Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 10, No. 4, 90-105
2026
Publisher: Learning Gate
DOI: 10.55214/2576-8484.v10i4.12560

Enhancing data governance framework for data privacy in Saudi Arabia

Zahyah H. Alharbi[1*], Amal A. Alwahbi[2], Tahani Alqurashi[3]
[1,2]Management Information Systems Department, College of Business Administration, King Saud University, Riyadh 12372, Saudi Arabia; zalharbi@ksu.edu.sa (Z.H.A.) amalalwahbii@gmail.com (A.A.A.).
[3]College of Computing, Data Science Department, Umm Al-Qura University, Makkah 24382, Saudi Arabia; tmqurashi@uqu.edu.sa (T.A.).

Abstract: This study evaluates data governance framework implementation in the Kingdom of Saudi Arabia, with particular emphasis on identifying data privacy challenges and proposing enhancement strategies. A qualitative research approach was employed, conducting semi-structured interviews with thirteen participants from private, government, and semi-government organizations that have implemented DAMA-DMBOK-based data governance frameworks. Thematic analysis was used to identify implementation challenges and improvement areas. Four primary challenges emerged: insufficient organizational awareness of data governance value, difficulties complying with international data protection regulations (particularly GDPR), inadequate data classification practices, and stakeholder resistance due to conflicts of interest. While framework adoption remains incomplete, participants recognize the need for enhancement through three strategic interventions: clearly defining strategic and operational objectives, increasing organizational awareness while developing human and technical resources, and strengthening data privacy through proactive integration into system design phases. This research provides actionable recommendations for Saudi organizations and policymakers to facilitate effective data governance implementation, emphasizing the balance between data protection requirements and organizational innovation needs.

Keywords: *DAMA-DMBOK, Data governance, Data privacy, GDPR compliance, Qualitative research, Saudi Arabia, Thematic analysis.*

1. Introduction

The significance of data utilization in businesses has gained prominence due to the recent upsurge in business activities. Data has demonstrated potential to optimize business operations [1]. Organizational data greatly impacts business decisions concerning operational and strategic activities. Data is a valuable organizational resource, and effective corporate governance is essential for exploiting data to help businesses make more informed decisions and enhance organizational efficiency and effectiveness [2].

Well-implemented data governance activities can have a positive impact on business revenue, cut operational and production costs, and increase shareholder value. Data governance delivers measurable value for a business. It ensures that the business has reliable, consistent, automated, and scalable data to support efficient decision-making and operations [3]. Data privacy is a critical consideration in data management. It governs the manner in which individuals within the organization can collect, store, or modify data within the information system. A robust data governance program can serve as the cornerstone for managing and safeguarding data assets [4, 5].

This study enhances a data governance framework for data privacy by reviewing existing literature, interviewing stakeholders, identifying and analyzing governance challenges, and proposing focused recommendations. It addresses a critical gap in the literature by offering a context-specific analysis of data governance frameworks in the Kingdom of Saudi Arabia (KSA), with a focused examination of data

History: Received: 27 January 2025; Revised: 2 March 2026; Accepted: 6 March 2026; Published: 30 March 2026
* Correspondence: zalharbi@ksu.edu.sa

privacy, contributing empirically informed and actionable recommendations aligned with organizational realities.

This paper is structured as follows: Section 2 covers related studies; Section 3 outlines the methodology; Section 4 discusses the findings; and Section 5 presents the conclusion and recommendations.

2. Related Work

This section provides a general overview of data governance and privacy, and data governance frameworks. Following that, we review studies that investigate data governance frameworks and privacy.

2.1. Data Governance

Otto [6] defines data governance as "a company-wide framework for assigning decision-related rights and duties to be able to adequately handle data as a company asset." Some academics believe that organizations that do not incorporate efficient data governance into their operations may struggle to remain competitive [7], as data management is critical to maintaining a competitive edge in today's business landscape. According to the Data Management Association (DAMA), data management is "the development, execution, and supervision of plans, policies, programs, and practices that control, protect, deliver, and enhance the value of data and information assets." [8]. Some researchers have stated that data governance complements rather than replaces data management [9], serving as the strategic layer that guides tactical data management activities.

The primary objectives of data governance for public organizations are to enable informed decision-making, ensure compliance with regulatory requirements, enhance operational efficiency and effectiveness, and support seamless integration of business operations. Data governance delivers direct benefits such as improved efficiency and reduced risks, as well as indirect benefits including enhanced stakeholder perception and trust in information management [10].

For Saudi enterprises, data governance entails not only acknowledging the significance of data assets as vital assets within the organization but also maximizing their value across the entire enterprise [11]. The implementation of data management practices should always adhere to the business's major strategic and operational policies and procedures [9]; however, data governance is considered to be a joint responsibility between IT and business.

2.2. Data Privacy Governance

Data privacy is a critical aspect of any organization's operation. It pertains to the handling of sensitive data and its privacy. It defines the parameters of how individuals within the organization collect, store, manipulate, share, or exchange data with third-party organizations within the information system [4].

Data security, on the other hand, focuses on the technical controls necessary to safeguard data from unauthorized access, manipulation, or disclosure. The CIA Triad is a fundamental concept within data security, addressing the core principles of data confidentiality, integrity, and availability [4]. Data security deals with the technical aspects of the collection of personally identifiable information (PII). Data privacy addresses the legal aspects of the data and focuses on the fundamental rights of individuals and organizations [12].

Following the announcement and implementation of the General Data Protection Regulation (GDPR) in 2016, the understanding of personal information has evolved and is now more broadly recognized. Cultural and geographical differences must be taken into consideration when defining personal information. Personal information can be defined as any digital or physical data that can be indirectly or directly associated with "natural persons" [13]. This definition extends beyond personal identifiable information (PII) and encompasses transactional information.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 10, No. 4: 90-105, 2026
DOI: 10.55214/2576-8484.v10i4.12560

The numerous factors contributing to data privacy risks present a significant challenge for organizations in risk management and mitigation [13]. Data governance addresses these challenges by proactively managing big data requirements, mitigating privacy risks, and fostering innovation through data quality criteria such as timeliness, meaningfulness, trustworthiness, and sufficiency.

2.3. Data Governance Framework

Data Governance Frameworks (DGF) play a crucial role in the successful implementation of data governance activities. The implementation components associated with data governance include people, processes, and technologies. The elements that define, construct, and deploy an effective data governance framework are common functional titles, diverse data governance roles and responsibilities, data ownership, policies, processes, standards, tools, supporting technologies, data governance bodies and committees, and data stewardship [13].

An efficient and effective data governance framework should consider four main components: standards, processes and policies, organizational structures, and tools and technology. There are two conventional approaches for implementing a data governance framework: the top-down approach and the bottom-up approach. The top-down approach prioritizes data control to optimize data quality. The bottom-up approach prioritizes data access to optimize end-users' access. In addition to these methods, a modern collaborative approach has emerged, which strikes a balance between these two philosophies [14].

2.4. Data Governance Related Work

Alhassan et al. [15] conducted a comprehensive literature review on data governance, analyzing data governance process activities. A total of 31 research papers were scrutinized. They explored data governance activities related to the definition of action areas in the data governance decision domain and revealed the scarcity of information on the implementation and monitoring of data governance.

Abraham et al. [16] aimed to introduce a conceptual framework for data governance, literature synthesis, and a detailed plan for scholarly investigation. This research is grounded in a comprehensive, structured literature review of 145 research papers by practitioners from 2001 to 2019. They identified and classified the major building blocks associated with data governance into six dimensions [16].

Albahar and Thanoon [17] noted that business organizations in the Middle East face a lack of data privacy rules, regulations, and policies. Small, medium, and large-scale businesses in the region are currently dealing with data privacy issues. Their research focuses on addressing these challenges in the Middle East and proposing solutions.

Al-Khalifa et al. [18] presented the Saudi Privacy Policy Dataset, a collection of Arabic data privacy policies from various sectors in Saudi Arabia and an interpretation of the 10 Personal Data Protection Laws (PDPL) developed to be compatible with GDPR. The primary objective is to promote research and development in privacy policy analysis, natural language processing (NLP), and machine learning (ML) applications related to privacy and data protection.

Kunnen [19] claimed that their research study discovers new data governance-associated challenges. The ultimate objective was to highlight feasible and convenient remedies. The researchers conducted a literature review of existing research and an interview survey in collaboration with a field expert to validate their findings. These serve as the basis for establishing a data governance framework for future use, in the form of a generalized template for data governance use cases based on advanced analytics.

3. Methodology

This section outlines the research methodology structured into three distinct segments: research design, data collection, and data analysis, as shown in Figure 1.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 10, No. 4: 90-105, 2026
DOI: 10.55214/2576-8484.v10i4.12560

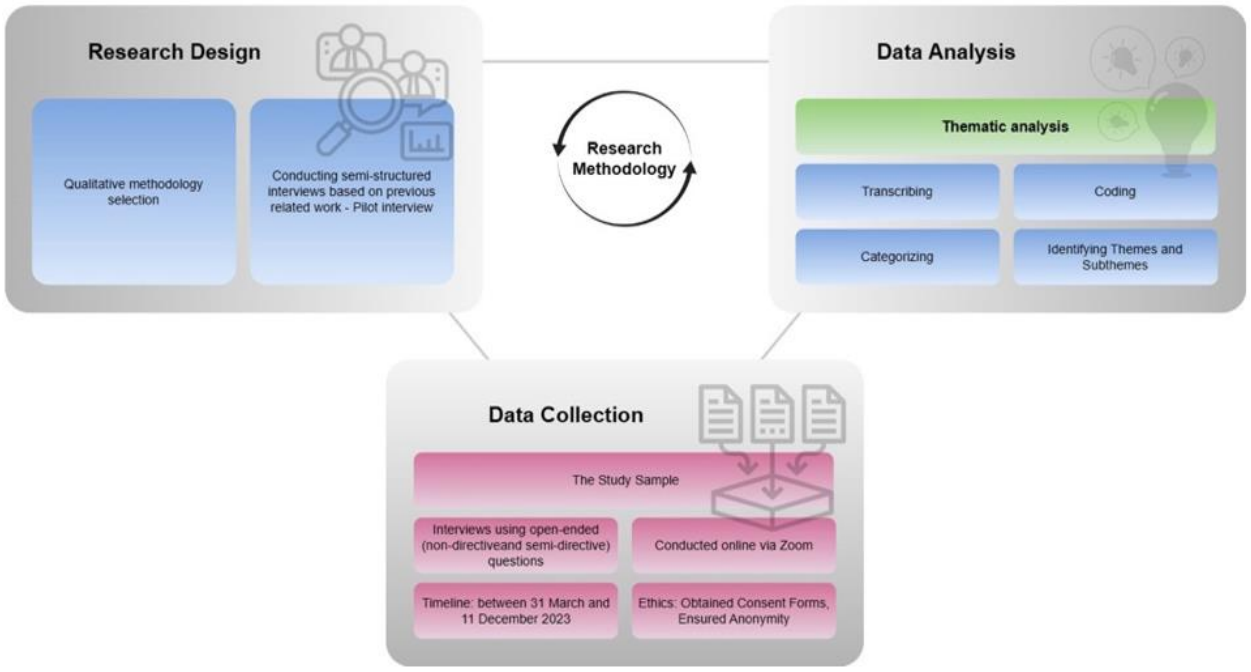

Figure 1.
Research Methodology.

3.1. Research Design

The study's purpose was to improve the data governance framework for data privacy in KSA and to examine challenges associated with data privacy governance. We endeavored to uncover reasons contributing to the inadequacy of the current data governance framework by exploring perspectives and attitudes of individuals employed in organizations adhering to the NDMO data governance framework. A qualitative research approach was employed, and interviews were conducted with individuals from semi-government and private organizations in KSA that have adopted data governance with data management offices. The interview method allows researchers and respondents to discuss phenomena under examination, as opposed to quantitative studies [20]. Semi-structured interview questions allow researchers to keep the discussion relevant while allowing respondents to discuss their experiences [21].

The researchers of this study formulated research-related interview questions based on a comprehensive literature review. We established an outline clearly defining areas of research interest and developed primary open-ended questions serving as a foundation for subsequent detailed discussions [22]. Questions were specifically tailored to elicit participants' perceptions and attitudes toward both conceptual aspects and practical applications of data governance frameworks, with a focus on data privacy. Efforts were made to formulate questions that avoided leading participants, thereby minimizing potential bias, yet were comprehensive enough to encompass a variety of specific topics related to assessing the state and effectiveness of data privacy governance frameworks.

Interview questions categorized organizations based on type (government, semi-government, private) and size. Questions delved into understanding individual definitions of data privacy in the data governance context, challenges faced in data privacy governance, frameworks in use, implementation methods, effectiveness in achieving data privacy goals, unmet needs, and suggestions on requirements to enhance frameworks. Prior to interviewing the entire sample, we conducted a single pilot interview to verify the effectiveness of the question format in achieving the desired clarity, scope, and depth of data. The outcomes of this pilot interview confirmed the comprehensive coverage of our investigative areas

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 10, No. 4: 90-105, 2026
DOI: 10.55214/2576-8484.v10i4.12560

and established that the primary question structure effectively facilitated detailed follow-up discussions on issues highlighted by participants [23]. It is important to mention that the individual interviewed in the pilot phase was selected from the same participant pool as our main research study.

3.2. Data Collection

Semi-structured interviews were conducted. Employing the snowball sampling technique, we began with two initial participants from organizations of varying types and sizes. Along with purposive selection, this approach led to the identification of thirteen suitable participants from the Data Management Office. To ensure data validity, coherence, and saturation, we set inclusion criteria requiring all participants to possess significant experience with data governance frameworks. Participants held varied roles and were involved in different aspects of the framework, providing a range of insights crucial for comprehensively addressing the research questions [23].

The study targeted various organizations in KSA, all implementing the data governance framework mandated by NDMO. Participants, as detailed in Table 1, held positions as chief data officers (CDOs), data consultants, or administrators in data management and privacy offices. In semi-structured interview-based research, reaching data saturation often justifies sample size. Following this principle, Francis et al. [24], we found interviewing thirteen individuals sufficient. Interviewing ceased once it was apparent that no further novel insights were emerging. Participation in the study was entirely voluntary, without financial or other incentives. Interviews were conducted on an individual basis, ensuring one-on-one interaction. Individual interviews were chosen as more fitting for the study objectives, allowing for more open and unbiased data collection.

The interview process was conducted remotely using Zoom from March 31 to December 11, 2023. Each session commenced with a brief personal introduction, followed by an explanation of the research purpose and obtaining participant consent. Prior to starting the interview, participants were asked for consent to record the session, which was crucial for accurate transcription. Once consent was given and recording devices were activated, standard qualitative research protocols were adhered to. This included assurances of confidentiality and a description of data and result utilization. No personally identifiable information was captured; responses were anonymized to maintain ethical standards. Participants were native Arabic speakers; therefore, interviews were initially recorded in Arabic, then transcribed in Arabic and subsequently translated into English.

Table 1.
Overview of Participants.

Participant Number	Organization Type	Participants Position
1	Government	CDO
2	Semi- Government	Data Consultant CDO
3	Government	Data Management and Privacy Office Director Data Governance Team Lead
4	Private	legal Consultant
5	Government	Data Management Specialist CDO
6	Private	CDO, Data Governance Team Lead and Data Management Specialist
7	Government	CDO
8	Semi- Government	Data Governance Team Lead CDO
9	Government	
10	Private	
11	Semi- Government	
12	Government	
13	Semi- Government	

3.3. Data Analysis

The study employed a thematic analysis methodology for the examination of interview transcripts. This method is widely recognized for its efficacy in discerning, analyzing, and delineating patterns or themes within datasets, and is apt for interpreting textual data to uncover recurring motifs responding

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 10, No. 4: 90-105, 2026
DOI: 10.55214/2576-8484.v10i4.12560

to the posed research questions [25]. Thematic analysis was deemed particularly suitable for exploring intricate aspects of the research aim, namely, identifying areas needing improvement. The research culminated in proposing a series of recommendations aimed at refining data privacy governance in KSA.

Transcription of interviews from audio to text is a critical step in research methodology. In this study, a thorough verbatim transcription was conducted promptly after each interview to facilitate exhaustive coding analysis of contributions made by each participant. To guarantee accuracy and reliability, each audio recording was repeatedly listened to, ensuring alignment with comprehensive field notes taken during and immediately after interviews. Additionally, a second researcher independently verified the fidelity of transcripts against audio recordings.

The coding process was executed manually, entailing systematic examination of each transcript. This approach drew inspiration from Braun and Clarke [21] and incorporated aspects of Grounded Theory as outlined by Charmaz [26]. The process commenced with initial coding, where a segment-by-segment technique was employed to discern similarities and differences within and across interviews, recognizing emerging patterns and their relevance to the research question. Subsequently, focused coding was undertaken, wherein codes deemed particularly significant were extracted from the initial set [26]. These focused codes were interconnected to form patterns within each interview, offering a concise summary of data while preserving the original meaning of respondents' statements. The next phase involved searching for themes. The coding framework facilitated the identification of themes, defined as consistent patterns emerging from qualitative data analysis. Focused codes were organized into a spreadsheet and scrutinized to pinpoint groups sharing common ideas or meanings, forming sub-themes aggregated into broader categories termed "main themes," further grouped into "major themes" directly related to the research question.

4. Findings and Discussion

This section presents the main findings of this research, which indicate that the implementation of data privacy governance has a significant impact. A comprehensive data governance framework, if existent, will result in high-quality and efficient data, transparency, increased productivity, and reduced data errors. The data governance framework in KSA includes a comprehensive policy for monitoring and regulating data-related activities. The following sections describe the current framework for data governance in KSA, discuss data privacy, illustrate the challenges concerning data privacy governance, and finally, present relevant recommendations.

4.1. Describe the Current Data Governance Framework

Our research findings indicated that the current framework for data governance in KSA is inadequate and requires significant improvement. The existing data governance frameworks were developed to improve data governance or increase data governance maturity using standard and unified frameworks, such as DAMA, DCAM, and CMMI. The Saudi Arabian government is currently adopting the DAMA Data Governance Framework [8], which is considered a comprehensive and integrated data governance framework that facilitates data-driven capabilities, data quality, and data utilization in addition to providing data protection services. This framework is expected to interconnect all data protection and data quality enhancement practices. The framework is primarily concerned with data management, including data privacy and protection considerations. As stated by interviewee 1, "Data privacy intersects with each phase of the data life cycle." The interviews indicated that data governance is an essential aspect of data management because it serves as an overarching framework and encompasses several areas. This framework comprises several areas, namely data governance, data integration and interoperability, data use, classification and availability, and data protection. These areas have been further divided into fifteen disciplines and fall under a number of specifications, standards, controls, and policies. These include data privacy, business intelligence and advanced analytics, machine learning, data operations, data monetization, data value realization, and data integration; data classification; open data; freedom of information; metadata and data catalogs; documents and archives;

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 10, No. 4: 90-105, 2026
DOI: 10.55214/2576-8484.v10i4.12560

data architecture; master data management; and data security, which is the specialty of the Cybersecurity Authority.

Data privacy falls under data protection, which has two aspects. The first aspect is the protection of personal data. The second aspect is data security. In other words, data privacy falls under governance, which includes establishing policies and regulations within the organization, and data sharing and data protection. Data sharing has its own set of special laws to ensure proper handling and protection; the DAMA framework generally does not address personal data specifically; rather, it integrates it within broader themes of governance, participation, and data protection, each having its distinct nature. The selection of an operating model is crucial, as it lays the groundwork for the activation of policies in the second phase. This process requires the application of technical and human resources, including the identification of data owners, data stewards, and data custodians. Once all areas have been completed and policies are activated, change management must be implemented, which involves the distribution of technical and business roles and responsibilities for data.

All interviewees affirmed that the application of the data governance framework conforms to the NDMO framework and is tailored to the needs of each organization. According to interviewee 6, "*The Data Governance Framework encompasses data privacy, but it is still in the implementation phase. Our company has constructed the framework and operating model, but the operation phase has not yet begun.*" Discussions on policies revealed that many organizations, particularly private ones, have made significant strides in governance. Although the ideal governance model may not be fully realized, privacy policies and data classification policies are now more prevalent. As stated by interviewee 4, "*Governance structures exist within the organization; however, they have not yet achieved the optimal configuration envisioned by stakeholders. Nevertheless, current practices demonstrate functional adequacy.*"

4.2. Data Privacy

Based on the interviews with the participants, we arrived at the following findings regarding data privacy in KSA: As noted earlier, data privacy is a critical aspect of data protection that focuses on the strengths and weaknesses of personal data management through the implementation of trustworthy methods in accordance with personal data protection policies and regulations. Data privacy is not only concerned with the security of personal data but is also considered the initial boundary for data protection, which is a fundamental aspect of data management and governance. Managing data privacy and determining an individual's rights and obligations are the most essential and primary aspects of personal data protection, particularly when an organization manages a large volume of personal data, whether internally or externally. Data privacy is also concerned with the integrity, confidentiality, authenticity, and authorization of personal data access, and it establishes the methodologies and standards for protecting sensitive, confidential, and valuable organizational data from unauthorized user access and modification [27].

Data privacy is considered the most important aspect of data management and governance. Compliance with the NDMO requirements is mandatory for all organizations in KSA to ensure the effective enforcement of data privacy. Several laws, regulations, legislation, and principles pertaining to data privacy have been defined and must be enforced in KSA to ensure data privacy, which safeguards the privacy and security of personal and sensitive organizational information. The purpose of these data privacy requirements is to prevent any unauthorized person from within or outside the organization from gaining unauthorized access to data, utilizing data, exchanging it with others, or manipulating this data to damage the country and its citizens [28].

Based on the analysis of the interviews, 40% of the respondents considered data privacy to be essential for both organizational and individual personal data. These two classifications of data, such as individuals' personal data and enterprise data, have distinct data privacy requirements. Individual personal data privacy is primarily focused on ensuring the privacy of a single person with limited requirements and fewer data privacy risks, whereas enterprise data privacy requires a higher level of privacy and security, as it relates to the data privacy of enterprise business processes, including financial

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 10, No. 4: 90-105, 2026
DOI: 10.55214/2576-8484.v10i4.12560

business statements, bids and offers, employees' salaries, and other confidential business information that must be protected and secured.

Organizations view the data privacy policy as an integral part of the data management process and a vital element of data governance. The data privacy policy in these organizations supports the management of personal data privacy and enforces implementation and compliance with data privacy-related laws, regulations, and statutes outlined by national law enforcement agencies. Some organizations in KSA have established data management offices to address data privacy and governance responsibilities, in accordance with government mandates. These organizations have implemented an appropriate data governance framework that encompasses comprehensive and inclusive data management elements, including personal data privacy protection.

As noted above, data privacy is closely associated with data governance, as it enables the monitoring of who and why organizational data is being accessed and helps protect personal data against unauthorized and unauthenticated user access. Furthermore, data privacy can be viewed as the transfer of data control from the data controller to the data subject, where individuals have the discretion to decide whether or not to provide their personal information to organizations. Individuals are aware of the purpose of collecting their data and their rights to view, access, manipulate, obtain a copy of, or request the deletion of their personal information [28].

In addition, data management offices are concerned with personal data, which serves as a means of identifying an individual through various parameter values such as name and ID number. As the interviewees noted, the privacy policy classifies personal data into two categories: non-personally identifiable information (non-PII) and personally identifiable information (PII). Non-PII refers to any personal data that does not identify an individual by their identity, such as a list of employees' age, language, sex, and nationality, as long as it is not linked to their identities. In that case, this is personal data, but according to the existing policy, it is classified as non-personally identifying information. On the other hand, personally identifiable information (PII) encompasses the name, identity, and any other details that reveal one's identity. Accordingly, governance policies manage personal data in accordance with regulations and legislation, while also allowing for its use for purposes such as data analysis and report extraction.

When utilizing the DAMA framework for data sharing, organizations only share data with consent from the data subject. The data is collected solely for its intended purpose, and all data protection provisions outlined in the DAMA data protection standards, including access control and encryption, must be followed in cooperation with cybersecurity employees [8]. Based on interviews with the participants, we concluded that the data classification process is a proactive, step-by-step process that determines whether the data can be shared and made accessible online as open data. This process involves the interconnected triangle of actions composed of data classification, data protection, and data availability.

4.2.1. The Impact of Data Privacy Governance

Data privacy governance, which operates at the organizational level, has far-reaching implications that extend to authorization, data privacy, compliance, and aspects of data reliability, reputation, and quality. It is one of the organization's most critical key performance indicators (KPIs), as a lack of proper data protection can erode consumer confidence and harm the organization's reputation, negatively impacting its operations. However, when a person believes that their data is safe, it fosters trust, which can result in an increased consumer base, return on investment, and income. As stated by interviewee 7, "*following the rules and regulations related to data governance and privacy can help avoid fines.*" Furthermore, effective data governance and privacy practices lead to better risk management, reducing the likelihood of data breaches and violations [29] that may harm the business. Thus, data privacy has a positive impact both externally and internally within the same firm, where employees trust the employer to properly protect their data, and customers entrust the organization with their data because the organization respects their privacy [30].

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 10, No. 4: 90-105, 2026
DOI: 10.55214/2576-8484.v10i4.12560

Many interviewees acknowledged that the existence of many laws may hinder many opportunities, but effective data privacy governance brings a good reputation for the organization, as explained earlier. However, it is not accurate to assume that data privacy laws provide an advantage for organizations. On the contrary, sometimes organizations without strict data privacy laws may benefit more in certain cases. It is worth mentioning that when data is improperly disclosed or compromised, the organization may experience significant consequences in the future. Preserving the rights and reputation of the organization, future opportunities, and customer trust are of utmost importance. Therefore, it is essential to adopt a balanced approach to data privacy. Overemphasizing data privacy may limit innovation, hinder data sharing, and restrict access to open data [31].

4.3. Challenges Concerning Data Privacy Governance

In light of the interview results, some challenges were identified that hindered the implementation of an effective data privacy governance framework within organizations, as shown in Figure 2.

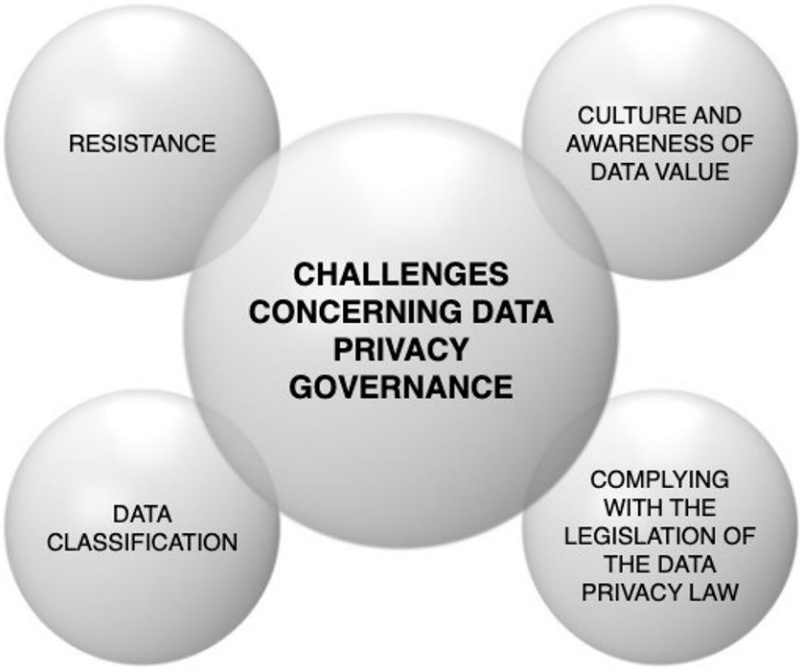

Figure 2.
The challenges concerning data privacy governance.

4.3.1. Culture and Awareness of Data Value

Based on the findings of the interviews, all participants agreed that the awareness and culture required to understand the value and importance of data privacy are common obstacles for any organization that decides to implement its data governance framework. As stated by participant 6, "*The benefit of data governance will be felt in the long term after several years. They are now unaware of it.*" This lack of institutional awareness can result in employees inadvertently disclosing sensitive information to competitors due to a lack of knowledge about the importance of data privacy. Furthermore, a lack of awareness regarding the privacy of personal data may cause individuals to decline to participate in data-sharing initiatives due to concerns about data protection. Data protection does not necessarily equate to non-participation; rather, it involves safeguarding the interests of individuals. Accordingly, they need to be aware of what information is appropriate to share.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 10, No. 4: 90-105, 2026
DOI: 10.55214/2576-8484.v10i4.12560

The responsibility of government agencies is to maintain data and provide services to citizens. Consequently, they are legally mandated to obtain and manage this data. There is also internal legislation through which they regulate participation. However, the problem arises from a lack of knowledge or comprehension of the statutory regulations on the part of the authorities. Moreover, there is a lack of data privacy education within the community.

4.3.2. Complying with the Legislation of the Data Privacy Law

According to the analysis of the interviews, 60% of the respondents said that adhering to the Data Privacy Law's regulations, particularly the European Data Protection Law (GDPR), was challenging. Due to inadequate data privacy practices, major international corporations face numerous financial fines. Large multinational corporations have the capacity to comply with laws and regulations, but the question remains as to whether such compliance will have a positive impact on the organization's financial income. As participant 4 stated, "Paying fines may not constitute a loss against their earnings." Some participants expressed the belief that these corporations may prefer to pay fines rather than comply with legislation that could impede their substantial sources of income. Furthermore, many organizations struggle with implementing data privacy practices due to the disruption it may cause to their business and the potential limitation of benefits. Some organizations that provide services to individuals may violate privacy if they believe it is in the public interest. Accordingly, there is no need to obtain individual consent. Interviewee 6 stated, "For example, we have an artificial intelligence model that predicts the characteristics of diabetes, such as a high blood sugar level of 400. This happens two or three times a week. This leads to poor vision and health problems related to diabetes. These data are recorded and linked using the *My Health* application. After collecting the characteristics of diabetics, this artificial intelligence model accesses the patient's mobile number and starts sending awareness messages such as 'you should check your eyes' and similar preventive messages about complications that are expected to occur to them. This is an explicit example of a violation of privacy because the consent of the customer to whom the messages will be sent has not been obtained".

4.3.3. Data Classification

The majority of participants stated that identifying and inventorying data for organizations is a significant challenge. The focus should be on prioritizing essential and crucial data to achieve strategic aspirations and objectives. If the data is identified well, it will be simple to govern. As Participant 1 stated, "The core or critical data are not yet clear in our organization. If core and critical data are not identified, the program will be impacted." Moreover, according to Participants 1, 2, 3, and 5, organizations' inability to distinguish between data that requires protection and data that does not is still a concern. Participant 3 explained, "We must distinguish between data. What data, if not protected, will harm the organization?" In addition, data management and governance involve dynamic data whose value fluctuates over time, as data is an asset, and the value of assets fluctuates. Therefore, it is crucial to approach data management and governance with a dynamic perspective, recognizing that the value of data can change over time. According to Participant 1, "The first year we see the data as core data, but after one or two years, it may change and become non-core."

4.3.4. Resistance

According to all the interviewees, any new change in the work environment, such as the implementation of new laws and policies, is met with resistance and opposition. The implementation of data governance policies also encounters resistance due to conflicts of interest. The lack of conviction among stakeholders, including senior management and others, regarding the significance and value of data governance results in resistance to all requirements, such as providing the budget for human resources recruitment and modern data governance techniques. Acceptance of data governance and management is a significant obstacle, as they are viewed as unconvincing [32]. Additionally, there are other challenges that impede cooperation with the data management office due to conflicts of interest,

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 10, No. 4: 90-105, 2026
DOI: 10.55214/2576-8484.v10i4.12560

such as acceptance of data management, which would not have been implemented without the government's mandate.

According to Participant 6, "Previously, data privacy was separated from data governance and placed under data security. This practice is not correct. We have changed this idea by placing data privacy with data governance independently in accordance with the Data Governance Policy. We found resistance to implementing this concept. The control of data privacy will be withdrawn from the Information Technology and Security Department, and its policies will be enforced in a more comprehensive and correct manner by the Chief Data Officer. We have encountered resistance in the implementation of policy because of conflicts of interest." Moreover, the implementation of data governance policies is further hindered by the cost of compliance. Previously, data was collected and processed without any restrictions or constraints. As Participant 7 stated, "The organization needs to hire new employees with experience." Subsequently, the implementation of a new framework incurs a significant cost.

Finally, the participants reported various challenges associated with implementing a data governance framework, including the scarcity of specialized human resources in data governance and privacy, as well as the lack of legal personnel with the necessary expertise to create and apply the law accurately. Additionally, when engaging external expertise, organizations cannot verify the qualifications of consultants, as they lack the means to evaluate them. It is worth noting that many government agencies currently view consulting firms as a means to learn from them, and the deficiency of human resources within government agencies is expected to impact the selection of external expertise, along with the high cost of employing external experts.

5. Enhancements and Recommendations

On the basis of the preceding analysis and recommendations by the participants, it has been determined that the data governance framework requires further development and refinement, particularly with respect to data privacy. Below is a list of potential improvements and recommendations.

5.1. Clearly Defining Strategic and Operational Goals

Many organizations still lack a well-defined strategy or plan of action, despite their growing interest and emphasis on implementing a data governance framework. To achieve the desired outcomes from the implementation of a data governance framework, organizations require an appropriate framework and operational model, as indicated by Respondent 2. Organizations need to have a clearly defined purpose and dedicated efforts to carry it out. Having a well-defined strategy and plan of action is also essential. Furthermore, ineffective frameworks were observed in organizations where there was no defined vision and working procedures, making implementation difficult.

As advised by Interviewee 7, "*The primary consideration is to move beyond theoretical frameworks and translate the obligations outlined in this framework into clear working procedures, because it is relatively easy to establish frameworks and policies and enforce them, but difficult to apply them in practice. For example, under the regulatory framework, the disclosure of personal data should only occur in certain circumstances, as outlined in the relevant regulations. The critical challenge involves ensuring that this policy is consistently upheld within the organization.*" This challenge, translating policy obligations into operational procedures, has been identified in recent data governance research as requiring systematic attention to technical system design and implementation architectures [33]. To translate these obligations into the operational framework, there must be defined procedures in place.

Additionally, as interviewee 8 mentioned, *"The framework is comprehensive. We have described what you are required to do, but it lacks guidance on implementation, methods, or how the framework functions. Guidelines are essential to determine how to implement the task."*

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 10, No. 4: 90-105, 2026
DOI: 10.55214/2576-8484.v10i4.12560

It is imperative to clearly delineate both the strategic and operational objectives in order to foster a heightened sense of commitment among employees regarding framework provisions. This can be achieved by implementing specific procedures, internal organizational policies, and guidelines, which will help prevent employees from violating these framework provisions and ensure that the desired outcomes and objectives are achieved.

5.2. Awareness and Development of Resources

Due to a multitude of factors, including the diversity of data quantity and nature, leading to task and job duplication, roles and responsibilities within the data governance framework have not yet been definitively established for all data sources. Consequently, organizations that adopt a data governance framework must establish distinct roles and positions for data governance, with a focus on avoiding redundancy and overlap with other organizational functions and departments. Most interviewees stated that it is challenging to identify all flaws at this stage, as they are currently in the implementation phase, which has not been fully completed. As revealed by some interviewees, despite the ongoing implementation phase, some shortcomings have already been identified, such as a lack of specialists in human resources for applying a data governance framework and a lack of experience. In addition, as noted by Participant 7, "*Privacy awareness among organizations is weak, particularly for organizations that heavily rely on data processing.*"

Due to the aforementioned challenges in implementing a data governance framework, including the need for funding, technical resources, and human resources, it is essential to have professionals with extensive experience in data management and governance oversee the operational model and enforce the corresponding policies. As stated by Interviewee 2, "*One of the requirements is to have specialists in the field who have experience in data management, governance, and data security. These specialists will manage the operating model."* Also, interviewee 3 says, "The requirements include a thorough understanding of organizations, along with their associated data. It is essential to have a team with expertise and capability to implement the relevant policy." In addition, it is pivotal to follow the best practices globally to learn from their experience and follow them in our work.

Furthermore, awareness initiatives, training, and education in the areas of data governance and data privacy are necessary for human resources. Technically, organizations need hardware, software, storage space, a backup strategy, data governance, and protection tools. Additionally, organizations require access control to prevent unauthorized data access. As stated by Participant 1, "We have proposed technical solutions that are essential and regarded as a requirement. The first solution is a data classification management tool since classification is the foundation for managing restricted, sensitive, and other data." Data encryption and effective mechanisms for privacy complaints, as well as a response plan or a solution plan in the event of a data intrusion, are also essential requirements. As stated by interviewee 2, "In general, we have control over access to data, but we do not have a response plan when a data breach occurs, and we do not have data encryption."

In terms of financial requirements, the project must have a budget for purchasing and employing tools that aid in protecting data and the privacy of sensitive data. It is important for these organizations to maintain a well-structured and qualified workforce. They should also foster a culture and raise awareness of the importance of privacy and data security at all levels. The development of solutions should be approached through an iterative development approach. Participant 3 said, "*We strive to find the best solutions because no solutions from past experiences are available.*" Workshops, awareness campaigns, and email campaigns are effective methods to raise awareness of the significance of privacy and data security. Some interviewees even distinguished between two types of awareness: development awareness and security awareness. As mentioned by Interviewee 6, "*The goal is to raise people's awareness, knowledge, and understanding of data and privacy issues. Once that is accomplished, we then begin raising awareness of the security aspect, which is privacy.*"

Regarding technological advancement, it is essential to keep up with the rapid pace of technological development. Cooperation must exist between employees within the organization, and staff members

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 10, No. 4: 90-105, 2026
DOI: 10.55214/2576-8484.v10i4.12560

should be educated and encouraged to pursue industry-specific certifications. Most interviewees in this study believed that staff training would increase cultural awareness among workers and reduce resistance. Thus, prior to initiating data governance, organizations must first fully develop their capabilities and increase awareness within the organization. When the requirements are clearly communicated and the level of awareness is high, the application of the data governance framework and data privacy policies will be greatly facilitated.

5.3. Enhance Data Privacy

While organizations are becoming more focused on implementing data governance frameworks, many still lack a comprehensive understanding of the differences between data privacy and data security, as well as the respective responsibilities of each during implementation. According to interviewee 5, "*It is widely acknowledged that data privacy focuses on the personal data of individuals, whereas data security focuses on the organization's overall data. The challenge we face is how to effectively integrate these two areas in practice.*" Furthermore, interviewee 3 pointed out, "Many organizations fail to differentiate between the duties of a data protection officer and a data management officer." Additionally, privacy was not given much consideration during the design phase. Interviewee 4 remarked, "*As data management professionals or data privacy specialists, we must take a proactive approach in the current period to ensure the strength of data privacy and data management is on par with data protection.*"

Currently, the majority of organizations only address privacy issues after a service has been launched, which is a misstep. Services should be designed from the outset to meet the established initial principles of privacy. According to interviewee 4, "*For example, when developing any information system or service in any organization, security requirements are typically included as technical requirements. I noted a substantial deficiency in that data privacy requirements are often not included in the initial design or launch phases.*" It is crucial that organizations prioritize data privacy and security in the planning and development stages to ensure their frameworks are effective and comprehensive.

Private organizations and government agencies that fail to comply with the European Data Protection Law (GDPR) face severe financial penalties for neglecting data privacy. It is within the capability of these organizations to meet all legal requirements. While the cost of the penalties may seem insignificant in comparison to the revenue generated through targeted advertising and other marketing services that utilize personal information, these organizations run the risk of incurring substantial losses in reputation and customer trust if they choose to settle for fines rather than comply with legislation that may restrict their revenue streams. Failure to adhere to the legislation may have a significantly adverse impact on the organization's ability to regain the trust of its customers [29].

For Saudi Arabia, the methodologies employed by organizations regarding personal data handling deviate from those of notable tech giants such as Facebook, Twitter, or Amazon [18, 34]. It is pivotal to strike a proportional balance between protecting individual privacy and the legitimate interests of requesters, to avoid automatic denials of requests that do not comply with privacy principles. As clarified by interviewee 4, "*The privacy principles outlined in the policies are not absolute requirements that one must adhere to without exception. They must be weighed against other considerations. Sometimes an opportunity may be significant, and it may be governed by the policy in one way or another, but we must be mindful of both the organization and the subject involved.*"

However, we advocate for the incorporation of data privacy at the outset of the project life cycle [35]. To efficiently facilitate change management, as well as the management of processes, tools, and personnel, privacy should be integrated into the project's design phase. It is pivotal to develop a protocol, solutions, and mechanisms to safeguard individual identities while maintaining an acceptable level of data privacy. Furthermore, it is crucial for organizations to distinguish between data security and data privacy.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 10, No. 4: 90-105, 2026
DOI: 10.55214/2576-8484.v10i4.12560

6. Conclusion

This study examined the current state of data governance implementation in the Kingdom of Saudi Arabia, with particular emphasis on data privacy challenges and opportunities. Through qualitative interviews with staff members from various Saudi organizations, the research identified critical challenges that organizations encounter during framework implementation. The findings indicate that organizations must strengthen their data governance frameworks to address persistent challenges in three key areas: clearly defining strategic and operational objectives, enhancing organizational awareness and resource capacity, and improving data privacy practices.

This research represents an initial investigation into data governance framework implementation in Saudi Arabia, specifically addressing data privacy considerations. The findings provide a foundation for future inquiry; however, several limitations should be acknowledged. First, this study focused exclusively on the Saudi Arabian context, limiting the generalizability of findings to other regulatory environments. Second, data collection occurred during the early implementation phase before organizations had achieved operational maturity with their governance frameworks.

Future research should longitudinally examine organizations after completing the implementation phase to assess whether the recommendations presented herein have been effectively adopted and to evaluate their impact on data governance maturity. Additionally, comparative studies extending beyond Saudi Arabia to include diverse regulatory contexts and a broader range of industries would enhance understanding of data governance implementation challenges and best practices across different organizational and cultural settings. Such research would contribute to the development of more universally applicable data governance frameworks while acknowledging context-specific adaptations.

Institutional Review Board Statement:

This study was approved by the institutional review board (Human and Social Research) of King Saud University with the approval code: KSU-26-0067.

Transparency:

The authors confirm that the manuscript is an honest, accurate, and transparent account of the study; that no vital features of the study have been omitted; and that any discrepancies from the study as planned have been explained. This study followed all ethical practices during writing.

Copyright:

References

[1] H. Quan, S. Li, C. Zeng, H. Wei, and J. Hu, "Big data and AI-driven product design: A survey," *Applied Sciences*, vol. 13, no. 16, p. 9433, 2023. https://doi.org/10.3390/app13169433

[2] A. M. Almatrafi and Z. H. Alharbi, "The impact of web analytics tools on the performance of small and medium enterprises," *Engineering, Technology & Applied Science Research*, vol. 13, no. 5, pp. 11753-11762, 2023. https://doi.org/10.48084/etasr.6261

[3] S. Myeong, M. J. Ahn, Y. Kim, S. Chu, and W. Suh, "Government data performance: The roles of technology, government capacity, and globalization through the effects of national innovativeness," *Sustainability*, vol. 13, no. 22, p. 12589, 2021. https://doi.org/10.3390/su132212589

[4] X. Fu, A. Wojak, D. Neagu, M. Ridley, and K. Travis, "Data governance in predictive toxicology: A review," *Journal of Cheminformatics*, vol. 3, no. 1, p. 24, 2011. https://doi.org/10.1186/1758-2946-3-24

[5] P. Dzurenda, S. Ricci, P. Ilgner, L. Malina, and C. Anglès-Tafalla, "Privacy-preserving solution for European Union digital vaccine certificates," *Applied Sciences*, vol. 13, no. 19, p. 10986, 2023. https://doi.org/10.3390/app131910986

[6] B. Otto, "Organizing data governance: Findings from the telecommunications industry and consequences for large service providers," *Communications of the Association for Information Systems*, vol. 29, no. 1, p. 3, 2011. https://doi.org/10.17705/1CAIS.02903

[7] M. Al-Ruithe, E. Benkhelifa, and K. Hameed, "A systematic literature review of data governance and cloud data governance," *Personal and Ubiquitous Computing*, vol. 23, no. 5, pp. 839-859, 2019. https://doi.org/10.1007/s00779-017-1104-3

[8] D. Henderson and S. Earley, *Data administration management association, eds., dama-dmbok: data management body of knowledge*, 2nd ed. Basking Ridge, NJ: Technics Publications, 2017.

[9] M. Al-Ruithe, E. Benkhelifa, and K. Hameed, "Key dimensions for cloud data governance," presented at the IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud) (pp. 379–386). Vienna, Austria: IEEE, 2016.

[10] J. Ladley, *Data governance: How to design, deploy and sustain an effective data governance program*, 2nd ed. London, UK: Academic Press, 2020.

[11] V. Stich, V. Zeller, J. Hicking, and A. Kraut, "Measures for a successful digital transformation of SMEs," *Procedia Cirp*, vol. 93, pp. 286-291, 2020. https://doi.org/10.1016/j.procir.2020.03.023

[12] J. Chen, G. Wu, L. Shen, and Z. Ji, "Differentiated security levels for personal identifiable information in identity management system," *Expert Systems with Applications*, vol. 38, no. 11, pp. 14156-14162, 2011. https://doi.org/10.1016/j.eswa.2011.04.226

[13] H. Y. Kim and J.-S. Cho, "Data governance framework for big data implementation with NPS case analysis in Korea," *Journal of Business and Retail Management Research*, vol. 12, no. 3, pp. 36–46, 2018.

[14] S. Sabeti *et al.*, "Collaborative data governance to support first nations-led overdose surveillance and data analysis in British Columbia, Canada," *International Journal of Indigenous Health*, vol. 16, no. 2, pp. 338–355, 2021. https://doi.org/10.32799/ijih.v16i2.33212

[15] I. Alhassan, D. Sammon, and M. Daly, "Data governance activities: An analysis of the literature," *Journal of Decision Systems*, vol. 25, no. sup1, pp. 64-75, 2016. https://doi.org/10.1080/12460125.2016.1187397

[16] R. Abraham, J. Schneider, and J. Vom Brocke, "Data governance: A conceptual framework, structured review, and research agenda," *International Journal of Information Management*, vol. 49, pp. 424-438, 2019. https://doi.org/10.1016/j.ijinfomgt.2019.07.008

[17] M. Albahar and M. Thanoon, "Privacy regulations in the middle east: challenges & solutions," *International Transaction Journal of Engineering, Management, & Applied Sciences & Technologies*, vol. 13, no. 5, pp. 01-11, 2022. https://doi.org/10.14456/ITJEMAST.2022.101

[18] H. Al-Khalifa, M. Mashaabi, G. Al-Yahya, and R. Alnashwan, "The Saudi privacy policy dataset," *arXiv preprint arXiv:2304.02757*, 2023. https://doi.org/10.48550/arXiv.2304.02757

[19] T. Kunnen, "Data governance in advanced analytics: Opportunities and challenges," M.S. Thesis, Inst. for Computing and Information Sciences, Radboud Univ., Nijmegen, Netherlands, 2022.

[20] D. L. Driscoll, *Introduction to primary research: Observations, surveys, and interviews, in Writing Spaces: Readings on Writing, vol. 2, C. Lowe and P. Zemliansky, Eds.* Anderson, SC: Parlor Press, 2011.

[21] V. Braun and V. Clarke, *Thematic analysis. In H. Cooper (Ed.), APA handbook of research methods in psychology: Research designs: Quantitative, qualitative, neuropsychological, and biological.* Washington, DC: American Psychological Association, 2012.

[22] R. Krueger, *Developing questions for focus groups.* London, UK: Sage, 1998.

[23] J. Ritchie and J. Lewis, *Qualitative research practice: A guide for social science students and researchers.* London, UK: Sage, 2003.

[24] J. J. Francis *et al.*, "What is an adequate sample size? Operationalising data saturation for theory-based interview studies," *Psychology and Health*, vol. 25, no. 10, pp. 1229-1245, 2010. https://doi.org/10.1080/08870440903194015

[25] M. E. Kiger and L. Varpio, "Thematic analysis of qualitative data: AMEE Guide No. 131," *Medical Teacher*, vol. 42, no. 8, pp. 846-854, 2020. https://doi.org/10.1080/0142159X.2020.1755030

[26] K. Charmaz, *Constructing grounded theory: A practical guide through qualitative analysis.* London, UK: Sage, 2006.

[27] P. Voigt and A. Von Dem Bussche, *The EU general data protection regulation (GDPR).* Cham, Switzerland: Springer, 2017.

[28] J. Cusick, *The General Data Protection Regulation (GDPR): What organizations need to know (White paper).* New York: CT Corporation, 2018.

[29] C. Kuner, F. H. Cate, C. Millard, D. J. B. Svantesson, and O. Lynskey, *Risk management in data protection.* Oxford University Press, 2015.

[30] P. Breitbarth, "The impact of GDPR one year on," *Network Security*, vol. 2019, no. 7, pp. 11-13, 2019. https://doi.org/10.1016/S1353-4858(19)30084-4

[31] S. Sirur, J. R. Nurse, and H. Webb, "Are we there yet? Understanding the challenges faced in complying with the General Data Protection Regulation (GDPR)," in *Proceedings of the 2nd International Workshop on Multimedia Privacy and Security*, 2018.

[32] M. Al-Ruithe and E. Benkhelifa, "Analysis and classification of barriers and critical success factors for implementing a cloud data governance strategy," *Procedia Computer Science*, vol. 113, pp. 223-232, 2017. https://doi.org/10.1016/j.procs.2017.08.352

[33] J. Powar, H. Janssen, R. Cloete, and J. Singh, "From policy to practice in data governance and responsible data stewardship: System design for data intermediaries," in *Proceedings of the 2025 ACM Conference on Fairness, Accountability, and Transparency*, 2025.

[34] K. Houser and W. G. Voss, "GDPR: The end of Google and Facebook or a new paradigm in data privacy?," *SSRN Journal*, 2018. https://doi.org/10.2139/ssrn.3212210

[35] M. F. Dennedy, J. Fox, and T. R. Finneran, *The privacy engineer's Manifesto: Getting from policy to code to QA to value.* New York: Apress Open, 2014.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 10, No. 4: 90-105, 2026
DOI: 10.55214/2576-8484.v10i4.12560