General Data Protection Regulation(GDPR) Adoption in Sri Lankan Businesses: A Data Governance Model

2022 2nd International Conference on Advanced Research in Computing (ICARC) | 978-1-6654-0741-0/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICARC54489.2022.9753790

P.A. Indhumini Ranathunga
Department of Industrial Management
Faculty of Science
University of Kelaniya
Sri Lanka
indhumini97@gmail.com

A.P.R. Wickramarachchi
Department of Industrial Management
Faculty of Science
University of Kelaniya
Sri Lanka
ruwan@kln.ac.lk

***Abstract*— For many data-driven businesses, the growing volume and complexity of data demand the use of specialized data protection solutions. The use of personal data resulted in a significant impact on privacy and security. Many countries have passed legislation to protect personal information. GDPR (General Data Protection Regulation) is one of them, and it is very vital for EU data processing companies. Although it does not directly apply to Sri Lanka, it applies to firms that deal with European Union counterparties. Sri Lankan firms must comply with GDPR to avoid losing business with the EU. Even though there has been minimal research into GDPR implementation guidelines it was found that the present resources available for Sri Lankan firms are not adequate. To address the problem, a comprehensive data governance model with multiple steps was developed. The proposed data governance model enables secured data management. Indicators and drivers that must be observed when applying GDPR principles were identified through interviews with industry specialists and a thorough literature review. This study provides a data governance model that data-driven enterprises may use to easily execute compliance.**

Keywords*— *Data Governance, General Data Protection Regulation, Data Privacy, Personal Data.

I. INTRODUCTION

This research focuses on how the European General Data Protection Regulation (Regulation 2016/679) can be adapted to Sri Lankan businesses using a data governance model. The European Union (EU) data protection regulation GDPR was enacted by the European Council in April 2016. But it was entered into force on May 25, 2018. The regulation affects how corporations process and manage personal data while enhancing citizen privacy rights and control. This research will look at the regulation and its core data processing principles, as well as the data protection practices that firms can use to comply with the Regulation. It has been extremely significant due to its scope, the responsibilities it imposes on businesses, and the fact that it is the most significant update to EU data protection legislation in 20 years. Because of the possibility of sanctions, businesses that handle even the tiniest amounts of personal data must exercise caution. Limited research has been conducted in Sri Lanka on this subject area of how organizations have implemented the Regulation.

Due to the constant development in digitization in Sri Lanka, where more and more data is generated, the need for data protection and privacy regulations is becoming more crucial. This research contributes to the field of research by identifying an effective implementation guide for the Regulation's easy adoption in most EU data processing enterprises in Sri Lanka. The purpose of this study is to develop a detailed data governance model that will make it easier to implement the General Data Protection Regulation (GDPR) in businesses that specially deal with EU citizens' data by integrating the seven key data processing principles of GDPR that firms must observe. The goal of this study is to discover the different types of data governance models that are accessible and to rebuild or develop one that meets the GDPR's requirements which will concern the main seven principles of GDPR.

The goals of this study would be to identify existing Data Governance models/frameworks from previous studies, identify GDPR data handling principles, determine the relationship between GDPR data handling principles and Data Governance frameworks, and develop a Data Governance model to support compliance. The major goal is to include the main personal data processing principles into a data governance architecture in order to make GDPR compliance simple for any firm; large or small.

II. BACKGROUND

A. Data Privacy

Initially, the law only provided remedies for bodily harm to life and property. However, as tangible property increased in value, so did the incorporeal rights that arose from it. There was the vast domain of intangible property, which included creative creations, goodwill, trade secrets, and trademarks. Recent discoveries and business activities highlight the next step that must be taken to protect the person and preserve what Judge Cooley refers to as the "right to be left alone" [1].

Instant photography and newspaper business has pierced the sacred boundaries of private and domestic life. The right to privacy establishes the foundation for the right to keep information private. The right of property, on the other hand, only protected the creator's right to any income derived from the publication at the time.

Possessing the right to personal data protection is a fundamental human right. These modern data collection techniques have changed the way organizations speak about privacy. Most data-related concerns, according to [2], are no longer discussed from an individual perspective; instead, conflicts are communicated in a way that affects individuals as a whole. Data security is currently under attack daily. Many worldwide data breaches have occurred, such as the case of Cambridge Analytica, in which a substantial amount of

978-1-6654-0741-0/22/$31.00 ©2022 IEEE

personal data was stolen without the knowledge of the data subjects and utilized in highly illegal ways [3].

Sri Lanka being an eCommerce gateway that conducts business with enterprises all over the world, adhering to important privacy legislation will assist in securing data, thereby gaining clients' trust and establishing commercial connections. Furthermore, the software is a major service sector in Sri Lanka, some of these products may be subject to international privacy legislation, such as the EU's General Data Protection Regulation (GDPR) [3].

B. General Data Protection Regulation (GDPR)

The major purpose of the GDPR is to ensure that personal data is handled equally in both the public and private sectors. GDPR imposes tougher data privacy regulations, allowing people more controllable over their personal information (data subjects). Businesses all around the world have become increasingly concerned about maintaining compliance since the GDPR was implemented, as the EU has imposed fines of up to 4% of annual sales per incident. According to [4] the frequency of breach warnings has increased by 19%, from 287 to 331 per day in prior years. In contrast, Google in France was fined $50 million for its lack of transparency, making it the company with the biggest fine to date. It is important to note that GDPR only applies to personal information.

Wider extraterritorial reach, accountability, privacy by design, data portability, the right to deletion, and reporting of data breaches are the primary topics that every firm should be aware of. Because as [4] depicts data processors are subject to direct obligations and severe fines ranging from 0.5 to 4% of total annual global revenue for not being compliant. The foregoing demonstrates that the GDPR cannot be ignored, and enterprises must take appropriate efforts not just to protect personal data but also to avoid hefty fines GDPR applies to you if you process personal data of European citizens, regardless of whether your company is based in the EU or not. The GDPR does not apply directly to persons outside the EU (third countries); rather, EU counterparties dealing with such persons enforce the legislation. As a result, any non-compliant GDPR counterparties outside the EU will be cut off from the EU counterparty. As a result, the prospect of losing EU commercial partnerships will compel Sri Lankan businesses to comply with GDPR. Until the ministry of digital infrastructure produced a framework for the protection of personal data legislation in May 2019 [5], personal data protection was a non-existent concept in Sri Lanka. However, as of November 2019, this proposed act had not yet reached the legislative bill stage.

Legislation to protect electronic personal information, as well as legislation to secure legal documents, are both critically needed in Sri Lanka. If the Legislature or the Judiciary decides to save legal documents and records electronically in the future, legislation prohibiting illegal access to those documents must be enacted. Sri Lanka's adoption of a comprehensive Data Protection Law is long overdue to facilitate and preserve essential electronic data [6].

C. Data Governance

Data governance, as the name implies, is the process of governing the availability, usability, integrity, and security of data in enterprises. A good data governance architecture safeguards personal information and ensures data consistency and reliability, as well as supporting businesses in meeting compliance requirements. Many studies have discussed various parts of the data governance model, but the study [7] has defined data governance in a different approach of a cross-functional framework for managing data.

Sri Lanka does not have any specific legislation on the protection of the right to privacy and through penal sanctions, the Computer Crime Act addresses matters that involve data that has been unlawfully obtained, the illegal interception of data, and the unauthorized disclosure of information. However, it was obvious during this investigation that Sri Lanka is trailing behind in terms of legislative protection for personal data privacy [5]. Though Sri Lanka has a draft bill on data privacy the provisions of the draft bill will be implemented on the date on which the draft bill is ratified by the Parliament of Sri Lanka, except for Part IV, which deals with the use of personal data to disseminate unsolicited messages. Data is no longer an afterthought in the company; it is now the lifeblood of everything they do [8]. Data governance is a broad notion that encompasses people, processes, strategies, guidelines, and more, and ensures that high standards are maintained throughout the data life cycle which assists in data protection and privacy regulation. Since Sri Lanka lacks such models for data protection, the requirement for a proper model for the implementation preparation phase of the new GDPR standard for businesses would be notable and important for authorities to take appropriate actions.

III. Related Work

The strategy of producing the literature review was structured and topic-centric, according to [7], [9], and [10]. To consolidate the relevant knowledge from peer-reviewed scientific literature and a few practitioner publications, a better explanation of the domain of data governance was required. Expanded the concepts of data governance and the General Data Protection Regulation, as well as synthesized key findings from peer-reviewed academic journals and selected practitioner publications. We followed standard protocol for literature reviews, citing [11] and [12] studies.

As followed in [13] we initiated a keyword search by preventing being biased on well-known authors or publications with a significant number of citations. We discovered "data governance" and "privacy" as search phrases during an early stage of exploring searches. Due to the fact that the terms "data governance" and "privacy" are commonly interchanged, the keyword "GDPR" was used as a search term for the searching process to be more explicit. The databases Research Gate, Emerald Insight, AIS Electronic Library Science, and Science Direct, as well as proceedings from important conferences such as the Americas Conference on Information Systems and the European Data Protection and Privacy Conference, were used.

However, we expanded the scope of our review to include foundational works on data governance and GDPR, as well as publications from industry groups like the International Organization for Standardization (ISO). Fig. 1 shows the methodology used to conduct the systematic literature review. There were a total of 210 hits across all databases as a result of this phase. Following that, a two-step qualitative analysis was conducted. To begin, publications were sorted based on their titles and abstracts, eliminating any that did not address data privacy through data governance or GDPR.

Articles having duplicate content and non-English content were also removed. As a result of this step, the number of hits

was reduced to 148. Secondly, reviewed the remaining 138 papers, excluding journal articles and research on data governance implemented in environments such as the Internet of Things (IoT), cloud platforms, big data, and so on, to focus on environments that process personal data specifically. Finally,125 study resources were examined after dividing them into the following categories: GDPR (38), Data Governance and Data Governance Models (60), Personal Data Protection (19), and Others (8).

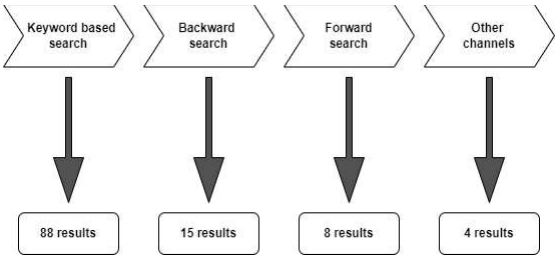

Fig. 1. Literature review search process

A. GDPR Data Processing Principles

The term "personal data processing" refers to any collection of manual or automated procedures of activities that involve personal data. Personal data collection, structure, storage, manipulation, usage, and distribution are examples of such activities. [14]. Under GDPR personal data must be processed following the Regulation's seven data protection principles [14]. The following principles apply lawfulness, fairness, and transparency; limitation purpose; data minimization; accuracy; storage limitation; integrity and confidentiality; accountability. The controller is in charge of demonstrating that all seven principles have been followed.

The data subject must be fully informed about the data processing procedures for it to be legitimate. The legal bases for processing personal data are as follows: consent, legal obligation, vital interests, public task, and legitimate interests are all terms that are described.

Purpose limitation introduces processing limits. Even if the processing purpose is supported by the Regulation's approved purposes for processing, failure to define the purpose of data processing before the commencement of processing will result in the illegal data processing. As a result, businesses must keep track of the content of their privacy policies and ensure that it is updated if data gathered is used for purposes other than those indicated above [14]. The data minimization principle tries to decrease unnecessary data. Personal data processing must be suitable, relevant, and confined to its intended purposes [15]. Organizations must create systems and processes that make it easier to provide sufficient data minimization proof to comply [14]. Personal information accuracy is determined by criteria such as accuracy, completeness, and reliability. Incorrect personal data must be corrected or destroyed as soon as feasible by the data controller [14]. Storage limitation is when personally identifiable information is no longer required, it must be removed or encrypted as soon as possible. Pseudonymization is a method of separating the data subject's identity from the data itself. It's not a good strategy for companies who don't have the means to reverse pseudonymization, which could be required in some investigations [14]. Integrity and confidentiality are managing personal data in a way taking integrity, confidentiality, and security into consideration. Organizations that collect data must keep data safe from manipulation and falling into the wrong hands. The organizations might also think about getting official certification, such as ISO 27001, to show their commitment to cyber security [14].

B. Data Governance Models

Many studies have discussed various parts of the data governance model, but one study [7] has defined data governance in a different approach to managing data in a cross-functional framework. As a result, data governance establishes decision rights and accountability for an organization's data decision-making. Data governance also formalizes and monitors data policies, procedures, and standards. Data governance, according to [7] facilitates six major areas. Specifies what data decisions must be made, how they must be made, and who in the organization has the authority to make these decisions, data governance creates data policies, procedures, and standards, and keeps track of compliance. When analyzing the definition provided by [7], it is clear that having a data governance model as guidance when creating a model is a much more appropriate approach.

When looking back at previous research, it was evident that many researchers attempted to implement data privacy in real-world companies to address the ongoing data privacy challenges. A study was carried out to investigate whether Sri Lanka has a proper legal framework in place to ensure the privacy of electronic health records [16]. Bank of Finland has a traditional data governance model that has comparable issues; however, in their research, they incorporated data privacy ideas and identify business concerns to create a proper data governance framework [17].

Even though there is a limitation of scholarly literature on data governance, the existing material helped us in understanding the concept of a data governance model. Though there exist data governance models related to accountability, accuracy areas, the proposed model considers personal data privacy. The research of [7], [17], [18] has focused on implementing data privacy through a data governance model and mentions a data governance model as a strategy for overall data openness and utilization. Data governance necessitates a framework that provides data collecting tactics and processing approaches. When it comes to data governance models/frameworks, there are several options available, each with different data management areas such as data quality management [19] models developed for private firms such as [17], and models developed for third-generation platforms [19].

An overview of the literature review on data governance models is shown in Table 1, along with the elements we identified in the available data governance models that match with the GDPR principles.

TABLE 1. Overview of the literature

References	Factor Evaluation	
	Factors considered	***Factors aligned with GDPR data processing principles.***
[2]	Data consistency, data integrity, and security, accountability	Integrity and confidentiality Accountability

References	Factor Evaluation	
	Factors considered	*Factors aligned with GDPR data processing principles.*
[20]	Data integrity, proper data storage, and data transparency	Integrity and confidentiality Storage limitation Lawfulness
[7]	Accountability, data retention requirements, data ownership, information accuracy, data storage for effective data management, data security, policies, standards and procedures regarding data storage, data retention and archival, data confidentiality, and integrity	Accountability Storage limitation Accuracy Purpose limitation Lawfulness
[21]	Data security and risks management, data lifecycle management, storage of information, and its specifications	Integrity and confidentiality Data minimization Storage limitation
[22]	Locus of accountability, confidentiality, integrity and availability of data, optimal storage media	Accountability Integrity and confidentiality Storage limitation
[23]	Privacy by data minimization: anonymity, unlikability, unobservability, and pseudonymity	Data minimization Transparency Integrity and confidentiality
[24]	Data transparency, differential privacy, data provenance, data pre-processing, data cleaning, integration, querying, and ranking, fault tolerance, and recoverability	Transparency, Integrity, and confidentiality

There have also been technical attempts to protect data privacy through investment regarding digital databases in Sri Lanka, the research[25] suggests a digital database protection system. It is concerned with getting content verification or presentation in digital databases using data mining methods, which use computer programs to establish meaningful and usable data patterns. The GDPR offers a challenge for businesses since it places rigorous restrictions on how they handle personal data and stipulates severe penalties in the event of a breach, including legal and monetary penalties. As a result, when creating such a system, it is critical to consider privacy from a social standpoint. Based on a socio-technical approach comprised of a modeling language and a reasoning framework, the study [26] provides a way to assist in the design of GDPR compliant systems.

IV. METHDOLOGY

This study is conducted to bridge the gap in Sri Lankan organizations' GDPR compliance due to the lack of a comprehensive data governance strategy. A qualitative strategy will be used in this study, which will include both a systematic literature review and interviews. This study's research technique is broken down into three distinct sections.

A. Systematic Literature Review

As stated in the related work section, the first step was to conduct a literature review to determine the relevance of existing data governance material, as well as existing and suggested approaches based on the most recent research papers (1997-2021). Variables related to GDPR, and data governance are operationalized using the data acquired to make the interviews and additional research easier.

B. Conceptual Model Development

Following that, the paper provides a conceptual model for data governance, highlighting the stages of data management as well as the essential areas that a business should focus on while adopting GDPR.

C. Interviews

To analyze and validate the conceptual model, interviews with industry experts on GDPR implementation were conducted.

V. DATA COLLECTION

The data for this study were collected in two ways: primary and secondary. Interviews would be the major source of data, but to get to that point, secondary data gathering must be conducted. To establish the study's background and operationalize the variables, secondary data is collected from prior studies in the same field, as well as research publications, journals, and books, as shown in Table 2.

TABLE II. Operationalization table

No	Indicators Evaluation	
	Variables	*Indicators*
1	Transparency	Notice Awareness Choice or consent
2	Accuracy	Data Review Automating error detection reports Accuracy standards Avoiding overloading - data entry team perspective
3	Integrity & Confidentiality	Pseudonymization and Encryption Data consistency Security and enforcement
4	Data Minimalization	Adequate Relevant Inventorying Limited
5	Accountability	Proper responsibility division Adequate documentation
6	Storage Limitation	Data retention requirement - the purpose Defining the data retention period Periodic review for erasing or anonymizing unwanted data Relevant industry standards or guidelines
7	Purpose Limitation	Purpose Specific Legitimate

One of the most used qualitative research approaches is interviews [27]. Interviews are conducted to gather information and learn individuals' viewpoints on a phenomenon. A series of interview questions was constructed after the operationalization of the study's variables.

Due to GDPR's limited experience among employees, it was necessary to filter out those who were most familiar with the concept. Since the goal of the study is to see how different IT businesses have implemented the Regulation, Chief Information Officers of European-Union-based companies were contacted and asked to recommend individuals from their own company who was well-versed in the GDPR and willing to be interviewed. As a result, DPOs (Data Protection Officers), information security officers, the Chief Information Officer, and the heads of enterprise data center were suggested. Six interviews were conducted targeting information security specialists employed in Sri Lankan IT companies that are GDPR compliant or are in the process of becoming GDPR compliant. Thematic analysis is employed

in this study through rigorous coding and analysis to uncover new indicators that were not discovered during the systematic literature review.

VI. Results and Discussion

Based on the findings of the literature review, a conceptual model for data management is developed, which incorporates the seven GDPR principles. Using the [7] and [28] models as a foundation, a conceptual model. Fig. 2 is built by removing a few organizational characteristics identified as antecedents and incorporating the data management stages identified by [7] and [28]. This study is being conducted to bridge the gap in Sri Lankan organizations' GDPR compliance due to the lack of a comprehensive data governance strategy.

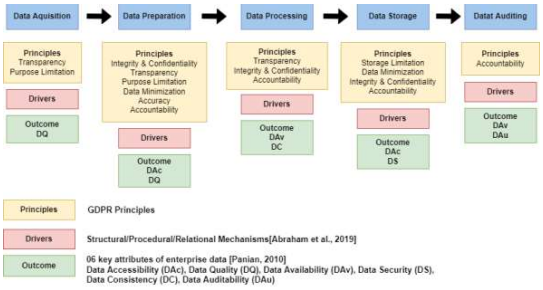

Fig. 2. Conceptual Data Governance model

As depicted in Fig. 2., structural, procedural, and relational mechanisms are the driving forces for GDPR implementation.

Structural Mechanisms (SM): Governance Bodies, accountabilities which include duties and obligations are defined by structured mechanisms.

Procedural Mechanisms (PM): Policies and standards, processes and procedures, compliance management. According to the procedural governance system, data should be consistently captured, securely stored, effectively utilized, and correctly shared along with data policies and standards.

Relational Mechanisms (RM): Training, communication, and coordination. Stakeholder collaboration is made easier via relational governance systems. Training programs ensure that all stakeholders, particularly employees, have the information and certifications they need to assist in the implementation of data governance.

Under data management, stages on how personal data is handled from the point it's been collected to the point it's been discarded were identified; data acquisition, data preparation, data processing, data storage, and data auditing. Enterprise data has six main qualities as depicted by the research [28]. It was used as a foundation for the proposed conceptual data governance model. The six critical properties of enterprise data are data accessibility, data quality, data availability, data security, data consistency, and data auditability.

During interviews with professionals in the sector, the model was validated. It was validated in conjunction with their insights about the techniques they've used to incorporate GDPR principles into the data management process. They were given the conceptual model and asked to conceptualize it before commenting on the add-ons and deposing. We were able to identify a few key practices and recommendations of firms when it came to GDPR adoption and maintenance from the interviews we performed.

1. Using a RACI (Responsible, Accountable, Consulted, and Informed.) matrix to define the data Processor's role, responsibilities, and liabilities in the workflow.
2. Since local departments interact with members' data, questions over ownership of the data have arisen. Additional emphasis on data subjects' rights, particularly when collecting personal data via online forms, by asking a few more questions about consent for how the organization may use their data.
3. Maintaining an orchestration dashboard that provides visibility into resource usage, consumption, and perspective to the customer.
4. Maintaining environments in compliance with GDPR (General Data Protection Regulation), ISO (International Organization for Standardization), NIST (National Institute of Standards and Technology), and HIPAA (Health Insurance Portability and Accountability Act), which assure customers over their data.
5. When using new systems and processes, an introductory assessment scheme is used that includes short questions about whether the system will handle personal data and how sensitive it will be.
6. To achieve compliance with the Regulation, the organization has a data protection plan and a data protection closure, both of which are updated and reported to management and the executive committee on an annual basis.
7. It was suggested that an independent national authority be established in Sri Lanka to monitor and access legal concerns relating to individual data protection offline and online, with easy contact and rapid management of privacy breaches with sufficient legal and technical understanding.
8. Design of GDPR-compliant systems that use technical approaches like artificial intelligence, machine learning, and data analytics to detect data breaches, human errors, and assess what data is required for a certain purpose to limit data minimization.

VII. Recommendation

The GDPR is still being implemented in Sri Lanka, and this study aims to make the process easier for data-driven businesses. The research proposed a new data governance model for the efficient adoption and implementation of GDPR in the IT business. A strategy for organizational change, as well as a budgeted timeline, are also required. It will take time to put the plan into action. Switching from one operating model to another will likely take several years.

VIII. Conclusion

The features and structure of the proposed data governance model are shown in the above study. This concept can serve as a foundation for the industry's GDPR implementation. To simulate the information flow and proper management of personal data, the study summarizes the types of prerequisites, procedures, processes that are necessary.

By adhering to the model requirements in data management, this model will be tested in the future with Data Protection Officers and relevant professionals. Since most IT

firms do not go through the whole data governance process as described in the data governance model, the entire model will not be tested. More indicators on how each concept could be implemented into the data governance model are also expected to be gathered through more interviews. All of these factors can be incorporated into a data governance model to make it easier for an organization to become GDPR compliant. Organizations might either embrace the model or utilize it as a direction for their compliance implementation by doing a gap analysis with their current governance model. More research into how firms align themselves with data protection and their data protection agility could be conducted based on the findings and limitations of this study.

REFERENCES

[1] S. D. Warren and L. D. Brandeis, "The Right to Privacy," Harvard Law Review, vol. 4, no. 5, pp. 193–220, Dec. 1890, doi: 10.2307/1321160.

[2] S. Gutwirth, Y. Poullet, P. De Hert, C. de Terwangne, and S. Nouwt, Eds., Reinventing Data Protection? Dordrecht: Springer Netherlands, 2009.

[3] N. Senaratne, "talkingeconomics - The Growing Need for Privacy and Data Protection in Sri Lanka." www.ips.lk, Jan. 13, 2020. [Online]. Available: https://www.ips.lk/talkingeconomics/2020/01/13/the-growing need-for-privacy-and data-protection-in-Sri-Lanka. [Accessed: August 26, 2021].

[4] M. Goddard, "The EU General Data Protection Regulation (GDPR): European Regulation That Has a Global Impact," International Journal of Market Research, vol. 59, no. 6, pp. 703–705, Nov. 2017, doi: 10.2501/ijmr-2017-050.

[5] S. Manjula and P. Nadine, "Sri Lanka - Data Protection Overview," DataGuidance, Nov. 22, 2019. [Online]. Available: https://www.dataguidance.com/notes/sri-lanka-data-protection-overview. [Accessed: Oct. 06, 2021].

[6] V. Singh, "Comparing The Sri Lankan Personal Data Protection Bill, 2019 And The GDPR - Privacy - India," www.mondaq.com, June 22, 2020. [Online]. Available: https://www.mondaq.com/india/data-protection/956530/comparing-the-sri-lankan personal-data-protection-bill-2019-and-the-gdpr. [Accessed: August 27, 2021].

[7] 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, Dec. 2019, doi: 10.1016/j.ijinfomgt.2019.07.008. [Accessed: Oct. 05, 2021].

[8] O. Hinkle, "Three Ways Organizations Can Achieve Data Governance Success," DATAVERSITY, Mar. 23, 2020. https://www.dataversity.net/three-ways-organizations-can-achieve-data-governance-success. [Accessed: Oct. 25, 2021].

[9] P. K. Senyo, K. Liu, and J. Effah, "Digital business ecosystem: Literature review and a framework for future research," International Journal of Information Management, vol. 47, pp. 52–64, Aug. 2019, doi: 10.1016/j.ijinfomgt.2019.01.002.

[10] S. Kalhoro, M. Rehman, V. Ponnusamy, and F. B. Shaikh, "Extracting Key Factors of Cyber Hygiene Behaviour Among Software Engineers: A Systematic Literature Review," IEEE Access, vol. 9, pp. 99339–99363, 2021, doi: 10.1109/ACCESS.2021.3097144.

[11] T. Zorn and N. Campbell, "Improving The Writing Of Literature Reviews Through A Literature Integration Exercise," Business Communication Quarterly, vol. 69, no. 2, pp. 172–183, Jun. 2006, doi: 10.1177/1080569906287960.

[12] F. Rowe, "What literature review is not: diversity, boundaries and recommendations," European Journal of Information Systems, vol. 23, no. 3, pp. 241–255, May 2014, doi: 10.1057/ejis.2014.7.

[13] A.-S. T. Olanrewaju, M. A. Hossain, N. Whiteside, and P. Mercieca, "Social media and entrepreneurship research: A literature review," International Journal of Information Management, vol. 50, pp. 90–110, Feb. 2020, doi: 10.1016/j.ijinfomgt.2019.05.011.

[14] IT Governance (Organization). Privacy Team, EU General Data Protection Regulation (GDPR) : an implementation and compliance guide, 4th ed. Itgp, 2020.

[15] Information Commissioner's Office, "Guide to the General Data Protection Regulation (GDPR)," ico.org.uk, Mar. 07, 2019. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/. [Accessed: Oct. 05, 2021].

[16] Sapukotana, Upeksha Madukalpani, "Health Information Privacy and Right to Information A case study of India and Sri Lanka," Kdu.ac.lk, 2017, doi: http://ir.kdu.ac.lk/handle/345/1678.

[17] J. Paananen, "A New Data Governance Model for the Bank of Finland," MSc Dissertation, Metropolia University of Applied Sciences, Finland, 2020.

[18] H. Yeong Kim and J. - Suh Cho, "Data governance framework for big data implementation with NPS Case Analysis in Korea," Journal of Business & Retail Management Research, vol. 12, no. 03, Apr. 2018, doi: 10.24052/jbrmr/v12is03/art-04.

[19] K. Wende, "A Model for Data Governance – Organising Accountabilities for Data Quality Management," ACIS 2007 Proceedings, Jan. 2007. [Online]. Available: https://aisel.aisnet.org/acis2007/80. [Accessed: Oct. 05, 2021].

[20] M. Al-Ruithe, E. Benkhelifa, and K. Hameed, "A Conceptual Framework for Designing Data Governance for Cloud Computing," Procedia Computer Science, vol. 94, pp. 160–167, 2016, doi: 10.1016/j.procs.2016.08.025.

[21] J. Yebenes and M. Zorrilla, "Towards a Data Governance Framework for Third Generation Platforms," Procedia Computer Science, vol. 151, pp. 614–621, 2019, doi: 10.1016/j.procs.2019.04.082.

[22] V. Khatri and C. V. Brown, "Designing data governance," Communications of the ACM, vol. 53, no. 1, p. 148, Jan. 2010, doi: 10.1145/1629175.1629210.

[23] A. Pfitzmann, M. Hansen, T. Dresden, and U. Kiel, "A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management," 2009. [Online]. Available: http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.32.pdf. [Accessed: Oct. 11, 2021].

[24] S. Abiteboul and J. Stoyanovich, "Transparency, Fairness, Data Protection, Neutrality," Journal of Data and Information Quality, vol. 11, no. 3, pp. 1–9, Jul. 2019, doi: 10.1145/3310231.

[25] T. B. Abeysekara, "A Proposal for the Protection of Digital Databases in Sri Lanka," ore.exeter.ac.uk, Jul. 2013. [Online]. Available: http://hdl.handle.net/10871/14172. [Accessed: Oct. 10, 2021].

[26] M. Robol, M. Salnitri, and P. Giorgini, "Toward GDPR-Compliant Socio-Technical Systems: Modeling Language and Reasoning Framework," Lecture Notes in Business Information Processing, pp. 236–250, 2017, doi: 10.1007/978-3-319-70241-4_16.

[27] A. Bryman and E. Bell, Business Research Methods, 3rd ed. London, England: Oxford University Press, 2011.

[28] Panian Zeljko. "Some Practical Experiences in Data Governance," World Academy of Science, Engineering and Technology, 2010.