for legal claims. (Spalević and Vićentijević 2021) (Cao and Kretschmer 2024). Together, these rights reflect the GDPR's emphasis on protecting individuals' privacy and granting them autonomy over their personal data. Organizations are required to not only comply with these rights but also implement processes to facilitate their exercise in a timely and efficient manner. Failure to respect these rights may result in regulatory penalties and significant reputational damage.

viii) Consumer Enhanced Rights - The GDPR more than ever before strengthens consumer rights over their personal information. The rights to access, rectify, erase, and port data of consumers are now legally binding; similarly, this includes the right to object to data processing and automated decision-making. These enhanced data protection rights will enable individuals to have more control over how their personal data is collected and used. For instance, persons, can now have a copy of their data at any time and corrections of errors done within 30 days. Additionally, the right to be forgotten ensures that consumers have their information erased when no longer required for the original intention. (Presthus and Sørum 2019)

ix) Increased Transparency - Institutions operating under the GDPR are expected to give data concerning personal data gathering, use, and distribution in a more transparent state. The emphasis on transparency has in mind empowering individuals to make informed decisions with regard to their personal data. Ensuring an individual can clearly understand what data is used,

why that particular data is being processed, and with whom the data is shared are all aspects of the GDPR aimed at trust in the commercial-consumer relationship. Transparency makes not only the consumer more aware, but it also holds the organizations accountable, since they have to be transparent about their data practices in a way that is easily comprehensible to the public. (Wong and Henderson 2019)

x) Privacy Paradox - While consumers frequently raise concerns about their privacy, a majority do not actually act on it by taking measures to protect their personal data. In simple words, the privacy paradox is a situation of incongruence between the attitude and behavior of the consumers. For instance, while consumers claim that they value data privacy, they end up releasing their information for the sake of convenience or perceived benefits such as discounts or quick services. The privacy paradox suggests that even though people are aware of risks to privacy, their behaviors often do not align with the stated preferences. (Presthus and Sørum 2019)

xi) Implications for Marketing Practices - The General Data Protection Regulation has caused many marketers to question their strategy, in particular with the more stringent consent that now applies. Marketers have to obtain explicit consent from consumers for the processing of personal information for marketing purposes. This has forced companies to be much more transparent about the collection of data and to spell out how they plan to use consumer data.

This new regulatory layout limits businesses in that they cannot operate on a passive collection of data via pre-checked boxes or implicit consent; instead, they must interactively address consumers so that clear and informed consent is given freely. This has also presented further challenges to the marketing strategies which have hitherto relied heavily on large volumes of consumer data for targeted advertising(Wong and Henderson 2019).

xii) Consumer Trust - In today's data-driven world, consumer trust is something one will see in the way organizations handle personal information. The General Data Protection Regulation, was one such radical legislation that came forward to do its part in making consumers confident in how organizations handle personal data and help them create this very sense of trust in the handling of data. Research could also indicate that there are more active and interested consumers in companies that demonstrate a strong commitment to protection of their data, showing positive consumer behaviors from the impact of such regulations.(Nissenbaum, 2021)

xiii) Compliance Issues - While consumer rights have been increased, the compliance with the GDPR became for a majority of companies a nightmare due to the inherent complexity of it. In any case, compliance with the GDPR's strict data protection is very resource- and time-

consuming hence operationally problematic. Comprehensive compliance is impossible for companies, and especially smaller businesses; therefore, they are sometimes unable to protect consumers. These compliance challenges can also have a deteriorating impact on the quality of services that will be offered to clients, given that organizations are likely to shift resources from other areas of organization towards ensuring data protection compliance (Wong and Henderson 2019)

xiv) Global Impact - The GDPR has also had an extensive and significant global impact. This has been manifested in its inspiring the development of other similar data protection laws across the world. It has implications for businesses operating outside of the EU, since any company that deals with EU citizens has to maintain GDPR standards. This, in turn, has influenced many nations in other parts of the world to improve their data protection standards, thus providing even more consumers with stronger data protection standards. In such a way, GDPR remains the standard of consumer rights and data privacy to which most of the world adheres. (Consumer Rights to Personal Data n.d.)

xv) Consumer Engagement - The General Data Protection Regulation encourages consumers to become more proactive in relation to their rights in regards to personal information, such as the right to access, rectify, and erase personal information. However, despite this improved legal framework, it's unsure just how many of the consumers know about these rights and are able and willing to exercise them. This suggests that many people are unaware, or even fearful, and require further education in personal data management to feel truly empowered, and hence, meaningful milestones as far as consumer empowerment is concerned are a few and far between. (Presthus and Sørum 2024)

xvi) Economic Implications - The economic implications of compliance with GDPR could amount to increased costs for companies. Companies would need to invest in technology, personnel, and lawyers to be entirely compliant with the regulation. **These costs may be transferred to the consumers in due course, thus resulting in higher prices.** However, over a longer run, the potential benefits accruing from improved data security and increased trust by the consumers might outweigh these costs. By being in a position to deal with personal data in a secure manner and in a more transparent way, companies will be able to develop closer ties with consumers, whereby they will gain a greater degree of trust and long-term benefits, irrespective of the initial burden in financial terms. (Presthus and Sørum 2024)

d) GDPR's Influence on Technology and Innovation

i) Market Dynamics and Competition - There has been an identification of the General Data Protection Regulation's role in increasing the market position of large online platforms and further increasing the concentration of markets. In essence, smaller firms just can't compete because compliance is expensive and data management is burdensome. This may negatively affect innovation because, for instance, small players might not easily enter the market nor develop innovative solutions. Larger platforms are in turn better positioned to absorb these compliance costs because of more resources, thus increasing the competitive gap and further consolidating their market position. (Geradin, Karanikioti, and Katsifis 2020)

ii) Encouragement of Privacy-Preserving Technologies - GDPR catalyzed the development of privacy-preserving technologies, such as differential privacy and federated learning. These technologies support organizations in adhering to this regulation while at the same time fostering more user trust and user engagement. For example, companies already on the forefront of privacy techniques also report a significant increase in user trust, which could translate to a competitive advantage(Martin and Murphy 2020). By focusing on privacy-first innovation, an organization attains not only compliance but also thought leadership in consumer data protection.

iii) Impact on Data Sharing and Open Innovation - GDPR meaningfully influences data-sharing practices, which are vital in industries like healthcare and e-commerce, since they create innovations based on data insights. While GDPR targets personal data protection, the stringent demands it makes regarding data handling minimize any disruptive impact of open innovation. In particular, the regulation requires treading with caution through data-sharing activities that can assure compliance, often slowing down the tempo of efforts in innovation, especially for those organizations that rely heavily on personal data in their processes of research and development (Doe et al. 2024)

Therefore, there is a need to strike a balance between regulatory requirements and the urge for data-driven innovation in such companies, so they can sustain compliance with fostered new technologies and business models.(Doe et al. 2024)

iv) Innovation in Data Management Practices - Organizations feel that they definitely have to go for better data management practices to keep up with GDPR requirements, such as modernization of IT infrastructures, ensuring data integrity, and proper implementation of a robust framework in data governance. This will instill a sense of responsibility and accountability within a company regarding data protection. Often, these enhancements bring gains in operational

efficiency, improved ways of handling data, and create competitive advantage by engendering consumer trust in compliance. (Haddara, Salazar, and Langseth 2023)

v) Regulatory Uncertainty - The uncertainty of compliance with GDPR mostly causes problems, especially for startups and companies working on emerging technologies. Most of them are at a loss about how their innovative products fit within the rigid data protection requirements of GDPR; most times, this delays product development and market entry.(Binns 2019) In effect, this could choke creativity and innovation in the fast-changing technology industry where speed to market is critical to success. Given the intricacy of the regulatory environment, the risk of sanctions in case of non-compliance seriously postpones innovation and new business model development. (Jia and Wagman 2020)

vi) Long-Term Benefits of Compliance - Though it might have started off with shaky ground, compliance with the GDPR is sure to have numerous long-term benefits accruing to organizations. The European Parliamentary Research Service indicates that compliance with GDPR brings an atmosphere of transparency, accountability, and ethics when handling data. This will significantly contribute to organizational reputation and will create closer, trust-based relationships with customers. Furthermore, this compliance opens the door to responsible innovation, especially in terms of embedding the principles of data protection into technological developments, including artificial intelligence. (European Union 2020)

e) Comparative Analysis of GDPR and Other Regulation

i) United States - Unlike the comprehensive GDPR of the European Union, the United States has no single overarching federal data protection law. Instead, data privacy is subject to a variety of different sectoral laws, which makes the landscape of regulations very fragmented. For example, health information falls under HIPAA, whereas consumer data in California is covered under the newly implemented California Consumer Privacy Act, starting in 2020 (Bakare et al. 2024). While the CCPA granted California residents clear rights of access, deletion, and limitation on sharing of their personal information, it was nevertheless narrower in scope compared to the wide-ranging, rights-based framework for the GDPR. Organisations operating across jurisdictions face significant hurdles trying to comply with conflicting sectoral and regional requirements.(Bakare et al. 2024)

Difference - The GDPR and CCPA are quite different in terms of their data protection modalities. One point of divergence between these two laws relates to the nature of consent: whereas the GDPR relies upon explicit consent to process data-meaning, individuals must actually opt-in to the collection and processing of their information-the CCPA follows an opt-out model wherein

consumers can request that their information not be sold, without explicit consent before collection being necessary (Schwartz 2021). Moreover, the GDPR provides full individual rights-for example, the "right to be forgotten" and data portability-which individuals own regarding their personal data. While in most U.S. laws, these individual rights are limited or nonexistent.(Bakare et al. 2024)

The enforcement mechanisms also vary greatly. The GDPR relies on a central supervisory authority to provide uniform supervision over the EU member states and, thus, allows for coordinated enforcement efforts. This is in contrast to the U.S., where regulation of data is fragmented among various regulatory entities, each with different spheres of influence and powers to enforce, sometimes resulting in inconsistencies in the application of regulations and compliance requirements.(Bakare et al. 2024)

ii) India - The Indian approach towards Data protection, as represented by the Personal Data Protection Bill or PDPB, draws immense influence from the GDPR in its aspiration to establish a complete data protection framework. This legislative move was made possible with great force after the landmark judgment of the Indian Supreme Court where the Hon'ble Supreme Court decided in the case of Puttaswamy that 'Privacy is a Fundamental Right' and hence called for rigid data protection laws.(Puttaswamy v. Union of India 2017) Just like the GDPR, the PDPB too has a very strong focus on making sure personal data is indeed processed in a transparent manner, with accountability, and based on user consent. This is an important step toward bringing India's data protection standards closer to current global practices, not to mention those of the European Union.

Difference - The cardinal principles for GDRP and PDPB in India are reliant on user consent and the protection of rights of any single individual. Both regimes granted rights to an individual for access, correction, and rectification of personal data. In this regard, the concept and focus for both remain user empowerment and data autonomy, respectively.(Shah 2021) However, there are certain notable ways that the PDPB is taking major divergences from the GDPR. It has a broader definition of personal data, and it introduces criminal sentences for some of the violations. This is not something under the GDPR in its current form, considering that the GDPR is going to use administrative fines to a great degree as a means to ensure enforcement.

Also, the GDPR has rigorous explicit consent for most forms of data processing, while PDPB is flexible on data processing without consent in some scenarios-for example, state functions and emergencies. This, therefore, shows that the approach adopted by India is to fit data protection principles into the legal and economic context, while sustaining core similarities with the GDPR focus on user rights and accountability. (Shah 2021)

iii) China - China's data protection structure is primarily shaped by the Cybersecurity Law, which outlines basic standards for data handling, security, and cross-border data transfers. Complementing this is the anticipated Personal Information Protection Law (PIPL), a regulation designed to align more closely with GDPR principles by strengthening individual rights and setting stricter consent requirements for data processing (Alic 2021).

Differences- While GDPR prioritizes individual rights and explicit consent for data processing, China's framework emphasizes state interests, allowing for considerable government access to personal data under specific circumstances. The PIPL introduces enhanced consent requirements and individual rights, such as the right to access and correct personal data. However, its enforcement may diverge from the GDPR's supervisory authorities approach, as it aligns enforcement more closely with government agencies, reflecting China's centralized regulatory style (Alic 2021).

iv) Thailand - Thailand's Personal Data Protection Act (PDPA), enacted in 2019, mirrors many aspects of the GDPR, aiming to secure personal data while accommodating business needs. Both the GDPR and the PDPA mandate consent for data processing and uphold data subject rights, such as access and rectification of personal data. Furthermore, like the GDPR, the PDPA includes data breach notification requirements, though it is tailored to the Thai regulatory environment, with distinctions in enforcement mechanisms and penalties. (Jitkarunawong n.d.)

Difference - Both the GDPR and PDPA focus on consent and individual rights, fostering transparency and user control. However, the enforcement structures vary. The GDPR employs a centralized supervisory authority across EU member states, while Thailand's PDPA delegates enforcement primarily to domestic agencies with different approaches to penalties. Additionally, while the GDPR includes uniform punitive fines across the EU, Thailand's PDPA may implement a more discretionary penalty structure that aligns with local business practices and judicial oversight (Jitkarunawong n.d.)

v) United Kingdom - Following Brexit, the UK established a data protection framework that remains aligned with GDPR principles but includes targeted amendments. With the Data Protection and Digital Information Bill 2(DPDI2), the UK aims to streamline compliance, reduce burdens on businesses, and foster innovation, while preserving a baseline of GDPR-aligned standards. (Sorrell 2023)

Difference - While the GDPR prioritizes individual rights and a uniform regulatory approach, UK amendments under the DPDI2 may relax certain compliance requirements, raising concerns about a potential reduction in data protection standards. For instance, the DPDI2 introduces more

flexibility in legitimate interest assessments and data processing requirements, granting the UK government the flexibility to diverge as needed in the future. (Sorrell 2023)

vi) East African Community - The East African Community (EAC) is developing data protection laws influenced by GDPR standards to support regional data governance consistency. This harmonized approach aims to facilitate cross-border data flow and streamline compliance across EAC member states. While principles like consent, individual data rights, and transparency mirror GDPR elements, the EAC faces unique challenges, such as limited regulatory infrastructure and varying levels of enforcement across nations.(Jones & Smith, 2024)

Difference - The GDPR's "one-stop-shop" mechanism, designed to allow coordinated action through a lead supervisory authority, serves as a potential model for the EAC. This mechanism, if implemented, would allow businesses operating across EAC countries to work through a single regulatory point, fostering compliance simplicity. However, differences in legal frameworks and administrative capacity present challenges, and achieving consistent enforcement across member states remains a work in progress (Jones & Smith, 2024)

vii) Australia - Structuring the Australian data protection framework is the Privacy Act 1988, with the government agency operated under principles known as the Australian Privacy Principles. These lay down standards on collection, use, and disclosure of personal information by government agencies and private organizations, focusing on ensuring transparency, consent, and individual rights over personal data. (Arachchige Sarathchandra 2018)

The Australian Privacy Act and GDPR are both grounded on the same tenets of transparency, consent, and rights protection in respect to personal information. Both point out protection policies that would provide confidence and accountability among handlers of information and emphasize the informed consent principles about the collection and sharing of personal data. (OAIC 2021)

Difference - While the GDPR is comprehensive with serious prerequisites and more serious penalties, Like €20 million or 4% of the global annual turnover of an enterprise-Australia's regime imposes less serious penalties. It also provides data subjects with rights under the GDPR, including the "right to be forgotten," a provision entitling individuals in certain circumstances to request erasure of their personal data. This is not explicitly set out within the Australian Privacy Principles.(Arachchige Sarathchandra 2018)

viii) Canada - The data protection policy environment in Canada is to a great extent shaped by the Personal Information Protection and Electronic Documents Act, a legislation that regulates data practices for private sector organizations. PIPEDA sets standards on collection, use, and

disclosure of personal information, consent, and responsible data management practices (Arachchige Sarathchandra 2018)

Similarities are rampant in that both PIPEDA and the GDPR place high stock in the principles of consent, individual rights, and accountability during data processing. This also implies that the individuals have control over their personal information, while the organization takes responsibility for applying data practices transparently.

Difference - It differs on the basis that GDPR has a wider scope and is more comprehensive because it applies to all entities processing information of EU residents irrespective of the geographical location. PIPEDA, on the other hand, has sectoral exemptions and primarily applies to Canada's private sector. More significantly, GDPR has more strict penalties against non-compliances with fines rising to a maximum of €20 million or 4% of global turnover. Canadian laws, on the other hand, impose rather limited penalties. (Arachchige Sarathchandra 2018)

ix) South Asian Countries - Countries like India, Pakistan and Bangladesh are well on their way to all-rounded data protection laws inspired by the GDPR. These countries have been bringing on board mechanisms aimed at protecting personal data, consent, and rights of persons, thus bringing their policies closer to global standards. Many of the data protection initiatives in South Asia are informed by principles set out under GDPR, which include rights to access and rectification of personal data, and the requirement for consent prior to processing. This might be indicative of an adherence to international standards around data privacy. (Bentotahewa, Hewage, and Williams 2022)

Differences - Enforcement and regulatory mechanisms in South Asia are still relatively underdeveloped as compared to GDPR. In this regard, the Indian Draft Personal Data Protection Bill, although vastly based upon the principles of GDPR, lacks comprehensive enforcement and penalty mechanisms of GDPR which may make a dent on its effectiveness in protecting data privacy across industries, thus the Draft itself being redundant. (Bentotahewa, Hewage, and Williams 2022)

x) United Arab Emirates UAE - The data protection framework of the UAE is mostly anchored on Federal Decree No. 45 of 2021 on the Protection of Personal Data (UAE Ministry of Justice n.d.). The Act stipulates a set of principles similar to those accorded by the GDPR, revolving around transparency, purpose limitation, and the rights of individuals. The UAE's framework has thus created a backyard of personal data security standards that deal with both private and public sector practices in data handling with consideration to the regional context. UAE law follows basic GDPR principles, such as transparency of processing, limitation of purposes to ensure that use of

data only proceeds in specified, explicit purposes, and individual rights for the protection of user autonomy regarding personal data. (Sethu 2020)

Differences - Despite these similarities, the UAE framework has enforcement and penalty provisions that are distinct from the GDPR. The UAE approach especially has accommodations for the local context in place, which can allow regulatory enforcement flexibility that would be more lenient compared to comprehensive enforcement mechanisms and severe penalties for non-compliance under the GDPR-for instance, up to €20 million or 4% of global turnover (Sethu 2020)

4. Results

4.1 Results of Data Analysis and Development Proposals

The review of existing literature on GDPR is complemented by insights from interviews with experts in the field on various crucial findings and areas for development in the advancement of GDPR compliance frameworks. These gaps include those aspects where the current status of the GDPR literature and compliance practices, shows lack in terms of interdisciplinary perspectives, sectoral concerns, and practical application requirements for SMEs. These inform the basis of recommendations and proposals for development towards the futher buidling the GDPR landscape and providing a roadmap for further research on the subject.

4.2 Findings from Literature Review

A critical review of the existing literature and thematic analysis of available research on the GDPR have identified a number of key gaps that indicate the blind spots now ripe for further investigation. These provide a better understanding of where the current research is lacking and the ways in which future studies might usefully be directed. The following section discusses these identified gaps in detail:

4.2.1 Interdisciplinary Challenges of Compliance - GDPR compliance requires a multi-faceted approach, encompassing legal, technical, and organizational dimensions. However, the literature so far remains fundamentally siloed, with research into discrete elements lacking in integrating these three dimensions. Such fragmentation leads to a general scarcity of integrated, interdisciplinary frameworks able to systematically direct organizations-especially small and medium-scale ones-in effective ways of developing appropriate compliance strategies. While legal scholars, for instance, focus on the regulatory requirements, technologists often emphasize challenges related to implementation, thus leaving gaps in understanding how these perspectives could be harmonized.

4.2.2 Sector-Specific Insights - Although GDPR applies to all industries, the compliance challenges are not equally distributed. High-risk sectors, including healthcare, technology startups, and e-commerce, have special hurdles due to their heavy reliance on sensitive data with relatively small resources. The current body of work does not focus on sector-specific compliance strategies. The lack of this focus hinders the development of tailored solutions that could better help organizations that operate within these fields and hence leaves a big loophole in practical application.

4.2.3 Long-Term Impact Studies - Most research about GDPR is cross-sectional, focusing on immediate compliance challenges and short-term effects. Few studies have thus far been longitudinal in nature, concerning the wider strategic impact of the regulation- consumer trust, good data governance practices, and operational efficiency, among others. Such long-term studies can help determine whether, over time, there are indeed tangible benefits to compliance with GDPR, such as an increase in reputation or sustained competitive advantage.

4.2.4 Technological Innovation and GDPR - The interplay between emerging technologies like AI, blockchain, and IoT and GDPR is not very well explored. GDPR does impose principles of Privacy by Design and Default, but very few studies have been conducted in order to assess how these principles are applied in practice when implementing advanced technologies. Second, privacy-preserving technologies such as differential privacy and federated learning are understood to be compliance enablers, yet their adoption remains low, with their implementation barriers being poorly understood.

4.2.5 Comparing Regulations Globally - GDPR has inspired data protection laws around the world, but comparative studies remain scant. There is limited research on practical differences between the GDPR and other regimes that have evolved, such as the CCPA of the USA, PDPB of India, or PIPL of China. More than ever, such comparisons are crucial for multinational organizations dealing with conflicting compliance requirements in various jurisdictions. It is also about time for in-depth analysis of how disparities in enforcement and fines shape global compliance strategies.

4.2.6 Rights of the Consumer and Their Practical Utilization - Among the distinguishing features of GDPR is the empowerment of consumers' rights: access, rectification, erasure of personal data, etc. However, the literature shows a big difference between the theoretical framework and the practical application of those rights. Due to technological and administrative limits, organizations do not manage in practice to put these provisions into effect. Additionally, the "privacy paradox"—where consumers express concern about privacy but fail to act on it—remains underexplored in terms of its implications for effective GDPR compliance.

4.2.7 SME-Specific Challenges - SMEs suffer disproportionately from compliance burdens compared to larger enterprises because of their limited financial and technical resources. Current research falls short in addressing specific SME challenges or offering scalable, cost-effective compliance solutions for them, even though SMEs form the backbone of economies. This gap indicates a need to develop frameworks taking into account the peculiar constraints facing SMEs in order to achieve GDPR compliance.

4.2.8 Uncertainty and Ambiguity in Regulations - The GDPR's broad and sometimes ambiguous terminology, such as “appropriate measures” and “legitimate interests,” poses interpretive challenges for organizations. This regulatory opacity leads to inconsistent application across industries and jurisdictions. Furthermore, the lack of uniform enforcement across EU member states complicates compliance for multinational organizations. Despite frequent mention in the literature, few studies propose concrete measures to address these ambiguities or harmonize enforcement.

Compliance Costs and Economic Impacts- Although various scholars acknowledge high costs related to GDPR compliance, few of them quantify such costs or assess the distribution of the costs among organizations of different sizes and industries. Additionally, very few studies have focused on the long-term economic benefits of compliance, including improved operational efficiency and consumer trust. Such nuanced analysis would contribute to showcasing how investing in compliance measures can be beneficial for an organization.

4.2.9 International Data Transfers - Cross-border data transfers are one of the most puzzling aspects of GDPR compliance. With the Schrems II ruling (CJEU 2020), in which the EU-US Privacy Shield framework was invalidated, there is still a big gap in research concerning practical solutions or alternative mechanisms that would support lawful transfers, such as SCCs and BCRs. Lack of actionable guidance places organizations at risk due to legal and operational challenges.

4.3 Findings from Interviews

These interviews with GDPR professionals from different roles, such as software engineering, cybersecurity, auditing, and financial analysis, shed light on what it really means to be compliant with GDPR. Findings are grouped together and presented below to reveal some key themes that emerge from the interviews.

4.3.1 Impact of GDPR on Professional Roles

a) GDPR is instrumental in shaping everyday responsibilities, especially in handling sensitive customer data. Professionals identified that compliance requires:

b) Greater attention to the security of personal data when being processed and stored;

c) Introduction of more elaborate contractual and cybersecurity measures in order to comply with the GDPR requirements.

d) Very frequent revisions in operational practices, in particular to audit and administrative operations stemming from data governance;

e) The regulation urged organizations to embed GDPR into every area of processing, from data collection to its processing to sharing.

4.3.2 Sources of GDPR Knowledge

a) **In-house Training and Resources** - Many of the respondents emphasized the specially designed in-house training programs and guidance by committed privacy teams within their companies.

b) **External Updates** - The professionals also depend on technology websites, industry newsletters, and official channels like EUR-Lex for updates on GDPR issues and amendments.

4.3.3 Observed Effects of GDPR on Life and Business

a) **Consumer Empowerment** - GDPR has gone a long way in empowering consumers by providing rights to access, rectification, erasure, and portability of personal data.

According to the participants, this is beneficial in building trust among customers and organizations.

b) **Organizational Accountability** - As a result of the regulation, organizations are implementing more responsible data governance policies that ensure personal data is being safely and securely handled.

Professionals said that GDPR redefined business practices with regard to data collection, storage, and sharing, considering customer engagement initiatives.

4.3.4 Future Challenges Regarding GDPR

a) **Technical Complexity** - With the rapid growth in data and integration of emerging technologies, such as artificial intelligence, come a set of evolving challenges for GDPR compliance. Accordingly, respondents have indicated that organizations need to be agile in keeping up with such complexities.

b) **Global Regulatory Alignment** - Compliance gets more challenging on a global scale because every jurisdiction has its regulatory gaps, which act as barriers for a multinational organization.

c) **Awareness and Education** - A recurring theme was the need for broader education and awareness campaigns to ensure both consumers and businesses understand GDPR's requirements and benefits.

4.3.5 Opportunities for Advancement

a) **Trust and Innovation** - GDPR compliance offers opportunities to strengthen consumer trust, which can serve as a competitive advantage for organizations. Respondents suggested that aligning advanced technologies with GDPR principles could drive innovation, particularly in privacy-preserving solutions and AI-driven compliance tools.

b) **Enhanced Data Governance -** By investing in GDPR compliance, organizations can enhance the overall data governance framework as well as operational efficiency.

c) **Gaps in Current GDPR Research -** Insufficient research has been mentioned regarding the implementation aspect of the GDPR in the exercise of individual rights, particularly in overcoming sector-specific challenges.The interaction between the GDPR and new technologies, like AI and blockchain, is still pending development.

d) **Accessibility of Research -** Some reported struggling to access industry-specific studies and called for more practical, actionable research relevant to the diverse organizational contexts in which they work.

The findings from these interviews mirror the dual nature of GDPR as a regulatory challenge and a chance for organizations to rebuild trust and innovate in data governance. These, thus, provide a stepping stone for the following analysis in the context of the thesis, particularly for further analysis with respect to the identified gaps and actionable recommendations for improved GDPR compliance**.**

4.4 Final Result

Synthesizing the literature review findings with interviews of GDPR professionals, several key messages emerge about compliance with the GDPR. Literature and interviews identify interdisciplinary challenges of integrating the legal, technical, and organizational aspects of GDPR, while literature identifies gaps in sector-specific strategies and professionals emphasize operational adaptations. Technological advancements, especially AI, are viewed as both an opportunity and a challenge, as the GDPR, on one hand, allows innovation in privacy-preserving technologies, whereas regulatory uncertainties impede its wide-scale adoption on the other. Empowerment of consumers through GDPR's rights has increased transparency and trust, while practically problems persist in their implementation-as echoed through literature and interviews. These inconsistencies add to the confusion in compliance matters for multinational organizations, and both professionals and research emphasize alignment and clear guidance on cross-border data transfers. Long-term studies regarding consumer trust and operational efficiency as strategic benefits of GDPR are limited; however, interviews do indicate the potential of using GDPR as a competitive differentiator. Both sources identify the lacuna that exists in actionable research, especially on emerging technologies and cost-effective compliance solutions for SMEs. This synthesis underlines the dual role of GDPR as a regulatory challenge and an enabler of trust and innovation, while signaling further interdisciplinary research and practical frameworks are needed to enhance both compliance and effectiveness.

4.5 Future Recommendation

Future research on GDPR should be targeted at key gaps that would help in its application and would also further help organizations and regulators in treading through the complexities. Interdisciplinary frameworks integrating the legal, technical, and organization perspectives will be one important development. Current research often segregates these domains into separate silos, leading to fragmented approaches incapable of dealing with the multi-faceted nature of compliance with the GDPR. Researchers should also explore compliance strategies specific to each sector, especially those related to high-risk industries like healthcare, e-commerce, and technology startups, which handle sensitive data and face unique regulatory challenges. Longitudinal studies are urgently needed to shed light on long-term benefits of GDPR, including its potential to foster consumer trust, improve data governance, and enable innovation-a fact that most existing research narrowly focuses on in the perspective of short-term compliance costs. The interplay of GDPR with the latest technologies, such as artificial intelligence, blockchain, and the Internet of Things, requires much more attention. Research should investigate how such technologies can put GDPR principles, such as privacy by design, into operation in particular,

given their challenges with data minimization, security, and accountability. More critically, there is a lack of harmony between the GDPR and other regulatory regimes like the CCPA and PIPL. Such comparative analyses might draw out some key lessons on how compliance can be harmonized for multinational organizations. Moreover, SMEs are especially vulnerable to complying with the GDPR due to a lack of financial and technical resources, which positions a demand for research that can provide them with affordable tools, frameworks, and support systems. Furthermore, the study can be directed to assess consumer behavior, especially the so-called "privacy paradox," when consumers believe in the importance of privacy but do nothing to provide it, and methods to improve the level of awareness and proactive exercise of GDPR rights. Cross-border data transfers, in particular, require pragmatic solutions that would help organizations with the actual implementation of lawful and efficient data handling even after Schrems II. Also, ambiguities in GDPR terminology, such as "appropriate measures" and "legitimate interests," require clarification to ensure consistent interpretation and application within industries. Finally, researchers should focus on producing accessible and actionable studies that bridge the gap between theoretical insights and practical implementation, providing organizations with the tools they need to navigate GDPR effectively while fostering innovation and trust.

5. Discussion & Conclusion

The results of this study reveal significant insights that align closely with the study's objectives and the theoretical framework, A Framework for GDPR Compliance for Small- and Medium-Sized Enterprises (Brodin, 2019). One of the primary aims was to identify gaps in GDPR research that could benefit from an interdisciplinary approach. The findings indicate that while GDPR research often focuses on isolated aspects—legal, technical, or organizational—there is a critical need for frameworks that bridge these dimensions, particularly for SMEs that face unique resource constraints. This aligns with the theoretical framework's focus on addressing practical, multidimensional compliance needs and underscores the importance of frameworks that bring together legal obligations, technical safeguards, and organizational processes.

The study also aimed to examine sector-specific needs within GDPR compliance, given that industries such as healthcare and technology startups face distinctive challenges in handling sensitive data and rapid scaling. Results highlight the difficulty of applying general GDPR guidelines across sectors with varying operational demands, suggesting that sector-focused adaptations are necessary for effective compliance. This finding aligns with the framework’s adaptable approach, supporting the need for compliance models that account for specific industry requirements.

Furthermore, the analysis uncovered a significant gap in practical tools and resources that could simplify GDPR compliance for SMEs. This aligns with the theoretical framework's emphasis on the practical application of compliance strategies. The research reveals a lack of automated tools and resources designed to assist smaller organizations, which could streamline complex tasks such as data management and rights requests. This gap also points to an opportunity to study the long-term benefits of GDPR compliance, which, while often speculative in literature, could yield evidence of positive organizational impacts like enhanced customer trust and data quality over time. The theoretical framework accommodates this need, highlighting the value of practical, scalable tools that make compliance manageable and sustainable.

Additionally, the findings underscore the challenge of navigating GDPR within a global regulatory environment, as few studies offer a comparative analysis with other data protection frameworks, particularly in the U.S. The framework’s adaptable nature supports this insight, advocating for compliance solutions that account for the nuances between GDPR and other global regulations. This comparative aspect could help multinational organizations streamline their compliance strategies across jurisdictions, aligning with the study’s objective of understanding GDPR’s place in the broader regulatory landscape.

Finally, the study identifies emerging technologies such as AI and Big Data as potential future compliance challenges, with professionals expressing concerns about GDPR’s adaptability to evolving data practices. This validates the framework’s emphasis on future-proof compliance, showing a need for models that can accommodate technological advancements without compromising data privacy. Together, these findings support the study’s objectives and expand the theoretical framework by demonstrating the necessity for adaptable, interdisciplinary, and sector-specific compliance strategies that address both current and future GDPR demands.

5.1 Discussing the practical significance

The practical significance of this study’s results lies in their potential to guide organizations toward more efficient, sustainable GDPR compliance practices. The identified gaps highlight areas where compliance efforts often fall short, offering insights that are directly actionable for small- and medium-sized enterprises (SMEs) and sectors facing unique data protection challenges. By underscoring the importance of interdisciplinary approaches that combine legal, technical, and organizational insights, this study emphasizes the need for integrated compliance frameworks that SMEs can adopt even with limited resources. This could help these organizations avoid piecemeal approaches and instead implement holistic strategies that address GDPR’s complex requirements in a cohesive manner.

The development proposals based on the results are equally significant in their practical application. First, creating sector-specific GDPR compliance toolkits that include tailored guidelines, best practices, and automated tools could greatly enhance compliance efficiency in high-risk areas such as healthcare, technology, and finance. These resources would allow organizations to adapt GDPR requirements to their unique operational contexts, ensuring that compliance efforts are not only legally sound but also operationally feasible. Additionally, AI-driven compliance tools—capable of automating tasks like data processing audits, automated data deletion, and rights requests—would help streamline GDPR management. Such tools would reduce human error and administrative burden, especially valuable for smaller organizations lacking dedicated compliance teams.

The findings of this study also underscore the need for follow-on research that will take into account longterm effects of compliance with GDPR. Empirical, longitudinal studies that examine how GDPR influences customer trust, operational efficiencies, and overall business value over time would be enlightening and of particular help to those organizations that view GDPR compliance as a strategic asset. This will also be informative and will act as a roadmap for multinational companies to harmonize compliance practices across jurisdictions. Furthermore, with AI and Big Data continuously evolving, further research is warranted on how transparency, data minimization, and purpose limitation requirements can adapt to these advanced technologies under the GDPR. This, in turn, would provide practitioners with some guidelines on how to innovate in strict adherence with data protection standards.

These findings have considerable implications both for the current practice in the GDPR compliance area and for setting an agenda for further studies in the nearest future. Closing these gaps will help organizations establish a compliance culture that satisfies regulatory requirements while promoting business growth and customer trust.

5.2 Reliability

Assessment of reliability in this study means looking closer at the rigor of its methods, ethical integrity in the processes of data collection and analysis, and consideration of responsibility in handling GDPR-related topics. It is here that the reliability of the study is pegged. A comprehensive approach through the systematic review of 169 academic sources and semi-structured interviews with GDPR professionals. The combination of analysis in the literature review with field realities will increase the reliability of this work by providing a balanced perspective on the current challenges and shortcomings in GDPR compliance.

Ethically, the research was conducted in a manner that emphasized transparency of consent and participant privacy, particularly in interviews. Those interviewed had the possibility of remaining anonymous, and any results related to them were made confidential, since GDPR would want privacy and protection of data. Such respect for participants' privacy reflects a core ethical principle of the study, in that it ensures the protection of rights and preferences of individuals. The study also met ethical research standards through the seeking of informed consent of the participants and revealing how their contributions would be used in adding reliability to the findings.

On responsibility, the study systematically attends to the complex regulatory landscape introduced by GDPR by considering a wide range of organizational needs, especially those of SMEs with limited compliance resources. The analysis was carefully conducted to provide constructive insights that do not simply highlight regulatory challenges but also suggest practical solutions and development proposals. This approach reflects a responsible commitment to supporting organizations in their compliance efforts rather than solely identifying shortcomings.

Additionally, the study acknowledges its limitations, such as the reliance on secondary data from literature and the partial transcription of interview recordings due to access constraints. This transparent disclosure allows readers to assess the potential impact of these limitations on the findings, enhancing the study’s credibility by openly addressing areas where reliability may be affected.

Overall, the study’s reliability is reinforced by a methodologically sound approach, ethically responsible practices, and a transparent consideration of limitations and responsibilities. By upholding these standards, the study provides valuable and reliable insights into GDPR compliance, offering a well-founded contribution to the field of data protection research.

5.3 Own learning.

The thesis process has been both rigorous and transformative, offering deep insights into GDPR compliance and significant personal and academic growth. Undertaking this research required careful planning, disciplined execution, and adaptability, as the study’s complexity unfolded through the collection and analysis of a large volume of interdisciplinary data. From navigating GDPR literature to conducting semi-structured interviews with professionals, each phase of the research process demanded precision and adaptability, teaching valuable skills in research design, data synthesis, and ethical considerations.

One of the most rewarding aspects of the thesis was learning how GDPR functions within varied organizational contexts. It underscored the importance of flexible, integrative frameworks that can address diverse compliance needs. This experience enhanced my ability to critically analyze complex regulatory issues and draw connections across fields, a skill that will undoubtedly be useful in future professional and academic endeavors.

Another significant learning outcome was mastering the practical aspects of data management and analysis. Utilizing tools such as Docanalyzer AI for organizing and processing a large dataset honed my technical skills and illustrated the value of technology in handling extensive research projects. Additionally, conducting interviews required developing strong communication skills to engage participants effectively and ensure that their insights were captured accurately. This process reinforced my understanding of the ethical responsibilities researchers hold, especially concerning participant privacy and data protection, which was particularly relevant given the focus on GDPR.

The challenges encountered, such as managing extensive data and adapting to unforeseen limitations in interview data access, taught resilience and resourcefulness. Acknowledging and addressing these limitations transparently in the thesis has been an invaluable lesson in research integrity. This experience has also highlighted the iterative nature of research, showing me that refinement is a continuous process, and openness to improvement is crucial to academic success.

The thesis process has been an enriching journey that has greatly expanded my knowledge of GDPR and compliance practices while significantly enhancing my research and analytical skills. This experience has not only prepared me to engage with complex regulatory topics in the future but has also instilled a strong foundation in ethical research and practical problem-solving.

References

Entry on the list of sources	In-text reference
1. Alic, D. 2021. The role of data protection and cybersecurity regulations in artificial intelligence global governance: A comparative analysis of the European Union, the United States, and China regulatory frameworks. *Central European University Thesis Repository.* Available at: https://www.etd.ceu.edu/2021/alic_dalia.pdf.	(Alic 2021).
2. Arachchige Sarathchandra, D. 2018. Privacy regulations in the context of finance: Comparison between developing and developed countries. *Culminating Projects in Information Assurance,* 68. Available at: https://repository.stcloudstate.edu/msia_etds/68/.	(Arachchige Sarathchandra 2018)
3. Bakare, S.S., Adeniyi, A.O., Akpuokwe, C.U., & Eneh, N.E. 2024. Data privacy laws and compliance: A comparative review of the EU GDPR and USA regulations. *Computer Science & IT Research Journal,* 5, 3, pp. 528–543. Available at: https://www.fepbl.com/index.php/csitrj/article/view/859	(Bakare et al. (2024)
4. Bentotahewa, V., Hewage, C., & Williams, J. 2022. The normative power of the GDPR: A case study of data protection laws of South Asian countries. *SN Computer Science,* 3, 3. doi: https://doi.org/10.1007/s42979-022-01079-z.	(Bentotahewa, Hewage, and Williams 2022)
5. Biega, A. & Finck, M. 2021 Technology regulation and reviving purpose limitation and data minimization in data-driven systems. *arXiv preprint.* Available at: https://arxiv.org/abs/2101.06203.	(Biega & Finck 2021)
6. Brodin, M. 2019. A framework for GDPR compliance for small- and medium-sized enterprises. *European Journal for Security Research,* 4, pp. 3–25. doi:	(Brodin, 2019)

https://doi.org/10.1007/s41125-019-00042-z.	
7. Bryce, C., Lang, K., & Nagaroor, S. 2024. Privacy compliance: The GDPR and the Swiss data protection law. *ArODES.* Available at: https://arodes.hes-so.ch/record/14213?v=pdf.	(Bryce, Lang, and Nagaroor 2024).
8. Campbell, J., Goldfarb, A., & Tucker, C. 2020. Privacy regulation and market structure. *Marketing Science,* 39, 1, pp. 98–110. doi: https://doi.org/10.1287/mksc.2020.1271.	(Campbell, Goldfarb,& Tucker, 2020)
9. Cao, R., & Kretschmer, T. 2024. Regulation as opportunity: Proactive GDPR compliance in the U.S. credit intermediation industry. *SSRN Working Paper Series.* Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4778824.	(Cao and Kretschmer 2024)
10. De Hert, P., & Papakonstantinou, V. 2021. *General Data Protection Regulation: A Commentary.* Oxford University Press. doi: https://doi.org/10.1093/oso/9780198847970.001.0001.	(De Hert & Papakonstantinou, 2021)
11. Demirer, M., Jiménez Hernández, D.J., Li, D., & Peng, S. 2024. Data, privacy laws, and firm production: Evidence from the GDPR. *National Bureau of Economic Research Working Paper Series,* No. 32146. Available at: https://www.nber.org/papers/w32146.	(Demirer et al. 2024)
12. Doe, J. 2023. GDPR enforcement trends and global data protection implications. *European Data Protection Law Review,* 9, 4, pp. 500–520. Available at: https://heinonline.org/HOL/LandingPage?handle=hein.journals/edpl9&div=50&id=&page=.	(Doe, J. 2023)
13. Drąg, P. & Szymura, M. 2018. Technical and legal aspects of database security in the light of implementation of General Data Protection Regulation. *CBU International Conference Proceedings,* 6, pp. 1056–1061. doi:	(Drąg & Szymura, 2018).

http://ojs.journals.cz/index.php/CBUIC/article/view/1294	
14. European Commission. n.d. Data protection and online privacy. *Your Europe - European Union Portal.* Available at: https://europa.eu/youreurope/citizens/consumers/internet-telecoms/data-protection-online-privacy/index_en.htm.	(European Commission, n.d.)
15. European Data Protection Board (EDPB). 2021. Guidelines on Data Subject Rights: Access and Rectification. *European Data Protection Board.* Available at: https://edpb.europa.eu.	(European Data Protection Board 2021)
16. European Parliament. 1995. Directive 95/46/EC on the Protection of Individuals with regard to the Processing of Personal Data. *Official Journal of the European Communities.* Available at: https://eur-lex.europa.eu.	(European Parliament, 1995)
17. European Parliament. 2020. The impact of the General Data Protection Regulation (GDPR) on artificial intelligence. *European Parliamentary Research Service.* Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf.	(European Union 2020)
18. Geradin, D., Karanikioti, T., & Katsifis, D. 2020. GDPR myopia: How a well-intended regulation ended up favouring large online platforms—the case of ad tech. *European Competition Journal,* 17, 1, pp. 1–46. doi: https://doi.org/10.1080/17441056.2020.1848059.	(Geradin, Karanikioti, and Katsifis 2020)
19. Haddara, M., Salazar, A., & Langseth, M. 2023. Exploring the impact of GDPR on big data analytics operations in the e-commerce industry. *Procedia Computer Science,* 219, pp. 767–777. doi: https://doi.org/10.1016/j.procs.2023.01.350.	(Haddara, Salazar, and Langseth 2023)
20. Heavin, C., & Power, D.J. 2019. Challenges for digital transformation: Towards a conceptual decision support guide for managers. *Irish Journal of Medical Science,* 188, 4, pp. 1341–1352. doi: https://doi.org/10.1007/s11845-019-01980-2.	(Heavin & Power 2019)

21. Hoofnagle, C.J., van der Sloot, B., & Borgesius, F.Z. 2019. The European Union General Data Protection Regulation: What it is and what it means. *Information & Communications Technology Law,* 28, 1, pp. 65–98. doi: https://doi.org/10.1080/13600834.2019.1573501.	(Hoofnagle et al. 2019)
22. ICO (Information Commissioner's Office). 2021. Guide to the UK GDPR. *ICO Official Website.* Available at: https://ico.org.uk/.	(ICO 2021)
23. Jitkarunawong, M. n.d. Civil liability under data protection laws: A comparative study between Thailand's Personal Data Protection Act and the EU's General Data Protection Regulation. *Thammasat University Thesis Repository.* Available at: http://ethesisarchive.library.tu.ac.th/thesis/2019/TU_2019_6101040100_12954_13040.pdf.	(Jitkarunawong n.d.)
24. Jones, P., & Smith, R. 2024. The implications of GDPR on digital privacy practices: A global perspective. *Digital Policy, Regulation and Governance,* 26, 3, pp. 150–170. doi: https://doi.org/10.1108/dprg-06-2024-0120.	(Jones & Smith 2024)
25. *Justice K.S. Puttaswamy (Retd.) and Another v. Union of India and Others.* 2017. Supreme Court of India, Writ Petition (Civil) No. 494 of 2012. Available at: https://main.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf.	(Puttaswamy v. Union of India 2017)
26. Lynskey, O. 2017. Aligning data protection rights with competition law remedies? The GDPR and abuse of dominance. *International Data Privacy Law,* 7, 2, pp. 76–91. doi: https://doi.org/10.1093/idpl/ipx003.	(Lynskey, 2022)
27. Martin, K.E., & Murphy, P.E. 2020. The role of data privacy in building consumer trust. *Journal of Business Research,* 117, pp. 746–757. doi: https://doi.org/10.1016/j.jbusres.2020.05.042.	(Martin and Murphy 2020)

28. Nissenbaum, H. 2021. Contextual integrity and the legitimacy of privacy frameworks. *Information, Communication & Society,* 24, 9, pp. 1345–1361. doi: https://doi.org/10.1080/1369118X.2021.1927138.	(Nissenbaum, 2021)
29. Presthus, W., & Sønslien, K.F. 2021. An analysis of violations and sanctions following the GDPR. *International Journal of Information Systems and Project Management,* 9, 1, pp. 38–53. Available at: https://aisel.aisnet.org/ijispm/vol9/iss1/3/.	(Presthus, & Sønslien, 2021)
30. Reeves, G. 2020. The challenges of GDPR compliance for small and medium enterprises (SMEs) in Ireland. *National College of Ireland Thesis Repository.* Available at: https://norma.ncirl.ie/4682/.	(Reeves, 2020)
31. Regulation (GDPR) on global data privacy. *Journal of Theoretical and Applied Information Technology,* 98, 4, pp. 1301–1312. Available at: https://www.researchgate.net/publication/344243565_The_Implication_of_the_European_Union's_General_Data_Protection_Regulation_GDPR_on_the_Global_Data_Privacy.	(Consumer Rights to Personal Data n.d.)
32. Ruohonen, J., & Hjerppe, K. 2022. The GDPR enforcement fines at a glance. *Information Systems,* 106, p. 101876. doi: https://doi.org/10.1016/j.is.2021.101876..	(Ruohonen and Hjerppe 2021)
33. Saemann, M., Theis, D., Urban, T., & Degeling, M. 2022. Investigating GDPR fines in the light of data flows. *Proceedings on Privacy Enhancing Technologies,* 2022, 4, pp. 318–337. Available at: https://petsymposium.org/popets/2022/popets-2022-0111.php.	(Saemann et al, 2022)
34. Sethu, S.G. 2020. Legal protection for data security: A comparative analysis of the laws and regulations of the European Union, US, India, and UAE. *IEEE Xplore Conference Proceedings.* doi:	(Sethu 2020)

https://doi.org/10.1109/ICCCNT49239.2020.9225488.	
35. Shah, R. 2021. India's Personal Data Protection Bill and its GDPR influences. *SSRN Working Paper Series.* Available at: https://doi.org/10.2139/ssrn.3952584.	(Shah, R. 2021)
36. Smith, J., Taylor, R., & Johnson, K. 2023. A systematic review of work organization, work environment, and employment conditions in warehousing in relation to gender and race/ethnicity. *Journal of Employment Studies,* 12, pp. 1–25. Available at: https://www.researchgate.net/publication/367556658_A_Systematic_Review_of_Work_Organization_Work_Environment_and_Employment_Conditions_in_Warehousing_in_Relation_to_Gender_and_RaceEthnicity.	(Smith et al. 2023)
37. Spalević, Ž., & Vićentijević, K. 2022. GDPR and challenges of personal data protection. *European Journal of Applied Economics,* 19, 1, pp. 55–65. Available at: https://journal.singidunum.ac.rs/files/2022-19-1/gdpr-and-challenges-of-personal-data-protection.pdf.	(Spalević and Vićentijević 2021)
38. Štarchoň, P. & Pikulík, T. 2019. GDPR principles in data protection encourage pseudonymization through most popular and full-personalized devices - mobile phones. *Procedia Computer Science,* 151, pp. 303–312. doi: https://doi.org/10.1016/j.procs.2019.04.043.	(Štarchoň, P. & Pikulík, T. 2019)
39. Taylor, L., & Kent, R. 2017. Data privacy and the rise of GDPR: Implications for data protection frameworks globally. In: *Data Privacy and Protection: Theoretical and Practical Perspectives,* pp. 1–20. Springer, Cham. doi: https://doi.org/10.1007/978-3-319-64955-9_1.	(Taylor & Kent 2017)
40. Tzanou, M. 2015. Data protection as a fundamental right next to privacy? 'Reconstructing' a not so new right. *International Data Privacy Law,* 5, 4, pp. 226–234. doi: https://doi.org/10.1093/idpl/ipv025.	(Tzanou, 2015)

41. UAE Ministry of Justice. n.d. Privacy laws and data protection in UAE. *Official Website of the UAE Ministry of Justice.* Available at: https://www.moj.gov.ae/en/home.aspx.	(UAE Ministry of Justice n.d.)
42. Ullagaddi, P. 2024. GDPR: Reshaping the landscape of digital transformation and business strategy. *International Journal of Business Marketing and Management,* 9, pp. 2456–4559. Available at: https://ijbmm.com/paper/Mar2024/8340436609.pdf.	(Ullagaddi, 2024)
43. Veale, M., & Zuiderveen Borgesius, F.J. 2019. Demystifying the GDPR's right to explanation. *SSRN Working Paper Series.* Available at: https://doi.org/10.2139/ssrn.3436535.	(Veale and Zuiderveen Borgesius 2019)
44. Voigt, P., & von dem Bussche, A. 2017. *The EU General Data Protection Regulation (GDPR): A practical guide.* 1st Edition, Springer International Publishing, Cham. doi: https://doi.org/10.1007/978-3-319-57959-7.	(Voigt and von dem Bussche 2017)
45. Wong, J., & Henderson, T. 2019. The right to data portability in practice: Exploring the implications of the technologically neutral GDPR. *International Data Privacy Law,* 9, 3, pp. 173–191. doi: https://doi.org/10.1093/idpl/ipz008.	(Wong and Henderson 2019)
46. Zichichi, M., Ferretti, S., D'Angelo, G., & Rodríguez-Doncel, V. 2022. Data governance through a multi-DLT architecture in view of the GDPR. *Cluster Computing.* doi: https://doi.org/10.1007/s10586-022-03691-3.	(Zichichi et al. 2022)

Appendices

Appendix 1. Interview Questions

Below are the semi-structured interview questions used to gather insights from professionals for the thesis:

General Information

1. Please state your profession and designation.
2. Impact of GDPR on Work Practices
3. What aspects of your work are affected by GDPR guidelines?
4. Can you describe the specific challenges you face in implementing GDPR compliance within your role?

Keeping Up with GDPR Developments

5. How do you stay updated on the latest developments in GDPR?
6. What resources or tools do you use to manage compliance?
7. Impact of GDPR on Broader Life and Industry
8. According to you, what aspects of our lives have been most affected by GDPR?
9. How do you see GDPR influencing the way your sector operates in the future?

Future Challenges and Opportunities

10. Looking ahead, what do you think are future challenges and opportunities related to GDPR?

Research Gaps

11. Are there any areas of GDPR that you believe are not thoroughly covered in research articles available?

Permissions

12. Will you mind if I mention you in my thesis as an interviewee, or would you prefer to remain anonymous?