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