Designing a Data Governance Model to Implement GDPR in Sri Lankan Enterprises

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

Dr.Ruwan Wickramarachchi
Senior Lecturer, Department of Industrial Management,
Faculty of Science, University of Kelaniya,
Sri Lanka
ruwan@kln.ac.lk

Abstract

The volume and complexity of data have expanded while demanding the need for specialized data protection solutions for many data-driven enterprises. Personal data is the internet's new oil and the digital world's new currency, has a big impact on privacy and security. Various laws have been implemented in many nations to protect people's personal information. One of them is GDPR (General Data Protection Regulation), which is particularly relevant for EU data processing businesses. Though it does not apply directly to Sri Lanka, it is directly applied to European Union counterparties. To avoid losing business with the EU, Sri Lanka must also comply with GDPR. Although there aren't many resources for GDPR implementation guidance, the existing ones are not very comprehensive. To resolve the issue, we went through a series of processes to construct a comprehensive model, after which we were able to develop a data governance model to deploy. The data governance model provides extensive direction for data management. We established the indicators and drivers that must be observed while applying the GDPR principles through interviews with industry professionals and completing an extensive literature study. A data governance model is provided in this study for data-driven organizations to simply implement compliance.

Keywords

Data Governance, General Data Protection Regulation, Data Privacy, Personal Data.

1. Introduction

This is a study about the European General Data Protection Regulation (Regulation 2016/679) and how it can be adapted to Sri Lankan enterprises easily in means of a data governance model. The General Data Protection Regulation (hereafter referred to as the Regulation or the GDPR) is a European Union regulation that governs data protection (EU). The European Council enacted the Regulation in April 2016 and it went into effect on May 25, 2018. The Regulation has an impact on how businesses process and manage personal data, as well as increasing citizen privacy rights and control. This study will address the Regulation and its data processing principles along with the data protection procedures the businesses could adhere to for Regulation's implementation. The Regulation received a lot of attention from the general public at the beginning of 2018. As the deadline for compliance approached, millions of businesses and organizations sent e-mails to their consumers and clients alerting them that their privacy policies had been revised to comply with the Regulation. Following the Regulation's implementation, websites hosted outside of the EU were temporarily prohibited from accessing IP addresses in the EU. The websites were non-compliant with the Regulation, and the website owners did not want to risk being sanctioned. Whether or not they are aware of the Regulation, they will be impacted by it during the implementation period. Whether or not aware of the Regulation, users were almost certain to be affected by it throughout the implementation period, especially if you used digital

services. The Regulation has generated interest due to its size, the demands it places on businesses, and the fact that it is the most major change in EU data protection policy in 20 years. Data collection organizations could not avoid implementing the Regulation without risking sanctions and unfavorable publicity. The possibility of sanctions necessitates care on the part of firms that handle even the tiniest sets of personal data. The Regulation does not distinguish between enterprises; the clearest distinction is made between them based on the number of employees and the data processing features. Small and medium-sized businesses must also be aware of the Regulation, and in some situations, to a significant level. There has been little research on how organizations have implemented the Regulation. Sri Lanka is being subjected to the continuous rise in digitalization where more and more data is generated, the need for data protection and privacy laws heightens timely. As a result, this study is motivated because it will contribute to the research arena of discovering an appropriate implementation guide for easy implementation of the Regulation in most EU data processing firms in Sri Lanka. The purpose of this study is to develop a precise data governance model for easy implementation of the General Data Protection Regulation (GDPR) in organizations that deal with EU citizens' personal information.

The study begins by defining the terms personal data and data protection, as well as covering the history of data protection. The research continues with a broad overview of the Regulation as well as a discussion of its major definitions and features. The Regulation then goes on to explain the seven key data processing principles that must be followed by companies.

The focus of this research is to identify the types of data governance models available and to redesign or build a model that helps in fulfilling the requirements of GDPR. In this study, we would only consider GDPR principles related to the data handling process. The proposed model will make it more convenient and easier for not only organizations but many other small enterprises with even little legal knowledge in complying with their businesses with GDPR. Though GDPR is EU-based compliance and is not directly enforced on countries outside the EU, the authorities shall enforce the law on counterparties including third-party countries involved with those counterparties as well. Since the majority of Sri Lankan corporates are dealing with the personal data of EU residents, it shall be required to comply with GDPR. The objectives of this research would be identifying the available Data Governance models/frameworks available in past studies, identifying GDPR principles which concern data handling, determining the relationship between data handling principles of GDPR and Data Governance frameworks, developing a Data Governance model to support compliance data handling principles of the GDPR. Identifying the data governance models available in past research papers and as well as the existing following data governance models in industries will be considered when designing the final model. The main aim is to integrate the main personal data processing principles into a data governance model to make it easy for any kind of organization to be GDPR compliant, no matter whether it a large or small.

2. Literature Review

According Abraham et al. (2019), Senyo et al. 2019 and Kalhoro et al. (2021) our method of writing the literature review was structured and topic-centric, similar to that of other existing literature reviews. We wanted to better explain the domain of data governance and consolidate the relevant knowledge from peer-reviewed scholarly literature and a few practitioner publications. We wanted to further define the areas of data governance and General Data Protection Regulation and synthesis important knowledge from peer-reviewed scholarly literature and chosen practitioner publications. We used standard practices for literature reviews in doing so (Zorn et al. 2006), (Rowe 2014) referring to this research.

We began by conducting a keyword-based search (Olanrewaju et al. 2020), (Ismagilova et al. 2019). By employing a keyword-based search, we were able to avoid focusing on well-known authors or articles with a large number of citations, which helped us avoid bias. During an early step of probing searches, we noticed "data governance" and "privacy" as search phrases. Because the phrases "data governance" and "privacy" are frequently interchanged and then we included "GDPR" to be more specific as a search phrase. We used the Emerald Insight and Science Direct, AIS Electronic Library, Research Gate databases which contain peer-reviewed IS journals as well as proceedings from major conferences such as the European Conference on Information Systems, the Americas Conference on Information Systems, and the European Data Protection and Privacy Conference, to name a few. Because new research may not have been published in journals yet, or may never be, we included conference papers.

We did, however, widen the scope of our assessment to include fundamental works on data governance and GDPR, as well as publications from industry organizations such as the International Organization for Standardization (ISO) and GDPR publications from the European Union. We conducted our systematic literature review in the format depicted in the Figure 1. We were able to obtain a comprehensive view of data governance and the application of GDPR in organizations and remove systemic biases by just selecting a set of scientific publications and conference papers. Finally, we looked at a total of 125 research materials under the categories GDPR (38), Data Governance and Data Governance models (60), personal data protection (19), and others (8) after going through keyword-based search, backward search, forward search and through other channels as well.

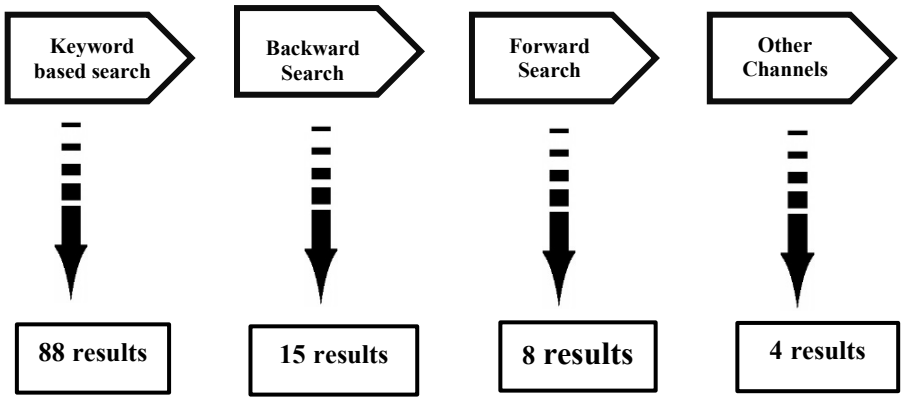

Figure 1: Literature Review Search Process

2.1 Personal Data Protection

It's a fundamental human right of having the right to the protection of personal data. Personal rights take a prominent place in the current society and that is rights and freedoms directly related to an individual itself. In the Personal Data Protection Act Personal Data is defined as "Personal data means any information relating to an identified or identifiable natural person (hereinafter: data subject); an identifiable person can be identified, directly or indirectly, in particular by reference to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity". Apart from the general personal data, there are other special categories of data: political opinions, trade union membership, religious beliefs, health or sex life, and personal data on criminal procedure. Personal data not only data exists in public documents it may: first name, last name, address, email address, GPS location, photographs, telephone number, IP/MAC computer address, biometric data, information about education videos, Radio Fidelity Identification (RFID) tags, bank account details, information about credit debt. There is an accelerated consciousness of the significance of data protection, not only the protection of the non-public lives of people but their freedom as well. The concept of privacy is evasive and ill-defined information has been defined as an aspect of withholding and concealment of information. These contemporary methods of data collection have altered the privacy discussions in companies.

According to Rodot`a (2009) now most data-related issues are not discussed from an individual point of view, conflicts are expressed in a way as a whole affecting people. For example, intensive retrieval of personal data by virtual data providers and handlers like taxpayers, taxi drivers, patients, bankers, employees, etc. Secondly, he has further mentioned that smart cards, images, and videos in social media activities have paved the way for quick records, reconstructing individual behaviors in minute detail. Currently, data protection is under attack every day. There have been many international cases of data breaches for example the case was the Cambridge Analytica where a large amount of personal data was harvested without the consent of the data subjects and been used in very illegal and unethical ways for profiling and sales targeting purposes (Senaratne 2020). Sri Lanka will have 10.10 million internet users by January 2020, according to Sri Lanka from Data Reported on Global Digital Insights in 2020, data with a 47 percent internet penetration rate. With the current pandemic problem and the growth of e-government services, where

the possibility of fraud and identity theft may be discovered, data protection has become increasingly important. Because Sri Lanka is an eCommerce gateway that does business with organizations all over the world, following important privacy legislation would help secure data, which would help win clients' trust and create commercial relationships. Furthermore, because software is a key service sector in Sri Lanka, some of these goods may be subject to international privacy legislation, such as the EU's GDPR, (Senaratne et al. 2020).

2.2 General Data Protection Regulation (GDPR) Principles.

The GDPR's main purpose is to ensure that personal data is handled properly in both the public and private sectors. The GDPR's primary goal is to ensure that personal data is processed fairly in both the public and private sectors (Comparing the Sri Lankan Personal Data Protection Bill 2019). GDPR contains stricter data protection standards, giving individuals more control over their data (data subjects). Since the adoption of the GDPR businesses all over the world have become increasingly worried about ensuring compliance, as the EU has imposed fines of up to 4% of annual sales per incident. According to DLA Piper's 2021 research, there has been a 19 percent increase in the number of breach warnings, up from 287 to 331 per day in previous years. Whereas, in France, Google was fined $50 million for lack of openness, making it the firm with the largest sanction to date.

It should be clear that the application of GDPR is referred to personal data only. Under the new EU data protection legislation, there have been introduced several novelties. The main areas every organization should be aware of are wider extraterritorial reach, accountability, privacy by design, data portability, and the right to erasure were all established as new concepts and rights, notification of data breaches is required. (Within the next 72 hours.), modifications in the acquisition and use of personal information. For example, consent that is unequivocal or explicit, Data processors are subject to direct obligations, more severe fines, ranging from 0.5 to 4% of total global yearly revenue, a more uniform data protection regime across the EU, appointing data protection officer (DPO). The above highlights the fact that the GDPR cannot be ignored, and businesses must take adequate precautions not just to protect personal data but also to avoid huge fines.

If you process personal data in the context of an EU-based organization, regardless of whether you treat personal data in the EU or not, the GDPR applies to you. If you process personal data in the context of an EU-based organization, regardless of whether you treat personal data in the EU or not, the GDPR applies to you. With these and other extraterritorial legislation, the question of how a foreign government or authority has jurisdiction over Sri Lanka and how they implement such laws is a recurring concern. The GDPR does not apply directly to persons outside the EU (third countries); rather, the regulation is enforced by EU counterparties interacting with such persons. As a result, any GDPR non-compliant counterparties outside of the EU will be cut off from the EU counterparty. As a result, the threat of losing EU commercial partnerships will push Sri Lankan corporations to comply with GDPR. Personal data protection was a non-existent concept in Sri Lanka until the ministry of digital infrastructure developed a framework for the protection of personal data act in May 2019. This proposed act, however, had not yet reached the parliamentary bill stage as of November 2019. Sri Lanka urgently needs legislation to protect electronic personal information, as well as legislation to secure legal documents if and when the legislature decides to save them online. If the Legislature or the Judiciary decides to retain legal documents and records electronically in the future, legislation must be passed to prohibit unauthorized access to those documents. As a result, the passage of a comprehensive Data Protection Law in Sri Lanka is long overdue to facilitate and preserve important electronic data (Singh 2020).

2.3 Data Governance Models.

Data governance (DG) is the process of regulating the availability, usefulness, integrity, and security of data in businesses, as the name suggests. Another component of data governance is the protection of firm customer private data, which is a top issue for businesses. A successful data governance model protects personal data and guarantees that data is consistent and reliable, as well as assisting enterprises in adhering to compliance standards. We couldn't discover a consistent definition of data governance in either the academic or practitioner literature. As a result, we looked at every description of data governance in our collection of papers and utilized open coding to uncover commonalities. Many research was talking about various aspects of the data governance model but in the research (Abraham et al. 2019), they have come up with a definition; Data governance specifies a cross-functional framework for managing data as a strategic enterprise asset. In doing so, data governance specifies decision rights and accountabilities for an organization’s decision-making about its data. Furthermore, data governance formalizes data policies, standards, and procedures and monitors compliance. As mentioned in Abraham et al. (2019) data governance

facilitates key six areas. Facilitates communication across functional departments and data domains, provides data management with structure and formalization, emphasizes data as a significant business asset, establishes 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, keeps track of compliance.

It's all about data management when it comes to GDPR implementation. Data must be managed properly from the time it is gathered until it is deleted when the purpose has expired, adhering to the principles of transparency, accountability, integrity, purpose limitation, storage limitation, accuracy, and data minimization. When considering the definition given by (Abraham et al. 2019) it proves the fact that utilizing a data governance model is the most appropriate to build a model to govern data with the integration of the GDPR data processing principles. Even though there is a limitation of scientific literature on the present state-of-the-art in data governance, the extant material helped grasp the concept of a data governance model. Various data governance models have been built for proper governing of data under aspects like quality, accountability, accuracy, etc. But here in the research, we consider personal data protection.

Abraham et al. (2019), Paananen (2020) and Kim et.al (2018) research 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, which provides data collecting tactics and process approaches to enable data integration and information management. When considering data governance models/frameworks several such models exist but with different data management areas like data quality management (Wende 2007), models developed for private firms like banks, (Paananen 2020) models developed to third-generation platforms, which guides organizations to define, design, develop and deploy services aligned with its vision and business goals (Yebenes and Zorrilla 2019).Here in the Table1, a summary of the literature review on data governance models will be presented. In addition, we propose a conceptual framework for data governance. The conceptual framework is based on the extensive data we gathered during our literature review. The Table 1 below shows some of the factors we recognized in the available data governance models that aligns with the GDPR principles.

Table 1: Overview of Literature

Reference	Factors considered	Factor aligned with GDPR data processing principles
Wende (2007)	Data consistency, data integrity, and security, accountability	Integrity and confidentiality, Accountability
Abraham et al. (2019)	Accountability, data retention requirements, data ownership, information accuracy, data storage for effective data management and data security, policies, standards and procedures regarding data storage, data retention and archival, data confidentiality, and integrity.	Accountability, Storage limitation, Accuracy, Purpose limitation, Lawfulness
Al-Ruithe et al. (2016)	Data integrity, proper data storage, data transparency	Integrity and confidentiality, Storage limitation, Lawfulness
Al-Ruithe et al. (2019)	Basic elements of a data governance initiative for privacy, confidentiality, and compliance, data accountability	Lawfulness, Integrity and confidentiality, Accountability
Yebenes and Zorrilla, (2019)	Data security and risks management, Data lifecycle management, storage of information, and its specifications.	Integrity and confidentiality, Data minimization, Storage limitation
Khatri & Brown (2010)	Locus of accountability, confidentiality, integrity and availability of data, optimal storage media,	Accountability, Integrity and confidentiality, Storage limitation
Micheli et al. (2020)	Strong accountability and	Accountability

	Standards.	
Kim & Cho (2018)	Accuracy, Consistency, personal information protection strategy and data disclosure/accountability strategy, security improvement, data transparency.	Integrity and confidentiality Purpose limitation, Accuracy Lawfulness, fairness, and transparency
Abiteboul and Stoyanovich (2019)	Data transparency, differential privacy, data provenance, data pre-processing: data cleaning, integration, querying, and ranking, fault tolerance, and recoverability	Transparency, Integrity, and confidentiality.
Dawes (2010)	Information stewardship (accuracy, validity, security, management, and preservation of information holdings.) and information usefulness, computer-mediated transparency: unidirectional and overly structured.	Accountability, Integration and confidentiality, transparency
Schlehahn and Wenning (2019)	Invisibility factor, the provenance of data, provenance of processes, and reasoning (or analytical) provenance, storage periods specifications.	Integrity and confidentiality, transparency, storage limitation.
Pfitzmann and Hansen (2010)	Privacy by data minimization: anonymity, unlikability, unobservability, and pseudonymity	Data minimization, transparency, integrity, and confidentiality

3 Methods

This research is being carried out to fill the gap in the lack of a comprehensive data governance model for GDPR compliance in Sri Lankan enterprises. In this research, a qualitative approach will be adopted where both a systematic literature review and interviews will be conducted. The research methodology of this study is carried out in three significant stages.

- The study will conduct a literature review to determine the relevance of existing available literature linked to data governance models, including existing and suggested techniques based on the most recent published (1997-2021) research publications.
- The study then proposes a conceptual model for data governance, demonstrating the stages of the data being managed with the critical areas that an organization should concentrate on while implementing GDPR.
- Interviews with industry experts on GDPR implementation were conducted to evaluate and validate the conceptual model.
- The interview data will be further analyzed and the final model for the data governance model will be finalized.

4 Data Collection

In this study data collection will take place in two ways, namely primary and secondary. The primary data collection would be from interviews, but to reach that stage the secondary data collection has to be completed. The secondary data collection is done on previous studies in the same field, as well as research articles, journals, and books, to establish the study's context and to operationalize the variables as shown in the below Table2.

Table 2: Operationalization Table

	Variables	Indicator	Indicator Description
1	Transparency	T1	Notice Awareness
		T2	Choice or consent

2	Accuracy	A1	Data Review
		A2	Automating error detection reports
		A3	Accuracy standards
		A6	Avoiding overloading - data entry team perspective
3	Integrity & Confidentiality	IC1	Pseudonymization and Encryption
		IC2	Data consistency
		IC3	Security and enforcement
4	Data Minimalization	DM1	Adequate
		DM2	Relevant
		DM3	Inventorying
		DM4	Limited
5	Accountability	ACT1	Proper responsibility division
		ACT2	Adequate documentation
6	Storage Limitation	S1	Data retention requirement - the purpose
		S2	Defining the data retention period
		S3	Periodic review for erasing or anonymizing unwanted data
		S4	Relevant industry standards or guidelines
7	Purpose Limitation	PL1	Purpose
		PL2	Specific
		PL3	Legitimate

Interviews are one of the most used qualitative research methodologies (Bryman and Bell 2011). Interviews are used to gather data and hear people's tales and perspectives about a phenomenon. The goal of qualitative interviewing is to take advantage of direct interaction and conversation between the researcher and the interviewee in a specific setting. Following the operationalization of the study's variables, a set of interview questions was created. The study's target population is information security experts employed in Sri Lankan IT companies that are GDPR compliant or are in the process of becoming GDPR compliant. The structure of the interview questions was based on the knowledge gained from the literature review and is divided into three sections.

As mentioned above questionnaire was created after the study's variables were operationalized. Based on the operationalization table (Table 2) the questions for the interview were developed covering all the areas under the seven principles of GDPR. An interview guide was created based on the study's research questions. All of the interviews followed the same three-phased interview. In the first phase basic questions regarding the interviewee's position and a brief description of the company in which he or she works, how does his or her job role in a normal day, and what they believe about EU legislation and their first steps in implementing the legislation were included. The primary goal of these questions was to collect valuable background information on the interviewee and his or her perception of the company in which he or she works. Data on perception is useful since it allows you to have a better knowledge of the organization and the interviewee's opinion on it. The second goal was for both the researcher and the interviewee to become accustomed to the interview scenario, resulting in mutual trust. According to Lutz (2007), interviewing without both the researcher and the interviewee having a shared understanding of the meeting's aim is meaningless. The interview questions were based on the research questions from the study, which were operationalized and classified into the research themes of implementation, guidance, and compliance.

5 Results and Discussion

There are research publications that focus specifically on data governance models, but they do not address GDPR and its implementation. As previously said, there has been limited research in this area, but the goal of this study is to

review publications comprehensively and identify all aspects that may affect the execution of the GDPR's seven principles. As a result, Table 1 above provides a more comprehensive overview of selected research studies and the factors identified in them.

5.1 Conceptual Model

Based on the results of the literature survey a conceptual model related to data management is developed integrating the seven principles of GDPR. Using Abraham et al. (2019), Panian (2010) models as the basis a conceptual model (Figure 2) is developed by eliminating a few organizational factors that were recognized as antecedents and integrating the data management stages recognized by (Paananen, 2020).

The following structural, procedural, and relational mechanisms act as the drivers for the implementation of GDPR principles.

Structural Mechanisms: SM1-Governance Bodies, SM2-Accountabilities, Structured mechanisms define governance entities and accountabilities, which include duties and responsibilities. The primary positions are data governance leader, data owner, data steward, data governance council, data processor, data controller, and data protection officer. The data governance leader is in charge of the day-to-day management of the data governance program. He or she guides data design, distribution, and maintenance, as well as assuring compliance with data policies. The data governance leader also oversees the operations of data stewards and provides regular updates on data governance performance.

Procedural Mechanisms: PM1-Policies and standards, PM2-Processes and procedures, PM3-Compliance Management. Data should be reliably recorded, maintained securely, used effectively, and shared appropriately, according to procedural governance systems. Different data policies and standards, processes and procedures, and compliance monitoring are all included. High-level guidelines and standards for the development, collection, storage, security, quality, and permitted use of data are provided by data policies. Data policies are used by organizations to express essential goals, data accountability, roles and responsibilities, and data retention periods. Data standards ensure that data representation and data-related activity execution are consistent and harmonized across the company. A clear data process is regarded as a critical component of a successful data governance implementation. Processes are ways for governing data that are standardized, recorded, and repeatable Procedures are the methods, strategies, and stages that are documented and followed to complete a certain activity or assignment. They differ greatly amongst businesses. Procedures, for example, describe how to create accountabilities and decision rights design a data model (Mosley et al. 2010), and identify and correct data mistakes. The goal of compliance monitoring is to track and enforce adherence to regulatory requirements as well as organizational rules, standards, processes, and service level agreements (SLAs).

Relational Mechanisms: RM1-Training, RM2-Communication, and coordination of decision-making. Relational governance systems make it easier for stakeholders to work together. Training programs guarantee that stakeholders especially employees have the knowledge and certifications they need to help with data governance implementation. The creation of an organizational culture that appreciates data assets is aided through communication and training. Communication attempts to raise awareness of the data governance program among stakeholders constantly, whereas decision-making coordination provides strategies for achieving alignment across departments.

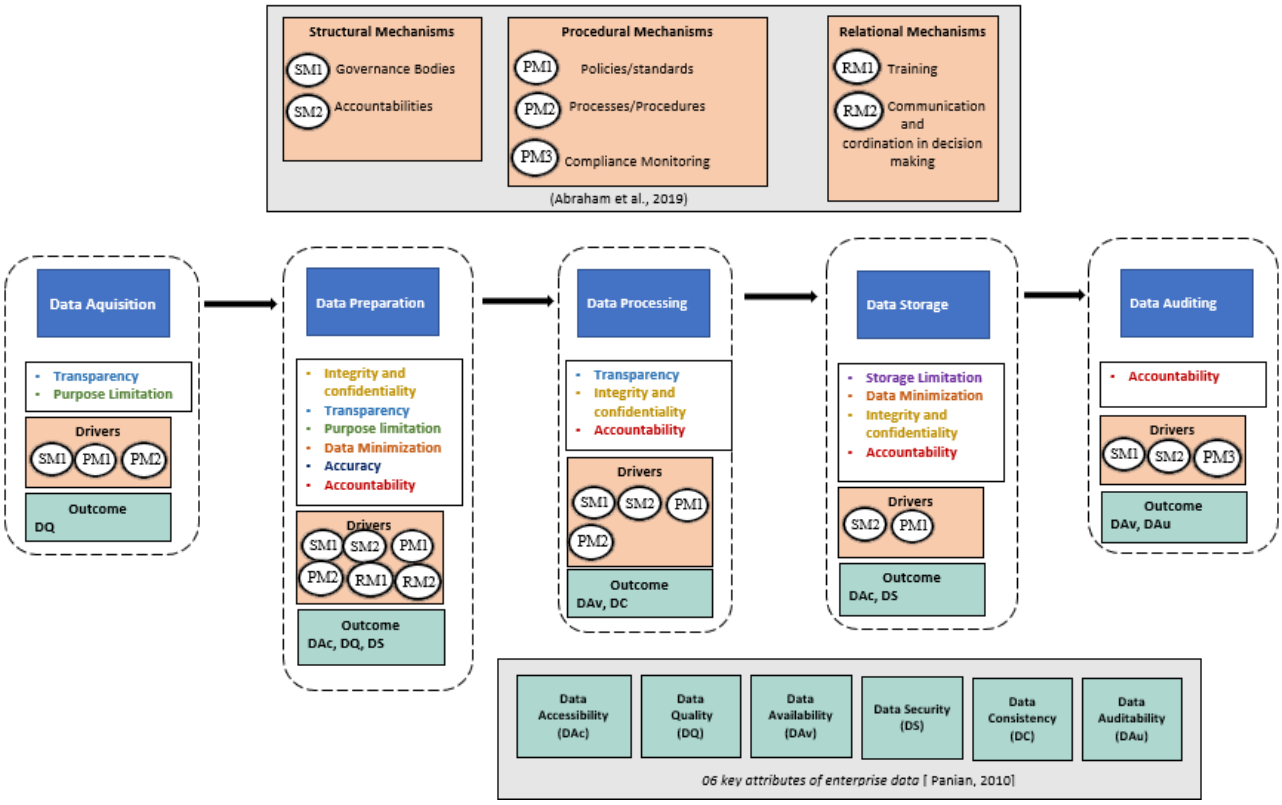

Figure 2: Conceptual Model

Data Management Stages:

- Data Acquisition A company's direct communication with the data subject occurs at this step. The stage at which data is collected is considered to be highly essential because more attention must be paid to elements such as transparency; the relationship between the data subject and the data controller; and purpose limitation; acquiring data solely for the purpose intended.
- Data Preparation This phase is in charge of translating data into a format that is safe to be processed. GDPR focuses on personal data, and it outlines the rules that must be followed while processing personal data. Integrity and confidentiality, transparency, purpose limitation, data minimization, correctness, and responsibility are the identified principles that must be followed.
- Data Processing The prepared data is processed in this step, and the processing must comply with the standards of transparency, integrity, and confidentiality, as well as accountability.
- Data Storage After the data has been processed, it is saved for future use or references. It must comply with principles such as storage limitation, data minimization, integrity, confidentiality, and accountability to keep the processed data in a safer environment.
- Data Auditing After the data processing phase is completed, auditing is required to assess and monitor compliance. Principles such as accountability play a significant role in data auditing.

Six key attributes of enterprise data. Six important features of enterprise data have been identified as the outputs of a solid data governance model, by the research (Panian 2010) that we used as a foundation for our conceptual data governance model. We may improve the outcomes even more by incorporating the GDPR principles into the existing

model at the same time. Data Accessibility, Data Quality, Data Availability, Data Security, Data Consistency, and Data Auditability are the outcomes.

5.2 Proposed Improvements

Following the main data collection, which includes interviews, the data will be studied further to revise the conceptual model, and then the final model will be finalized. In this study, the Thematic analysis method will be used to analyze the collected data. The goal of thematic analysis is to find patterns in the interview material. This analysis necessitates a constant back-and-forth between the complete data set and the coded data extracts that we have gathered. The acquired data must go through four phases in this analytical method (Mortensen 2020):

- Familiarize yourself with the information gathered. For interviews by familiarize yourself with the audio recordings. Transcripts must be written, and then first thoughts for codes to describe our content must be jotted down.
- Generating initial code: Data is allocated codes here. The term "code" refers to a quick explanation of what is mentioned in an interview, which is relevant to your area of study.
- Searching for themes: Themes are used to interpret the codes after they have been highlighted. Themes will give the codes a more active meaning.
- Reviewing the themes: Themes will be reviewed and refined in this section.
- Defining and Naming themes: The identified topics will be given a name and a description at this phase.

5.3 Validation

The model will be validated while conducting interviews with professionals in the field. Along with their insights into the strategies they've used to incorporate GDPR principles into the data management process, the validation of the model will take place.

6 Conclusion

The study comes to a close with a general conclusion, followed by a discussion of the study's limits and contributions. The chapter comes to a close with research recommendations. Various measures have been used to apply the Regulation in organizations, depending on the terms of the Regulation, the organizations' starting circumstances, and their needs. The success of the implementation is determined by elements such as the amount of time and resources given to it, as well as organizational structures and the implementation of indicators precisely. Through the conducted interviews as well we intend to gather more indicators on how each principle could be incorporated to a data governance model. Incorporating, all these factors into a data governance model makes it more convenient for the organization to make themselves GDPR compliant. Either the organizations could adopt the model, else they can use the model as guidance for their compliance implementation by doing a gap assessment with the existing governance model. Based on the findings and limitations of this study, more research into how businesses align themselves with data protection and their data protection agility could be conducted. It may be advantageous to assess employees' understanding of data security and the threat it poses to businesses in the event of data breaches or other similar situations.

References

Abraham, R., Schneider, J., & vom Brocke, J., Data governance: *A conceptual framework, structured review, and research agenda. In International Journal of Information Management* (Vol. 49, pp. 424– 438). Elsevier Ltd, 2019.

Bryman, A., & Bell, E.,Business research methods (3rd ed ed.). Oxford: Oxford University Press, 2011.

Comparing The Sri Lankan Personal Data Protection Bill, And The GDPR - Privacy - India. (n.d.), 2019, https://www.mondaq.com/india/data-protection/956530/comparing-the-sri-lankan-personal-data-protection-bill-2019-and-the-gdpr, Accessed:2021-09-14.

How to Do a Thematic Analysis of User Interviews | Interaction Design Foundation (IxDF), https://www.interaction-design.org/literature/article/how-to-do-a-thematic-analysis-of-user-interviews, Accessed:2021-10-10.

Ismagilova, E., Hughes, L., Dwivedi, Y. K., & Raman, K. R., Smart cities: Advances in research—*An information systems perspective. In International Journal of Information Management* (Vol. 47, pp. 88–100). Elsevier Ltd, 2019.

Kalhoro, S., Rehman, M., Ponnusamy, V., & Shaikh, F. B., *Extracting key factors of cyber hygiene behavior among software engineers*: A systematic literature review. In IEEE Access (Vol. 9, pp. 99339–99363). Institute of Electrical and Electronics Engineers Inc., 2021.

Kim, H. Y., & Cho, J.-S., Data governance framework for big data implementation with NPS Case Analysis in Korea. In www.jbrmr.com *A Journal of the Academy of Business and Retail Management* (Vol. 12). ABRM. www.jbrmr.com, 2018.

Mosley, Mark., Brackett, M. H., & Data Management Association, *The DAMA guide to the data management body of knowledge* (DAMA-DMBOK guide). Technics Publications, 2010.

Olanrewaju, A. S. T., Hossain, M. A., Whiteside, N., & Mercieca, P., Social media and entrepreneurship research: A literature review. In International Journal of Information Management (Vol. 50, pp. 90–110). Elsevier Ltd.,2020.

Paananen.J.P., A New Data Governance Model for the Bank of Finland,2020.

Panian, Z., " Some Practical Experiences in Data Governance", *World Academy of Science, Engineering and Technolog*y, 2010.

Rodot`a , In Reinventing Data Protection? Springer Netherlands. https://doi.org/10.1007/978-1-4020-9498-9, 2009.

Rowe, F., What literature review is not: Diversity, boundaries, and recommendations. *In European Journal of Information Systems* (Vol. 23, Issue 3, pp. 241–255), 2014.

Senyo, P. K., Liu, K., & Effah, J., Digital business ecosystem: Literature review and a framework for future research. *In International Journal of Information Management* (Vol. 47, pp. 52– 64), 2019.

Singh, Comparing *The Sri Lankan Personal Data Protection Bill*, And The GDPR - Privacy - India,2019.

Talking economics - *The Growing Need for Privacy and Data Protection in Sri Lanka*, https://www.ips.lk/talkingeconomics/2020/01/13/the-growing-need-for-privacy-and-data-protection-in-sri-lanka/, Accessed:2021- 08-26.

Wende, K. (2007). Association for Information Systems AIS Electronic Library (AISeL) A Model for Data Governance-Organising Accountabilities for Data Quality Management Recommended Citation Wende, Kristin, "*A Model for Data Governance-Organising Accountabilities for Data Quality Management"* A Model for Data Governance-Organising Accountabilities for Data Quality Management. http://aisel.aisnet.org/acis2007/80.

Yebenes, J., & Zorrilla, M. (2019). Towards a data governance framework for third-generation platforms. Procedia Computer Science, 151, 614–621. https://doi.org/10.1016/j.procs.2019.04.082.

Zorn, T., & Campbell, N., Improving the writing of literature reviews through a literature integration exercise. *In Business Communication Quarterly* (Vol. 69, Issue 2, pp. 172–183), 2006.

Biographies

P.A.Indhumini Ranathunga is a final year undergraduate at the Department of Industrial Management of University of Kelaniya, Sri Lanka who is reading for her BSc (Hons) in Management and Information Technology degree. She is specializing in Information Technology and is currently completing her final year undergraduate research in the area of Personal Data Protection.

Ruwan Wickramarachchi is a Senior lecturer at the Department of Industrial Management, University of Kelaniya. He holds BSc in Industrial Management from the University of Kelaniya and MPhil in Management studies (specialized in Information systems) from the University of Cambridge, United Kingdom. He received his PhD in distributed simulation from Sheffield Hallam University, United Kingdom. His current research interest includes applications in distributed simulation, management of information technology and project management. Currently, he is also servicing as Director of the Information and Communication Technology Centre, University of Kelaniya.