Vidyodaya Journal of Management
2022, Vol. 8 (I) **169 - 200**

ISSN 2448-9344 (Print) ISSN 2448-9352 (Online)
ISBN 978-955-23-0019-3
Reprints and permissions:
vjm@sjp.ac.lk
DOI: https://doi.org/10.31357/vjm.v8il.5608

Holistic Approach in Introducing Proper Legal Framework to Regulate Data Protection and Privacy in Sri Lanka

Thusitha B. Abeysekara
Senior Lecturer in Law, University of Sri Jayewardenepura, Sri Lanka

Amali E. Ranasinghe
Attorney-at-Law at Supreme Court of Sri Lanka

Abstract

Data protection and privacy law have never been important as they are today. Data protection and privacy ensure that data is safeguarded from unlawful access by unauthorised third parties and misappropriation of the same. A successful data protection strategy will be helpful to prevent data loss, theft, or corruption of data. It is evident that information and communication technology is developing daily and privacy issues or the threats against personal data of the persons also equally increasing. Responsibility of a government to provide effective privacy and data protection laws/policies cannot be disregarded at any point. Until very recent Sri Lanka did not have a separate legislation to deal with data protection and privacy and it was identified as a major lacuna in our law. At present, in addition to the Personal Data Protection Act No. 09 of 2022 there are several other legislations that may be applied to regulate certain aspects of data protection and privacy. In this research, researcher is aiming to assess whether existing legal framework on data protection and privacy in Sri Lanka is adequate and effective. This will be done by comparing the Sri Lankan legal framework with UK and Singapore, countries that are known as pioneers of data protection and privacy. Ultimate goal of the researcher is to contribute towards assurance of data protection and privacy right of the individuals in Sri Lanka.

Keywords: *Data protection, Privacy, Information Communications Technology, Personal data*

Corresponding Author:
Thusitha B. Abeysekara, University of Sri Jayewardenepura, Sri Lanka. E-mail: thusitha@sjp.ac.lk

Introduction

Primary aim of this research is to assess the effectiveness of the data protection and privacy law in Sri Lanka compared to the UK and Singapore and to make suggestions on how to establish a comprehensive data protection and privacy regime in Sri Lanka. Data protection and privacy laws primarily ensure that your data is safeguarded from unlawful access by unauthorised third parties and misappropriation of the same. Though the term data protection and privacy are often used concomitantly there is a significant difference between these two norms. Data privacy deals with ability to access to data and data protection provides tools and policies that are available to restrict interdependent (Rouse 2021).

Data protection and privacy laws are increasingly becoming crucial to Sri Lanka too, mostly due to the rapid digitalisation. Moreover, data protection and privacy has become more vital due to the emergence of e-governance and e-commerce. Sri Lanka's e-commerce industry generated USD 400 million by year 2020. Today most of the businesses will be conducted through digital platforms therefore having a robust data protection and privacy measures would secure data and alongside it will improve the business and consumer confidence. A successful data protection strategy will be helpful to prevent data loss, theft, and corruption of data. Data privacy is also a guideline on how data need to be collected or handled, it may vary according to the sensitivity and importance of data concerned. Data privacy ensures that sensitive/important data can be accessed only by authorised persons. Data protection includes both prevention of unauthorised access as well as the protection against loss caused by natural or human-created reasons (Nadkarni, 2016).

Prior to the so-called information revolution, information and data of the individuals were only stored in traditional filing cabinets or in similar places. Other than the owner of said data third parties could not easily gain access to such data. However, with the emergence of computer technology people started storing their data in computers concurrently with the development of internet/computer networks personal data became much more widespread. Said developments increased the potential of data and privacy invasion (Rowland et al., 2012).

Development of technology has no territorial boundaries. But responsibility of a government to provide effective privacy and data protection law/policy cannot be disregarded. Apparently, mere recognition of data protection and privacy is

not adequate it can be labelled as a mere "dead letter" as legislation and judicial findings have only a marginal effect (Koops, 2014). Sri Lanka is a country which didn't have a separate statute to regulate data protection and privacy until very recent. Thus, some laws and regulations applicable to certain aspects of data protection and privacy could be found within several piece of legislations which are industry specific e.g. – Intellectual Property Act No. 36 of 2003, Computer Crimes Act 2007 etc.

In addition, remedy against breach of individual privacy can be found within the Roman Dutch law it is the Sri Lankan common/residuary law which form an action against injury (wrongful aggression upon the person, dignity or reputation) under *actio injuriarum* (*Nadarajah v Obeysekera (1971) 52 NLR76*). Nonetheless this action is very restrictive as there are many requirements to be fulfilled to succeed a particular claim (*Sinha Ratnatunga v The State (2001) 2 SLR 172).* Arguably absence of proper law to deal with privacy/data protection have adversely affected on individuals/entities in Sri Lanka as it is detrimental to the development of e-commerce and international trade/investment (Senarathna, 2020).

There are three main risk factors attached to the privacy and data protection. First one is the risk of injustice cause due to the significant inaccuracy of personal data; e.g. – function creep, unjust inference. The second risk is, one may control another person over by collecting his/her personal data. Finally unauthorised invasion of data can be identified as a threat to the personal dignity of the persons. (Senarathna, 2020). It is conclusive that unless there is an effective law to deal with data protection and privacy deterrence of aforesaid risk factors would be a difficult task.

Significance of the study

The study intends to assess whether prevailing legal framework on data protection and privacy in Sri Lanka is adequate and effective and to provide suggestions on how to establish a comprehensive data protection and privacy regime in Sri Lanka. This will be done through comparing the Sri Lankan legal framework with UK and Singapore since these two countries has been recognised as having an effective data protection and privacy laws. Apparently providing an equal and universal privacy and data protection framework is not an easy task, but it is essential to provide at least a basic and minimum protection (Bainbridge, 2007).

This study is particularly important to Sri Lankan context as it recently enacted Personal Data Protection Act No. 09 of 2022 which is primarily aiming to safeguard the personal data of the persons. This study will further contribute towards the development of the legal framework on data protection and privacy in Sri Lanka since Personal Data Protection Act No. 09 of 2022 is a newly enacted legislation and its effectiveness is yet to be tested. Analysis planned to be done between UK and Singapore laws will be helpful to identify the gaps of the Sri Lankan law and in giving the recommendations of the researchers in order to formulate an effective data protection and privacy law in Sri Lanka. Ultimate goal of the researchers is to contribute towards assurance of data protection and privacy right of the individuals in Sri Lanka and to fill the gaps in existing law.

Scope and Limitations

This research will be mainly limited to the Sri Lankan law on data protection and privacy. Researchers will primarily analyse the Sri Lankan law with two other jurisdictions, (UK and Singapore), in order to bring an additional comparative point of view to this study. Principal purpose of this study is to assess the effectiveness of the Personal Data Protection Act No. 09 of 2022.

Literature Review

In this section, researchers evaluate the available literature within the selected field of study in order to identify the existing research gap and to determine how this research study should address the said gap. Moreover, another key aim of this chapter is to assess how knowledge has been evolved within the selected field of study.

Importance of data protection and privacy laws

Recent inventions and business methods calling attention to take steps for protecting persons and for securing their right referred as “right to be let alone”. Privacy can be identified as an essential part of every individual’s life as invasion of privacy can cause mental pain and distress which would be greater than the mere bodily injury. Therefore, providing a legal remedy for such injury would treat wounded feelings of the persons as a substantive cause of action as invasion of privacy constitutes a legal injuria and it demands a redress. Arguably unwarranted invasion of individuals privacy must be prevented as far

as possible (Warren and Brandies, 1890). After introducing the first generation of computers which were able to store and manipulate data, issues relating to the data protection and privacy significantly increased (Rowland et al., 2012). Later on, safeguarding data protection and privacy was identified as a fundamental right in major international human rights legislations such as Universal Declaration of Human Rights (UDHR) and International Covenant on Civil and Political Rights (ICCPR) (Stefan et al., 2019).

The growing need for data protection and privacy in Sri Lanka

EU General Data Protection Regulation (GDPR) introduced new changes to the data protection laws, for an example it requires companies not having any physical existence in EU to comply with GDPR regulations if it offers goods or services to EU countries and at the same time if personal data transfers outside the EU controller of such data must ensure that a similar protection is given to the said data like in EU. So that it is important for every country including Sri Lanka to have an effective domestic legislation to protect data and privacy which is synonymous with existing international standards (De Soyza, 2017). During past few decades Sri Lankan government paid more attention towards strengthening the legal framework for use of information technology in various fields through the enactment of some important legislations like Electronic Transactions Act of 2006 and Computer crimes Act of 2007 these two legislations provide the laws and relevant legal procedures for effective and correct use of technology". Nevertheless, many academics contended that in addition to enacting these regulations government should take immediate steps to improve the standards of information technology usage specially in connection to the data protection and privacy.

As digitalization generates more data, it heightens the need of having adequate and effective data protection and privacy laws. This need has become more crucial with the emergence of e-governance and e-commerce in Sri Lanka (www.ips.lk). Since Sri Lanka didn't have a specific data protection and privacy legislation until very recent people always attempted to protect their data and privacy via manual forms such as storing them in isolated computer systems, but effectiveness of such measures obviously doubtful. Thus, with the enactment of Personal Data Protection Act No. 09 of 2022 it is be believed that this position would be changed.

Data Protection and Privacy in UK and Singapore

UK is one of the first countries to implement GDPR in local law. UK introduced its own version of EU GDPR which is known as UK GDPR under its European Union Withdrawal Agreement in 2020. The UK's GDPR is supplemented through the DPA 2018 (Carey and Treacy, 2015). Despite of existence of a specific law to deal with data protection and privacy in UK, Warwick Ashford suggested that it is not an end point but it is just the beginning. Since data protection and privacy aspects are an evolutionary process as no business, industry, or technology stand still (Ashford, 2018).

Singapore enacted the Personal Data Protection Act in 2012 which provides a baseline standard of protection for personal data of the persons. It basically imposes nine data protection obligations on organizations operating in Singapore (Benjamin, 2017). Key rationale behind the implementation of data protection laws and regulations in Singapore is to; (i) protect the privacy interests of the individuals and (ii) to advance the economic interests of Singapore (Chesterman, 2012).

As per the data of the United Nations Conference on Trade and Development (UNCTAD) most of the countries around the world (137 out of 194 countries) including UK and Singapore have their own laws and regulations to deal with data protection and privacy (www.unctad.org, 2021). Sri Lanka is a country which did not have a separate legislation to deal with data protection and privacy until very recent. Apparently above discussed literature establishes the importance of having an effective legal framework to deal with data protection and privacy. Thus, none of the literature assess the effectiveness of Personal Data Protection Act No. 09 of 2022 as it is a very recent enactment.

Methodology

In this section, researchers describe the methodologies as well as the data collection methods involved in this research. Accordingly, researchers adopt a qualitative research approach together with doctrinal research method and comparative and international research methodology. Furthermore, in this section researchers aim to outline the said data collection methods and methodologies and also clarifies the rationale behind choosing aforesaid methodologies and data collection methods.

Research problem

Every day a vast amount of data will be collected, stored and transmitted across the globe due to the impact of the technology. Undoubtably rapid development of the technology and innovation have increased the need of having an effective data protection and privacy law for a country. Similarly, as we can see data has also become incredibly important asset at present therefore most of the time data of individuals are vulnerable to theft, loss, corruption or to similar threats. Sri Lanka is a country which didn't have a consolidated /separate legislation to deal with data protection and privacy until very recent. Thus, some of the provisions that are indirectly applicable to data protection and privacy could be found within several other piece of legislations which are industry specific.

Absence of a proper legal framework to regulate data protection and privacy in Sri Lanka had already caused multiple adverse impacts such as; violation of rights of the persons (collection of personal data without the knowledge/consent, misuse of data), loss of direct/indirect foreign investments etc. This was identified as a major gap or lacuna in the Sri Lankan law. Therefore, academics argued that it is essential to provide an effective solution to this problem with immediate effect, as a result government of Sri Lanka enacted the Personal Data Protection Act No. 09 of 2022. However, the effectiveness of this statute is still doubtful. Hence in in this research, researchers are aiming to assess the effectiveness of the existing legal framework in Sri Lanka on data protection and privacy comparatively to the UK and Singapore experience.

Research Questions

a) Why Sri Lanka was reluctant to introduce a specific law to deal with data protection and privacy?
b) Why data protection and privacy is important to Sri Lankan context?
c) To what extent prevailing laws on data protection and privacy in Sri Lanka is adequate to provide solutions for the emerging issues arising from the rapid development of technology?
d) What are the lessons that Sri Lanka can learn from the UK and Singapore's experience on data protection and privacy?
e) What are the suggestions that can improve the effectiveness of data protection and privacy regime in Sri Lanka?

Hypothesis

Unless there is an effective legal framework which is in line with international standards, dealing with problems associated with data protection and privacy would be problematic. Therefore, as a developing country Sri Lanka also need to have an effective legal framework which is in line with international standards to regulate data protection and privacy.

Objectives

a) To examine the efficacy and adequacy of existing laws concerning data protection and privacy in Sri Lanka.
b) To examine successful mechanisms relating to data protection and privacy and significant international standards.
c) To collect UK and Singapore's experience on data protection and privacy.
d) To recommend new strategies that can be adopted in to Sri Lankan context to provide an effective and efficient data protection and privacy strategy.

Research data

Researchers are using a qualitative research method in order to have a comprehensive research approach to the study. Data for this study will be gathered from both primary and secondary sources. Reviewing the said primary and secondary sources will be helpful to identify the gaps of the present legal framework on data protection and privacy in Sri Lanka. Moreover, this research will be based on doctrinal and comparative methods. Doctrinal method will be used to answer the first two research questions and Comparative and International Research Methodology will be used to answer the last three research questions.

Primary and secondary data

Primary data may include; statutes, international conventions, regulations and case law etc. by analysing these data researchers will be able to enter into their final conclusions and provide suggestions on establishing an effective data protection and privacy regime in Sri Lanka based on UK and Singapore's experience. In addition, researchers are aiming to use secondary data such as; books, scholarly articles, law journals, websites… as these are the pre-existing

works relating to the selected subject matter, these secondary data will provide a basic guidance to this study.

Qualitative and quantitative data

As this research will be conducted in a critical and analytical manner, researchers will adopt the qualitative research methodology. Unlike the quantitative data, which deals with the numbers and figures, qualitative data is more descriptive in nature. By using the qualitative research approach researchers are aiming to collect appropriate data to conduct this research and establish research objectives.

Data collection system

Data selection is the process of determining the appropriate data/sources as well as suitable instruments to collect data. Data for this research will be primarily gathered from direct observations and documents and pre-existing records (qualitative data) as it will allow the researchers to adequately answer the concerned research questions. (sir is it okay to delete this section?? As it is similar to the previous section??

Method of data analysis

Doctrinal Method (Black Letter Approach)

By using the doctrinal research method, researchers will analyse the existing legal materials such as statutes, case law, textbooks, journal articles etc. and attempt to identify the existing gap in the data protection and privacy regime in Sri Lanka. Thereby researchers will be able to incorporate new elements of law into the existing legal system (Hutchinson and Duncan, 2012).

Comparative and International Research Methodology

Cross-national comparative research method requires a sound knowledge and understanding of both national and international contexts. Use of comparative and international research methodology will be helpful to understand the variances of different legal approaches in connection to a particular question, also it will be helpful to understand the gaps in knowledge and to suggest new perspectives. Accordingly this approach will be helpful to understand the gaps of the Sri Lankan law compared to UK and Singapore.

Sri Lankan Legal Framework on Data Protection and Privacy

In Sri Lanka there are several legislative provisions that can be applied to certain aspects of the data protection and privacy. Said legislations consist of; Constitution of Sri Lanka (1978) (Article 14A (2)), Computer Crimes Act No. 24 of 2007 (s3 – 10, s19, s22, s24), Electronic Transactions Act No. 19 of 2006 (s2), Right to Information Act No. 12 of 2016 (s5 (1) (a)), Banking Act No. 30 of 1998 (s77), Telecommunication Act No. 25 of 1991 (s49, S52), Intellectual Property Act No. 36 of 2003 (s160). In this section, applicability of these laws towards the data protection and privacy will be assessed.

As mentioned previously data protection and privacy increasingly becoming relevant to Sri Lanka due to the rapid rise of digitalization. As digitalization generates more data, it heightens the need of having an adequate and effective data protection and privacy laws (Abeysekara, 2017). This need has become more vital with the emergence of e-governance and e-commerce in Sri Lanka. Although there are multiple legislations dealing with electronic transactions, cyber-crimes and consumer protection there is no specific/separate law that regulates data protection and privacy this can be identified as a major gap.

Key statutes, regulations, directives and bills

In order to amend or introduce a new law, analyzing the existing laws and identifying its flaws is always a must. Therefore, primary aim of this section is to assess the adequacy and effectiveness of the existing Sri Lankan legal framework on the data protection and privacy.

Constitution of Sri Lanka (1978)

Constitution of Sri Lanka did not recognize neither right to information and right to privacy originally, subsequently, right to information was guaranteed under the 19th Amendment to the Constitution. Simultaneously, Right to Information Act No. 12 of 2016 was enacted. At present right to privacy is protected in Sri Lanka only as a delictual matter under the concept of *Actio Injuriarum* or in other words right to privacy is concerned as a private law issue and this area is still evolving through case law. *Actio injuriarum* is an independent remedy available against wrongful aggression on persons, their dignity or reputation and it is arguable that *actio injuriarum* is not adequate enough to deal with modern aspects of data protection and privacy issues.

Nadaraja v. Obeysekara in this case court attempted to elaborate the term "invasion of privacy" and it was emphasized that prevention of others interference on someone's space is the purpose of privacy law. However, absence of proper judicial interpretation on right to privacy also shows the State's lack of intention to protect right to privacy. Altogether entrenchment of the right to information without ensuring the right to privacy has created number of social issues ((1971) 52 NLR 76). Differently to the Sri Lankan approach more than 90 countries around the world have recognized both right to information and right to privacy concomitantly.

Moreover, Article 14A of the Constitution (19th Amendment) refers to certain privacy concerns within the context of restrictions imposed on the right to information. Accordingly, Article 14A (2) of the constitution restricts right to information of the persons subject to limitations prescribed by law to uphold the interest of the national security; to safeguard territorial integrity, public safety, for the purpose of preventing crimes, protection of health, morals, privacy of persons. However, this is not a direct provision where right to privacy is expressly granted and expounded as fundamental right of the citizens of Sri Lanka.

Apparently, Article 14A (1) merely ensures right to access to information by persons without ensuring their right to privacy this can result in severe violations of privacy of the persons (De Soyza, 2017). If government or an administrative arm of the government infringe any fundamental right of the citizens such actions can be questioned by invoking the exclusive jurisdiction of the Supreme court as set out in the Article 17 read with Article 126 (1) but this is not possible since right to privacy is not a fundamental right under the Constitution of Sri Lanka and privacy aspect is merely recognized as an exception to the right to information (Marsoof, 2008).

Universal Declaration of Human Rights (UDHR) was the first international instrument which attempted to recognize right to privacy as a separate fundamental human right. Subsequently International Covenant on Civil and Political Rights (ICCPR) also recognized the right to privacy, family, home and correspondence from arbitrary and unlawful interference and it ensures that everyone should have protection of the law against unlawful interferences. Both right to information and privacy plays important roles and it is noteworthy that under human rights law no right can gain greater weight than another. As a member of UDHR and ICCPR Sri Lanka also could adopt a similar approach to

protect these rights simultaneously (Sooriyabandara, 2016). However, these Conventions are not directly enforceable in Sri Lanka until the enactment of a separate legislation to that effect.

Key statutes on data protection and privacy in Sri Lanka

Though there are multiple statutes that are indirectly applicable to data protection and privacy in Sri Lanka few key statutes will be discussed herein. These statutes were specifically selected as they at least consist of few provisions which may indirectly applicable to data protection and privacy and restricts/prohibits unlawful access to data stored in computers, illegal invasion of data, illegal interception/transmission of telecommunication contents and protection of confidential data.

Computer Crimes Act No. 24 of 2007

This Act deals with the identification of computer crimes and also it provides the procedure for the investigation and prevention of computer crimes and matters incidental and connected therewith (Computer Crimes Act No. 24 of 2007, S1). Accordingly, S3 to s10 deals with the key substantive offences recognized under the Computer Crimes Act of Sri Lanka. S3 of the Act stipulates that unauthorized access to a computer as an offence. As per s4 doing any act to secure unauthorized access in order to commit an offence also recognized as crime. Additionally, to the S3 and S4, S5 addresses another important aspect of computer crimes, which is the causing a computer to perform a function without a lawful authority. E.g. – modification, corrupting, falsification, deletion or alteration of data stored in a computer. It is arguable that if a person accessing into a computer with the intent of stealing, modifying data of another offender violates the data protection and privacy too (Abeysekara, 2015).

S10 of the Computer Crimes Act provides another strong protection to the user's information collected by service providers. In addition, s19 of the Act also somewhat relevant to the certain aspects of data protection and privacy as it empowers investigators to give directions to responsible persons to preserve related data for a specific period of time. Further s22 of the Act directs the police officer who conduct a particular search under this Act to issue a complete list of items and data including the data and time of such seizure. Altogether s24 enable the maintenance of confidentiality of the information that has been

collected during the course of investigations (Computer Crimes Act No. 24 of 2007, s19, s22).

It is clear that Computer Crimes Act of Sri Lanka do not directly deal with the data protection and privacy, thus several provisions of the Act have some sort of application to the data protection and privacy. Thus, existence of such provisions is not adequate or effective enough to deal with data protection and privacy requirements of a country. Computer Crimes Act been enacted for the primary purpose of criminalizing the unlawful access to a computer, computer program, data or information. Data processing and transportation of personal data will not be directly governed by the Act. Therefore, it is always recommendable that most effective way to deal with a particular legal matter is to have a separate piece of legislation or regulations rather than referring to several legislations which are not directly deal with a matter concerned.

Electronic Transactions Act No. 19 of 2006 (ETA)

Digital laws primarily regulate the use of electronic data and digital documents for official and personal transactions (Electronic Transactions Act No. 19 of 2006, s2). The main purpose of ETA is to regulate e-transactions. Though this Act is applicable to any data or communications made in electronic form, Act doesn't define what shall be considered as personal data and it contains no provision in relation to data protection and privacy. Even though Sri Lanka adopted a progressive approach towards the regulation of e-transactions gaps in connection to the data protection, privacy and consumer protection still remains the same and it is detrimental to the effective enforcement of the law on e-transactions as well (Ariyaratna, 2016).

Right to Information Act No. 12 of 2016 (RTI)

RTI provides an absolute right and grant effect to the citizens constitutional right to access to information under the s3 of the Act. However, this right been granted subject to certain limitations specified in the s5 of the RTI Act (Greenleaf, 2017). S5 (1) (a) can be recognized as a vital provision which is directly affecting to the data protection and privacy. This section stipulates that disclosure of personal information which does not have a relationship with any public activity or interest or which will allow the unwarranted invasion of privacy of the individual unless there is a considerable public interest which is justifiable or unless the person concerned consent to such disclosure in writing… access to information shall be refused (Right to Information Act No.

12 of 2016, s5 (1) (a)). It is apparent that this provision is seeking to strike a balance between right to information and data protection and privacy.

Banking Act No. 30 of 1998

Financial service companies including banks and non-bank financial institutions process large amount of personal data without any doubt. S77 of this Act impose privacy obligations on directors, managers, officers and other persons employed in the licensed commercial banks/licensed specialized banks… accordingly they shall sign a declaration before undertaking their duties to observe a strict secrecy (subject to exceptions) in respect of all the transactions of the bank, its customers and the state of accounts of any person including other incidental matters (Banking Act No. 30 of 1998, s77). At present, financial institutions are increasingly becoming susceptible to data/privacy breaches by the criminals due to the importance of the data they store.

Telecommunication Act No. 25 of 1991

S49 of this Act stipulates that a telecommunication officer or any other person who performs the official duties in connection to telecommunication services commits an offence if he; (a) willfully destroys, secrets, alters or does any other act other than his duties or intentionally modifies /interfere with the contents of the messages which has been received for the transmission/delivery… (b) omits to transmit/intercept or detains any message. (c) other than pursuance of his duties or as directed by the court disclose the contents of any message or any parts of the contents of any message to a person other than to who the message is addressed (Telecommunication Act No. 25 of 1991).

S52 of the Act stipulates that any person who intrudes without lawful authority (a) contents of a message or its usages information… (b) with the intention of interfering any message or its usage information. (c) with the intention of unlawfully learning the contents of the message or its usage information… commits a punishable offence under this Act. Moreover, willful interception of telecommunication transmission, interception and disclosure of contents of a message.… also being recognized as an offence. Further s54 recognizes interception and disclosure of contents of a message by telecommunication officials as an offence (Telecommunication Act No. 25 of 1991, s52, s54). It is clear that aforesaid provisions are also closely linked with the data protection and privacy concerns.

Intellectual Property Act No. 36 of 2003

Particularly S160 of the Sri Lankan IP Act deals with the unfair competition and undisclosed information. S160 (6) (a) stipulates that; any act or practice in the course of industrial or commercial activities that results in disclosure of the undisclosed information without obtaining the consent from rightsholder of that information and when someone act contrary to the honest commercial practices it amounts to an unfair competition (www. [iesl.lk], 2021). As explained in the s160 (6) (b) disclosure, acquisition or use of undisclosed information by others without the consent of the rightful holder may result in; (i) industrial/commercial espionage. (b) breach of contract. (c) breach of confidence. (iv) inducement to commit any of the aforesaid acts. Seemingly these provisions can be applied to protect data/privacy of the organizations as well as individuals who holds valuable data (*Douglas v. Hello Ltd & Ors*).

Personal Data Protection Act No. 09 of 2022

With the intent of modifying the existing data protection framework in Sri Lanka government introduced the Personal Data Protection Act No. 09 of 2022 (PDPA).. This Act is attempting to fill a long-standing gap in Sri Lankan data protection and privacy regime. Said Act primarily aims to ensure following aspects; (a) to protect the personal data given to the entities. (b) to grant rights to the data subjects. Followings are the key features of this Act; (i) regulating the processing of personal data. (ii) rights of the data subjects will be strengthened. (iii) it will regulate the dissemination of unsolicited messages using personal data. (iii) designation of the data protection authority. (iv) to provide a legislation to deal with the matters incidental to the processing of personal data.

Generally, it provide measures to protect the personal data of the individuals held by banks, telecom operators, hospitals and other similar data processing/aggregating entities. Alongside this Act is not applicable to the personal data processed solely for someone's personal, domestic or household purposes (S2 (3) of PDPA 2022). This legislation primarily intends to balance the interests of the enterprises relying on personal data processing and also the interests of the individuals whose personal data will be processed. As per the S4 of the Act data controllers are obliged to process personal data in compliance with the obligations specified in the Act. Moreover s6 (1) of the Act require data controllers to define the purpose of personal data processing. Also, they are obliged to ensure that personal data will be processed only for; specified, explicit and legitimate purposes (S6 (1) (a) (b) (c) PDPA 2022). SS7 – 11

further specifies the other important data protection obligations of the data controllers.

Accordingly, it's clear that, PDPA 2022 attempts to ensure the transparency and accountability of such processing activities. Part II of the Act deals with the rights of the data subjects. This can be identified as another crucial feature as it will be helpful to strike a balance between rights and obligations of the data controllers and data subjects. Some important rights of the data subjects can be listed as follows; where the processing is done subjected to the consent of the data subjects, data subjects are entitled to withdraw the consent given to the controllers, object to the processing of data as stipulated in S14 (1). Right to rectification is ensured under the S15 of the Act. As per this section data controllers are obliged to rectify or complete inaccurate/incomplete data. Furthermore, right to erasure also safeguarded through S16 of the Act under certain circumstances.

Part III of the Act is applicable to the data controllers and processors. Several obligations being imposed on entities collect/process personal data referred as data controllers and processors, they are required to designate/appoint Data Protection Officer in order ensure the compliance with the provisions of this Act (S22 (1) PDPA 2022). Concurrently data controllers must ensure the security/confidentiality of personal data by adopting suitable technical/organizational measures. Also, they must always consider about transparency obligations underlined in the Act (Data Protection Bill (2019), s22).

PDPA 2022 further aims to govern data breach incident. Under the S23 (1) of the Act when there is a personal data breach, controller shall notify the Authority. Part V of the Act deals with the aspects relating to "Data Protection Authority" specifically about its establishment, objectives, powers etc. Apparently, Data protection Authority is responsible for all the aspects incidental to the personal data protection in Sri Lanka including the implementation of the provisions of the proposed Act. Another crucial functionality of Data protection Authority is it is capable of issuing directives to the entities that fails to comply with the provisions of the proposed Act and it can impose administrative penalties (S32 of PDPA 2022).

It is clear that when drafting this Act committee had followed best practices adopted by various international standards such as; OECD Privacy Guidelines, APEC Privacy Framework, EU General Data Protection Regulation etc. After considering the rapid technological developments and other associated matters

(digital strategies adopted by the government and the private sector) it can be argued that Data Protection legislation is urgently required for Sri Lanka.

Criticisms against the Personal Data Protection Act No. 09 of 2022

Despite of the afore discussed plus points some critics questions the effectiveness of ***Personal Data Protection Act No. 09 of 2022***. Main criticism against the Act is inclusion of vague clauses. Apparently critics contend that this legal uncertainty can discourage flow of the foreign investments into the country. Next this Act does not contain a provision which facilitate data transfers with the consent of users similar to the GDPR which provides derogations when data subjects give their explicit consent. Moreover, the Sri Lankan government is capable of setting up or appointing anybody statutory or otherwise as the Data Protection Authority (S28 (1) PDPA 2022).

Though PDPA 2022 do not prevent government from establishing an independent Data Protection Authority government will obviously have a significant control over this Authority and it is likely to dilute its legitimacy as an independent expert body. E.g. – government can issue directions to the Data Protection Authority in connection to the discharging of its functions, this shows the lack of independence of this authority. Which is contrary to the principles set out in the EU GDPR as it suggests that supervisory authority set out by the member States must be an independent public body.

Another problem attached to the Act is it impose obligations on both data controllers and processors. Hence data processors are bound to comply with the conditions of processing set out in the five Schedules of the Bill. Failure of the data processors to comply with the provisions of the Act result in data processors being penalized. Under the GDPR data processors will not be subjected to such penalties. Critics contend that these aspects are against the international standards and it will increase the regulatory burden of the data processors and also it will impact on investments in data processing and outsourcing industry in Sri Lanka.

Furthermore, the proposed Act requires data controllers to conduct Data Protection Impact Assessments (DPIA). DPIA's need to be done when data processing is likely to result in high-risks to the rights and freedoms of the data subjects. DPIA's also should be conducted in connection to profiling and large-scale processing of sensitive personal data. This can be seen as a particularly a broad requirement which will convert DPIA into a precautionary tool which will

delay the delivery of innovative products and services (S24 (1) PDPA 2022). In addition, PDPA 2022 classifies data into two identical categories as personal data and special categories of personal data. However, it's been criticized as it is somewhat problematic.

Yet PDPA 2022 is not effective. Nevertheless there are several ancillary legislative provisions that can be applied to certain aspects of the data protection and privacy. Apparently, said legislations and policy frameworks are inadequate and doesn't provide an effective protection to the data and privacy. Therefore, there is no guarantee for the people living in Sri Lanka regarding the safety of their personal data and their personal data is likely to be misused without their knowledge and/or consent. Hence introducing a specific legislation to ensure data protection and privacy of the persons can be deemed as a crucial requirement.

PDPA 2022 to can be identified as a major step relating to the data protection and privacy in Sri Lanka as it consists of following aspects as discussed in the above sections; extra territorial scope, data classification, lawful grounds for data processing, obligations of data controllers and processors, cross-border data flows, rights of the data subjects etc. It can be suggested that followings factors also must be taken into the account when enforcing this legislation; including a specific exception to ensure that Right to Information Act will not be overridden in any case of inconsistency, impartial data protection authority without governmental intervention, removal of the financial data and personal data relating to offences/criminal proceedings and convictions from the special categories of personal data to ensure further access to information (Madushani, 2021).

Uk and Singapore Standards on Data Protection and Privacy

Usually, the protection of data and privacy requires a holistic approach which is a combination of legal, administrative and technical safeguards. In this section, researchers will assess the effectiveness of the data protection and privacy laws of UK and Singapore. The primary purpose of this section is to identify their best practices and emerging trends on data protection and privacy that can be adopted into the Sri Lankan context.

Data protection and privacy in UK

UK recently passed a legislation to supplement the data protection requirements which is in line with the EU General Data Protection Regulations (GDPR). Data Protection Act (DPA) 2018 came into force on 25th May 2018 by repealing the Data Protection Act 1998 and EU Data Protection Directive 95/46/EC which regulates the collection and processing of personal data across all the sectors of economy. DPA 2018 primarily specifies the application of GDPR into UK. Though UK voted to leave European Union in 2016 under the withdrawal agreement among UK and EU, they agreed to continue the application of GDPR until the end of the implementation period. Subsequent to this transition period GDPR was incorporated into the UK law as the UK GDPR. UK GDPR can be deemed as the domestic law (O'Donoghue et al., 2021).

Data Protection Act 2018 (DPA)

DPA 2018 can be split into six key parts; (a) general processing. (b) law enforcement processing. (c) intelligence service processing. (d) data supervisory authority UK. (e) information commissioner's office (ICO). (f) enforcement and (g) supplementary and final provisions. Under the DPA 2018 everyone is responsible for using personal data subject to the strict rules known as "data protection principles". Accordingly, everyone is obliged to make sure that information will be used; fairly, lawfully and transparently, to use information for specified, explicit purposes, in a limited manner or only for what it is required for, to keep data for no longer than it is necessary, moreover to handle data by ensuring appropriate security, protecting against unlawful/unauthorized processing, access, loss, destruction or damage (www.gov.uk/data-protection, 2021).

Under DPA 2018 individuals has a right to find out what information the government and other organizations store about you. This right include followings as well; to know how your data will be used, to update the incorrect data, to erase data, to stop/restrict processing of your data, object how your data is processed under certain instances. In addition to aforesaid rights when a particular organization is using your personal data for; automated decision making without any human involvement or profiling for predict or behavior individuals can exercise aforesaid rights. It is clear that DPA 2018 simply regulates how data can be lawfully collected, processed and used in UK (www.gov.uk/data-protection, 2021).

UK General Data Protection Regulation (GDPR)

Enactment of UK GDPR can be seen as a progressive step since its provisions were articulated based on domestic requirements. It is arguable that rather than blindly following the international standards countries must always attempt to adapt their own version of law based on their economic, social and political standards without disregarding the international best practices. UK's post Brexit version of GDPR is substantially similar to the EU regulation and it also places similar obligations on data controllers and processors (Carey and Treacy, 2015). The UK GDPR is supplemented through the DPA 2018. DPA 2018 applies the provisions of GDPR to certain matters those are outside its regulation scope including; processing by public authorities, moreover it set out data processing regimes for law enforcement processing and intelligence processes. Hence, it's clear that DPA 2018 and UK GDPR exists concurrently.

UK GDPR is applicable to UK organizations that collect, store or otherwise process the personal data of the persons residing in UK and non-UK organizations that offer goods/services or monitor the behavior of the UK residents. This measure ensures that both UK organizations and non-UK organizations will strictly adhere into these data protection laws. Organizations functioning in UK should adhere into these two data protection laws; (a) DPA 2018 and UK GDPR if they process only domestic personal data. (b) DPA 2018, UK GDPR and EU GDPR if these organizations offer good/services and monitor the behavior of the EU citizens. This clearly shows that even if UK has their own domestic law to regulate data protection, application of EU GDPR into certain aspects still effective.

Similarities of UK GDPR and EU GDPR can be listed as follows; **(a) accountability and governance** – data controllers must demonstrate their compliance with law by adopting following measures; keep a detailed record of all data protection regulations, carrying out data protection impact assessments regarding high-risk processing operations, implementation of technical/organizational measures etc. (General Data Protection Regulation Art 5 (2)). **(b) six data processing principles;** data controllers are required to follow six data processing principles – **(i) lawfulness, fairness and transparency** - they are obliged to process personal data lawfully/fairly and transparently and collect data only for legitimate purposes (Data Protection Act 2018, s35: General Data Protection Regulation Art 5 (1) (a)).

(ii) purpose limitation - adequate/relevant and limit to what is necessary (Data Protection Act 2018, s36: General Data Protection Regulation Art 5 (1) (b)). **(iii) data minimization** – accurate, relevant and limit to what is necessary (Data Protection Act 2018, s37: General Data Protection Regulation Art 5 (1) (c)). **(iv) accuracy** – processed personal data must be accurate and up to date if personal data is inaccurate/misleading they should be rectified or erased (Data Protection Act 2018, s38: General Data Protection Regulation Art 5 (1) (d)). **(v) storage limitation** – personal data shall not be kept stored for any longer than it is necessary for a specific purpose. Data controllers can delete the unnecessary data (Data Protection Act 2018, s39: General Data Protection Regulation Art 5 (1) (e)). (vi) **integrity and confidentiality (security)** – personal data processed for any of the law enforcement purposes must be processed in a manner that ensures security of the personal data using appropriate technical and organizational measures (Data Protection Act 2018, s40: General Data Protection Regulation Art 5 (1) (f)). These data protection principles indeed prevent/minimize possible data breaches.

Under UK GDPR data subjects are given following rights – right to be informed, right to access, right to rectification, right to erasure, right to object etc. (www.gov.uk, 2021). Unless data subjects are given such rights enforcement of the obligations imposed under DPA 2018 and UK GDPR would not be fruitful. Furthermore, UK GDPR permits the transfer of personal data in certain circumstances. E.g. – where destination country provides an adequate level of data protection primarily through Standard Contractual Clauses (SCCs) and complying with an approved certification mechanism. It is another viable measure which ensure that data of the UK personals will be protected outside the country. These are only few key features of the UK GDPR. Apparently, there are multiple benefits of GDPR compliance including; building the trust of customers, reducing the risk of data breaches, increasing privacy and information security etc.

EU General Data Protection Regulation (GDPR)

Some crucial aspects of the EU GDPR will be discussed herein to determine the similarities and variances between the EU GDPR and UK GDPR. Article 2 of the EU GDPR explains its general scope as; processing of personal data wholly/partly by automated means or processing personal data other than by automated means. As per Art 4 of the EU GDPR any treatment of data will be considered as processing including; collecting, organization, structuring, erasing

of data. It's clear that EU GDPR interprets its scope in a broader manner in order to ensure high level of protection (Arts 2, 4).

Although it has data protection in its name EU GDPR is equally concerned about the data privacy as well (Clifford et al., 2018). The primary aim of EU GDPR is to harmonize data privacy laws across Europe in order to protect sensitive data of EU citizens (Voigt and Bussche, 2017). Apparently, followings are the basic principles of EU GDPR; (a) lawfulness, fairness and transparency. (b) purpose limitation. (c) data minimization. (d) accuracy. (e) storage limitation. (f) integrity & confidentiality. (g) accountability. (h) lawfulness. It is clear that EU GDPR is more concerned about rights of the individuals before business interests (IT Governance, 2017).

Criticisms against data protection and privacy laws in UK

UK has been recognized as one of the world's most progressive data protection and privacy regimes. Thus it still contains several retrograde elements including some gaps and contradictions. First criticism is the provisions of the DPA 2018 grants an unacceptable power to alter the provisions of the GDPR. E.g. – conditions relating to the processing of personal data. However, UK government had justified this as giving flexibility to deal with changing circumstances. Moreover DPA 2018 does not provide adequate safeguards in connection to the exceptions to the prohibition set out in Article 22 of the GDPR or the automated decision making without the human intervention. E.g. – need of transparency in connection to automated decision making.

It is also arguable that DPA 2018 is quite comprehensive and covers wide range of subject matters hence it is complex. DPA 2018 does not clearly explain what will happen to the personal information of the persons or what they should do when their personal information been misused or there is no sufficient judicial remedy against data breaches. National security concerns have exempted wide range of bodies from data protection oversight. Moreover DPA 1988 grants unfettered powers to the intelligence agencies to transfer personal data across borders without adopting appropriate safeguards. Apparently DPA 2018 is not welcomed by all, according to critics this legislation requires increased transparency and accountability from organizations also more stronger rules to protect loss of data and theft including serious sanctions and fines against those who deliberately/negligently misuse data (Ashford, 2018).

Data Protection and Privacy in Singapore

Sub-Committee for Technology & Law Reform Committee of the Singapore Academy of Law showed three primary reasons for introducing a data protection law in Singapore; (a) to protect the interests of the individual data subjects in view of the fundamental nature of privacy rights. (b) to provide standards of conduct for data users. (c) to adhere into international data protection standards (Law Reform Committee, 1990). Personal Data Protection Act (PDPA) provides a baseline standard of protection for personal data of the persons. Equivalent to UK, Singapore's legal framework on data protection and privacy is also focusing on their domestic requirements.

PDPA 2012 regulates how personal data is handled, it simply set out an overreaching data protection framework in relation to collection, use, disclosure and protection of personal data by private sector organizations. There are two major legislative purposes to the PDPA.; to recognize the individual's right to data protection and to develop trust in data protection in Singapore. More importantly it imposes nine data protection obligations on organizations operating in Singapore, that are enforceable through a private action or public enforcement (Benjamin, 2017).

In addition, Model Data Protection Code (2002) intended to facilitate two distinct functions; (a) operational function – which is to establish minimum acceptable standards for data protection. (b) facilitative function – to promote the harmonization of data protection rules among different sectors. However, it was emphasized that this Model Code consist of several shortcomings in relation to its scope, processes and enforcement (National Internet Advisory Committee, 2002). At present Model Code 2002 and PDPA 2012 is applicable to the private sector and other pre-existing legislation and internal rules are applicable to the public sector (patchwork laws such as common law, sector specific legislations and various other self-regulatory or co-regulatory codes (Chesterman, 2012).

Key principles underpinning the PDPA 2012 will be discussed herein. **(a) consent;** organizations must obtain the consent of the individuals before collecting, using or disclosing personal data for a particular purpose unless said act/s subject to an exception (Personal Data Protection Act 2012, s13 – 17). **(b) purpose limitation;** organizations may collect use, disclose personal data only for specified purpose/s (Personal Data Protection Act 2012, s18 – 20). **(c) deemed consent;** an individual is deemed to consent to collection, use or

disclosure of his/her personal data if said individual provides personal information to a particular organization voluntarily. **(d) withdrawal of consent;** individuals are capable of withdrawing their consent at any time in connection to collection, use or disclosure of their personal data (Personal Data Protection Act 2012, s18 – 20).

(e) reasonableness; organizations are allowed to collect, use or disclose personal data if the data was collected would be considered appropriate. **(f) accuracy;** organizations shall always take reasonable steps to ensure that the collected personal data is accurate (Personal Data Protection Act 2012, s23). **(g) protection obligation;** organizations are obliged to protect personal data in its possession/control (Personal Data Protection Act 2012, s24)**. (h) retention limitation obligation;** this limits the power of an organization to retain personal data if retention is no longer required (Personal Data Protection Act 2012, s25). **(i) transfer;** organizations are bound not to transfer personal data outside the Singapore if such personal data cannot be protected effectively (Personal Data Protection Act 2012, s26). All these principles attempt to prevent/minimize possible personal data violations.

Additionally, to the framework set out in the PDPA 2012 there are some other sources that deals with the data protection and privacy in Singapore but PDPA serve as the key statute. In Singapore banks are regulated by Banking Act 2008 which contain rules on banking secrecy. The primary rule that deals with the banking secrecy is the s47 (1) which specifies that customers information shall not be disclosed by any of the bank/its officers to any other person unless expressly provided in the Act (Banking Act 2008, s47 (1)). E.g. – to safeguard the interest of the bank or public, implied/express consent of the customer etc. (*Susilawati v American Express Bank Ltd [2007] SGHC 179*). Human Biomedical Research Act 2015 also contain provisions to protect the privacy of the research subjects (Human Biomedical Research Act No 29 of 2015).

Enforcement Mechanisms

Singapore introduced an institutional framework consisting two regulatory bodies to deal with data protection and privacy; **(a) The Personal Data Protection Commission (PDPC)** – PDPC mainly deals with the administration of PDPA 2012 or in other words it is Singapore's Data Protection Authority (Personal Data Protection Act 2012, s7), **(b) Data Protection Appeal Panel (Appeal Panel)** – the appeal panel is an independent appellate body to

directions/decisions of PDPC may be appealed. These enforcement mechanisms primarily focus on achieving legislative purposes.

Criticisms against Data Protection & Privacy laws in Singapore

There are multiple criticisms against the data protection and privacy regime in Singapore. Some critics argue that safeguards offered through the PDPA 2012 are far weaker than how it appears. Apparently PDPA facilitates the collection, use and disclosure of personal data though it is against such acts. Another criticism against PDPA is obligations on collection, use and disclosure of personal data are not applicable to certain classes of actors such as public agencies/government etc. "Data anonymization" can be recognized as another issue associated with the PDPA.

Data anonymization means the conversion of personal data into data not referable to identify any individual. PDPA approach allow organization to have two parallel sets of personal data and its problematic (Benjamin, 2017). Moreover, PDPA is not applicable to the business application information or PDPA expressly excludes business contact information. (Personal Data Protection Act 2012, s4 (5)). Business contact information exclusion can be recognized as ostensibly a broad approach and another problematic area of PDPA.

In this section researchers primarily assessed the effectiveness of the data protection and privacy laws of UK and Singapore. Similar to many countries around the world UK have passed a legislation (DPA 2018) which is designed to supplement the data protection requirements in line with the EU GDPR. UK is one of the first countries to implement GDPR in local law which is known as UK GDPR. Thus, still there are certain criticisms against the data protection and privacy regime in UK.

In the same section data protection and privacy laws in Singapore also been assessed. Singapore enacted PDPA 2012 and it provides a baseline standard of protection for personal data of the persons. In addition, Singapore has a sector-specific regulatory framework. When compared to the UK's legal framework Singapore's data protection and privacy regime seems to be slightly unique. While GDPR and PDPA 2012 bear some similarities and differences UK GDPR is more like a copy of EU GDPR. After considering the legal frameworks prevailing in UK and Singapore, it is apparent that there is a huge gap/lacuna in Sri Lankan law in relation to the data protection and privacy.

Hence it can be suggested that Sri Lanka should consider the legal standards that have been adopted by both UK and Singapore in articulating its data protection and privacy law/s. By observing the legal standards adopted by UK and Singapore Sri Lanka can develop its own data protection and privacy framework which is suitable for Sri Lanka's economic, social and cultural needs. Moreover, Sri Lanka can take into account the criticisms presented against data protection and privacy regime in UK and Singapore before articulating the Sri Lankan legal framework on this subject matter as it will be helpful to minimize the possible flaws.

Findings and Recommendations

Findings

According to the facts presented in the previous sections, it appears that providing an equal and universal privacy and data protection framework is not an easy task. However, it is essential to provide at least basic/minimum standards relating to the data protection and privacy. The lack of a comprehensive legislation pertaining to data protection and privacy in Sri Lanka has always been a matter of concern. This concern has been particularly expressed by academics, professionals and individuals and more importantly the foreign investors and firms that are doing business in Sri Lanka.

Undoubtably existence of an effective and efficient data protection and privacy legal framework will ensure the security of the data of the persons from unauthorized collection, usage, transfer, and from disclosure. Differ to the Sri Lankan approach most of the countries around the world including UK and Singapore have enacted separate legislations to regulate data protection and privacy primarily to meet their domestic requirements. Apparently Sri Lanka was reluctant to introduce a proper law to regulate data protection and privacy mainly due to the existing economic, social and political factors.

Since there was no specific statute to regulate data protection and privacy in Sri Lanka until very recent several other data protection and privacy enabled legislations such as; Computer Crimes Act No. 24 of 2007, Telecommunication Act No. 25 of 1991, Banking Act No. 30 of 1988 Intellectual Property Act No. 36 of 2003 etc. were applied to regulate certain aspects of the data protection and privacy and said legislations could ensure protection of data and privacy up to some extent. However, these legislations are incapable of providing an

effective protection to data/privacy since main objective of these legislations is not to protect data/privacy.

As mentioned in the previous sections there is an inseparable connection between the data and privacy. Privacy is important to protect personal or commercial data from the unauthorized access. Privacy is recognized as a fundamental human right in many international human rights treaties. E.g. - Article 12 of the UDHR and the Article 17 of the ICCPR. Thus, Sri Lankan constitution do not recognize right to privacy as a fundamental right. Though existence of right to privacy is important in multiple ways. One of the main significances right to privacy is it can automatically protect data of the persons and organizations as no one can arbitrarily interfere or collect the data of the others without authority.

In Sri Lanka there is no balance between the right to privacy and right to information. As there is a legislation on right to information but right to privacy is not specifically recognized. Government of Sri Lanka had a great power to collect and control data of persons and organizations while citizens of the country are incapable of protecting their data and privacy until the enactment of Personal Data Protection Act No. 09 of 2022 also individuals/entities were incapable of bringing actions against those who violates data protection and privacy rights due to the non-existence of proper legal framework (Marsoof, 2008). Thus, it is also noteworthy that Personal Data Protection Act No. 09 of 2022 is a very recent enactment therefore no one can guarantee its effectiveness.

Thus, Personal Data Protection Act No. 09 of 2022 can be identified as a comprehensive legislation. But it still lacks the international consistency in relation to the regulation of certain aspects of privacy. Moreover, it is likely to further restrict international trade and investment. It is also suggestable that creation of legislation blindly following other jurisdictions or international standards is not an effective solution but countries should identify their specific needs and articulate their own laws while learning lessons from the experiences of other countries.

Based on these findings this study concludes that as a country which deals with the modern technological developments Sri Lanka need to have an effective legal framework to deal with data protection and privacy compared to UK and Singapore.

Recommendations

Based on the above findings following recommendations can be made;

(a) Government must take immediate steps to enforce Personal Data Protection Act No. 09 of 2022 as it can be identified as a legislative priority.
(b) It is essential to ensure that individuals are capable of bringing actions against data violations under the Personal Data Protection Act No. 09 of 2022 in an effective manner. Unless there is such definite enforcement mechanism assurance of compliance would be challenging and legislation would become a mere piece of paper.
(c) Government must ensure the independence of the Data Protection Authority, so that its members need to be appointed by an independent body rather than the government itself.
(d) Data protection obligations should be applicable to organizations of all sizes and across all industrial sectors. More precisely data protection and privacy obligations need to be applied without any categorization based on the nature, size or business place of the organizations.
(e) Imposing obligations on data controllers and processors to implement organizational and technical measures in order to make data processing principles more effective. E.g. – organizations can use Data Protection Impact Assessment (DPIA) which is a privacy related impact assessment to identify and analyze how data privacy is likely to be affected via certain actions or activities.
(f) It is essential to strike a balance between the interests of the data subjects, data users and the wider community. This can be done by placing them on equal footing yet priority must be always given to the rights of the data subjects.
(g) Cross-border transmission of personal data of the Sri Lankan nationals shall be done only with the consent of the data subjects and only if the recipient country has adequate laws to protect personal data and privacy of the persons. As if a particular country do not have adequate and effective laws/regulations to protect data and privacy of the individuals securing personal data outside the country would be problematic.
(h) Sri Lanka must recognize right to privacy of the persons as a basic/fundamental right as existence of Right to Information Act No. 12 of 2016 without right to privacy is controversial. Further recognition of right to privacy is crucial when ensuring data protection since these two concepts exist simultaneously in certain circumstances.

Conclusion

It is conclusive that data protection and right to privacy is uncontroversial in countries like UK and Singapore as they have given proper attention to ensure

said rights. However, Sri Lanka has a different perception on data protection and privacy when compared to UK and Singapore. Until very recent Sri Lanka did not value the importance of data protection and privacy, best practical example is Sri Lankan Constitution do not recognize privacy as a fundamental right of the persons and even though Personal Data Protection Act No. 09 of 2022 was enacted recently it is yet to be enforced. In contrary countries like UK and Singapore has given more attention towards the data protection and privacy as they always intents to promote the rights of their citizens (Erbelding, 2019). Arguably Sri Lanka was reluctant to introduce adequate and effective law to regulate data protection and privacy due to numerous reasons such as; political issues, funding issues, inability of proper enforcement of laws due to human and technical resource restrictions, inadequate IT infrastructure, incapability or unwillingness to handle cross-border requests for data etc. As a result, data protection and privacy was protected through indirect and ineffective means. But use of inappropriate mechanisms to regulate data protection and privacy cannot be approved as it is obviously detrimental to the rights of the interested parties. Hence it is conclusive that Sri Lanka must enforce Personal Data Protection Act No. 09 of 2022 with immediate effect to safeguard data protection and privacy of the persons.

This research study provides a basic guideline to the policymakers in Sri Lanka on how prevailing data protection and privacy regime need to be improved as non-existence of specific/separate law to deal with data protection and privacy can be identified as a considerable gap in law. Notably primary aim of the researchers was to identify the adequacy and effectiveness of the existing Sri Lankan law on data protection and privacy compared to UK and Singapore. In addition, researchers focused on establishing the need of specific/separate legislation to deal with data protection and privacy based on the experience of UK and Singapore. The future researchers will be able to evaluate the effectiveness of the Personal Data Protection Act No. 09 of 2022 ***Sri*** Lanka which is supposed to be enforced in near future.

Declaration of Conflicting Interests

The authors declared no potential conflicts of interest with respect to the research, authorship, and publication of this article.

References

Abeysekara, T.B., (2015). Computer Crimes; Endless Race of Road Runners, *JSA Law Journal*, 3, 127-141.

Abeysekara,T.B., and Peiris, H.A.M. (2017). Legal and Engineering Aspects of Deployable Black Boxes with Video Recording Capability. *International Journal of Multidisciplinary Studies*, 4(1), 40-47.

Ariyaratna, R., (2016). Contracting in Cyber Space; A Comparative Analysis of Electronic Transaction Law in Sri Lanka, *Proceedings in Law, 9th International Research Conference – KDU Sri Lanka*, 1, 39-44.

Ashford, W. (2018). New UK Data Protection Act Not Welcomed by All, (2018). https://www.computerweekly.com/news/252441814/New-UK-Data-Protection-Act-not-welcomed-by-all, accessed February 14, 2022.

Bainbridge., D. (2007). *Introduction to Information Technology Law*. Harlow: Pearson Education, UK.

Benjamin, W.Q. (2017). "Data privacy law in Singapore: The Personal Data Protection Act 2012", *International Data Privacy Law*, 7(4), p. 287-302.

Carey, P. and Treacy, B. (2015). *Data protection: a practical guide to UK and EU law*, 4th edn, Oxford University Press.

Chesterman S., (2012). After Privacy: The Rise of Facebook, the Fall of WikiLeaks, and Singapore's Personal Data Protection Act 2012, *Sing JLS*, 391, p. 414.

Clifford D., Ausloos J., (2018). "Data Protection and the Role of Fairness", *Yearbook of European Law*, 37, p. 130.

De Soyza, S. (2017). Right to Privacy and a data protection Act; need of the hour, (*Daily*, 31st March 2017)

Erbelding., (2019). Cornelius, Privacy Perception in Developing Countries, 1, researchgate.net, https://www.researchgate.net/publication/337211237_Privacy_Perception_in_Developing_Countries, accessed February 14, 2022. .

GOV.UK, "Data Protection" <https://www.gov.uk/data-protection> accessed August 17, 2021

Greenleaf, G., (2017). Privacy in South Asian (SAARC) States: Reasons for Optimism, *Privacy Laws & Business International Report*, 149, 18-20.

Hutchinson T., Duncan, N., (2012). Defining and Describing What We Do: Doctrinal Legal Research, *Deakin. L. Rev* , 17(1), p.84.

IT Governance, *EU General Data Protection Regulation (GDPR); an implementation and compliance guide* (2nd edn. Ely Cambridgeshire UK, 2017).

Koops, B., (2014). The Trouble with European Data Protection Law, *International Data Privacy Law*, 4, p.250.

Law Reform Committee, (1990). Data Protection in Singapore: A Case for Legislation, Singapore Academy of Law Working Paper No 1.

Madushani, P. (2021). *Legislative Brief; Personal Data Protection Bill 2021*, (Transparency International Sri Lanka 2021) https://www.tisrilanka.org/wp-content/uploads/2021/07/TISL-

Marsoof, A., (2008). The Right to Privacy in the Information Era: A South Asian Perspective *SCRIPT-ed*, 5(3), Available at SSRN: https://ssrn.com/abstract=1578222.

Nadkarni, P. (2016). *Clinical Research Computing: A Practitioner's Handbook*, Elsevier Science & Technology.

National Internet Advisory Committee (2002). Model Data Protection Code for the Private Sector, Singapore Law Reform Commission, 5, http://www.commonlii.org/sg/other/SGLRC/report/R5/5.html

O'Donoghue C., O'Brien J., (2021). 'Data Protection Act 2018 Comes into Force', <https://www.technologylawdispatch.com/2018/06/privacydata-protection/data-protection-act-2018-comes-into-force/> accessed 14 August, 2021

Rouse M, "What Is Data Protection and Why Is It Important? *Definition from WhatIs.com"* <https://searchdatabackup.techtarget.com/definition/data-protection> accessed April 28, 2021.

Rowland, D., Andrew Charlesworth, and Uta. Kohl. *Information Technology Law* (4th Ed. London; New York: Routledge, 2012)

Senarathna, N. (2020). 'Talkingeconomics - The Growing Need for Privacy and Data Protection in Sri Lanka' (*Ips.lk*, 2020) <http://www.ips.lk/talkingeconomics/2020/01/13/> accessed April 28, 2021.

Sooriyabandara, V., (2016). Balancing the Conflict between Right to Information and Right to Privacy under Sri Lankan Fundamental Rights Perspective, *Sabaragamuwa University Journal*, 15(1), p.1.

Stefan, D., Jordan F., (2019). The General Data Protection Regulation: What U.S.-Based Companies Need to Know, *The Business Lawyer*, 74(1), 205-215.

UNCTAD, (2021) "Data Protection and Privacy Legislation Worldwide" <https://unctad.org/page/data-protection-and-privacy-legislation-worldwide> accessed August 14, 2021

Voigt, P., Von dem B. (2017). *The EU General Data Protection Regulation (GDPR) A Practical Guide*, 1st ed, Cham: Springer International Publishing.

Warren, S.D., Brandies, L.D., (1890). The Right to Privacy, *Harvard Law Review*, 4(5), 193–220.

Acts/Bills

Banking Act No. 30 of 1998

Computer Crimes Act No. 24 of 2007

Constitution of the Democratic Socialist Republic of Sri Lanka (1978)

Data Protection Act 2018 (UK)

Data Protection Bill (2019)

Electronic Transactions Act No. 19 of 2006

EU Data Protection Directive 95/46/EC

EU General Data Protection Regulation (EU GDPR)

Human Biomedical Research Act 2015 (No 29 of 2015)

Intellectual Property Act No. 36 of 2003
International Covenant on Civil and Political Rights (ICCPR)
Personal Data Protection Act 2012 (Singapore)
Personal Data Protection Act No. 9 of 2022
Right to Information Act No. 12 of 2016
Telecommunication Act No. 25 of 1991
UNCTRAL Model Law on Electronic Commerce and UN Electronic Communication Convention (1996)
Universal Declaration of Human Rights (UDHR)

Cases

Channa Peries vs. AG (1994) 1 SLR 1
Douglas v. Hello Ltd & Ors [2005] All ER 128
Nadarajah v Obeysekera [1971] 52 NLR 76
Sinha Ratnatunga v The State, [2001] 2 SLR 172
Susilawati v American Express Bank Ltd [2009] 2 SLR(R) 737