Are SMEs and Journalists Safe under Sri Lanka's Data Protection and Privacy Regime? Lessons from the EU and UK for an Effective Legal Framework

Pattiarachchige Nelsani Udeshika Pattiarachchi

Master of Arts (By Research)

University of York

Law

September 2025

ABSTRACT

In the digital era, personal data has become a valuable asset across many sectors in Sri Lanka. Previously, Sri Lanka lacked proper data protection legislation before enacting the 'Personal Data Protection Act No. 9 of 2022' (PDPA). However, the effectiveness of this act remains uncertain, as it is the latest legislation, and the implementation process is still underway. This research primarily evaluates the effectiveness of the current legal framework governing data protection and privacy in Sri Lanka, with particular focus on SMEs and journalistic purposes, in comparison with the EU and the UK. The study mainly adopts a doctrinal approach, with comparative analysis across selected jurisdictions. The findings reveal that the PDPA does not fully conform to international standards and is not sufficiently tailored to SMEs and journalistic purposes compared to the EU and UK data protection laws. In conclusion, this research offers recommendations to address the challenges identified.

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

(CCA) Computer Crimes Act, No. 24 of 2007

(CJEU) The Court of Justice of the European Union

(CPA) Centre for Policy Alternatives

(DCS) Department of Census and Statistics

(DPA 2018) Data Protection Act 2018

(DPA) Data Protection Authority

(DPD) Data Protection Directive

(DPIA) Data Protection Impact Assessments

(DPO) Data Protection Officer

(ECHR) European Convention on Human Rights and Fundamental Freedoms

(ECtHR) European Court of Human Rights

(EDPB) European Data Protection Board

(ETA) Electronic Transactions Act, No.19 of 2006

(EU) European Union

(GBP) Great Britain Pound

(GDPR) General Data Protection Regulation

(GSLI) Global Services Location Index

(GDP) Gross Domestic Product

(ICCPR) International Covenant on Civil and Political Rights

(ICO) Information Commissioner's Office

(ICT) Information Communication Technology

(IDTA) International Data Transfer Agreement

(IT) Information Technology

(MSMEs) Micro, Small and Medium-Sized Enterprises

(OECD) Organization for Economic Co-operation and Development

(PDPA) Personal Data Protection Act, No 9 of 2022

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

(SCCs) Standard Contractual Clauses

(SMEs) Small and Medium-Sized Enterprises

(UDHR) Universal Declaration of Human Rights

(UK) United Kingdom

(US) United States

(WWW) World Wide Web

ACKNOWLEDGEMENT

I would like to use this wonderful opportunity to express my sincere gratitude and respect to my dissertation supervisors, Prof. T.T. Arvind and Dr Dimitrios Tsarapatsanis, who have been the major supporters and encouragers of this work from the moment the research proposal was conceived. Their invaluable support and guidance encouraged me to do this work successfully.

I also wish to thank the MA (by research) degree coordinators for their ongoing support. Finally, I am profoundly grateful to my parents, my husband, and all those who helped me complete the Master's programme at the University of York.

DECLARATION

I declare that this thesis is a presentation of original work and I am the sole author. This work has not previously been presented for a degree or other qualification at this University or elsewhere. All sources are acknowledged as references.

CHAPTER 1

INTRODUCTION

1.1 The Background

The main purpose of this research is to appraise the efficacy of the current legal regime regarding data protection and privacy in Sri Lanka, with special reference to Small and Medium-sized Enterprises (SMEs) and journalistic purposes, compared with the European Union (EU) and the United Kingdom (UK), and make recommendations for creating an effective legal regime to regulate data protection and privacy with the balance between other rights such as right to information based on the emerging technology environment in Sri Lanka.

Data can be regarded as the most precious resource in the modern world.[1] Also, Personal data holds significant importance in the digital age.[2] Due to the significant growth of the internet and technology, digital transactions are rapidly increasing, and online consumers are more vulnerable in the virtual market. Similarly, Sri Lanka has been one of the developing countries with an open market economy since 1977. Therefore, in the digital era, personal data has become a significant asset in many fields in Sri Lanka.

There are many reasons for having a strong legal framework for protecting personal data. Data is one of the most important assets of a company in the development of transactions

[1] The Economist, 'The world's most valuable resource is no longer oil but data' (*economist.com*, 6th May 2017) <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data> Accessed 12 December 2024.

[2] Grant Longstaff, 'The importance of data privacy law in the digital age', 11 October 2024, Accessed 12 December 2024.

through technology, which is associated with the advancement of modern technology. [3] As the data economy has expanded, businesses have increasingly recognised the importance of gathering, exchanging, and utilising data. Also, the rapid growth of online services in Sri Lanka can be identified, and transportation apps like Uber, Pick Me, and Loyalty Card Systems are examples. In addition, people share data through social media platforms. Also, the banking, educational, telecommunication, and hospitality sectors collect huge volumes of personal data for daily transactions. These data can be misused frequently. Therefore, personal data is at great risk in that current situation. As a result, data protection is a critical issue that must be resolved.

The country lacked dedicated legislation addressing data protection and privacy before enacting the 'Personal Data Protection Act, No. 9 of 2022' (PDPA). Instead, only a limited number of provisions scattered across various statutes provided indirect coverage of these issues, such as the 'Post Office Ordinance No.11 of 1908',[4] 'The Telecommunication Act, No. 25 of 1991',[5] 'The Electronic Transaction Act, No.19 of 2006'[6] (ETA), 'The Payment Devices and Frauds Act, No.30 of 2006'[7], 'The Computer Crime Act, No.24 of 2007'[8] (CCA), 'The Right to Information Act, No.12 of 2016'[9] (RTI) etc.

Also, in Sri Lanka, the right to privacy is not explicitly guaranteed in the constitution and is protected as a concept of 'delict' called *actio injuriarum*. It is a standalone remedy

---

[3] Jeff Petters, 'Data Privacy Guide: Definitions, Explanations and Legislation' (Varonis,28 September 2020) accessed 10 February 2025.

[4] The Post Office Ordinance No 11 of 1908, s 75.

[5] The Telecommunication Act, No. 25 of 1991, s 52, s 53.

[6] The Electronic Transaction Act, No.19 of 2006.

[7] Payment Devices and Frauds Act No 30 of 2006, s 3(d).

[8] The Computer Crimes Act, No. 24 of 2007, s 3, s 8, s 10, s 14.

[9] Right to Information Act, No. 12 of 2016, Part II, section 5(1) (a).

available for wrongful assaults on individuals, their reputation, or their dignity. This principle has evolved through case law. In the *Nadaraja v Obesekara*[10] case, the term 'Invasion of privacy' was examined. However, *actio injuriarum* may not be sufficient to address current data protection and privacy issues. Because this remedy has limitations and requires several elements to be satisfied for claims, it is not widely used.

In response to these shortcomings, the Sri Lankan Parliament enacted the PDPA on 19th March 2022, representing a significant effort to address the longstanding absence of a comprehensive legal framework for data protection in the country. Nevertheless, some issues regarding data protection and privacy have not yet been resolved, and there are some implementation issues regarding this new data protection law, such as the implementation issues regarding SMEs in Sri Lanka. According to the PDPA, all SMEs which process personal data should comply with the act. This will negatively affect SMEs, which hold minimal human and financial resources. As a result, all SMEs will have to face problems such as insufficient human resources, budget limitations, complexities in data processing, lack of awareness, etc. Also, an imbalance between data protection and the right to information, especially for journalistic purposes, is another issue under the PDPA.

Accordingly, this study aims to evaluate the sufficiency and effectiveness of the current legal regime governing data protection and privacy in Sri Lanka, with special reference to SMEs and a Journalistic perspective compared with the EU and the UK data protection laws, and propose an effective legal framework for Sri Lanka.

An effective data protection and privacy regime will be beneficial in preventing the misappropriation of data and protecting the rights of the people. Reconciling the right to privacy with the right to access information is important to ensure transparency and

[10] [1971] 52 NLR 76.

accountability while protecting personal data. Nevertheless, these laws should not negatively affect the SMEs, which play a major role in national economic development. 'The government of Sri Lanka recognises SMEs as the backbone of the economy, as they account for more than 75% of the total number of enterprises, provide 45% of the employment and contribute to 52% of the Gross Domestic Product (GDP).'[11]

Therefore, this study is crucial to the legal regime of Sri Lanka since the PDPA has just been passed, and the efficiency and effectiveness of this act are also to be tested. Hence, this research will assist in strengthening the data protection and privacy law regime in Sri Lanka. A comparative examination of the legal frameworks of the EU and the UK will help identify the gap and provide recommendations to solve the issues regarding SMEs and journalistic purposes to establish an efficient and well-regulated data protection and privacy system within the Sri Lankan context.

1.2 The Research Problem

Before the enactment of the PDPA, Sri Lanka did not have a dedicated law governing data protection. Certain provisions in various statutes offer indirect applicability to data protection and privacy. This issue is evident in the introduction of a few provisions in the CCA to address data protection.[12]

Nevertheless, some case laws have addressed the concept of privacy in Sri Lanka before adopting this new law. In the *Sinha Rathnathunga V. State*[13] case, the court accepted the concept of privacy. The Sunday Times newspaper's editor was charged with two counts of

[11] 'National Policy Framework for Small and Medium Enterprises (SME) Development', 2016, chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/http://www.sed.gov.lk/sedweb/en/wpcontent/uploads/2017/03/SME-fram-work_eng.pdf> Accessed 10 February 2025.

[12] The Computer Crimes Act, No. 24 of 2007, s.3, s.8, s.10, s.14.

[13] [2001] 2 SLR 172.

defamation under Sections 480 and 479 of the Penal Code, read with Sri Lanka Press Council Law, Section 15, since his article injured the reputation of the president of the country.[14] However, Sri Lankan courts have rarely addressed these data protection and privacy issues.

Even though the Sri Lankan Parliament passed the PDPA, the effectiveness of this act is still doubtful. It can be identified that several issues regarding this new law exist. The government has a large amount of control over the Data Protection Authority (DPA) under the PDPA. Also, the unclear wording of the act may have influenced the discouragement of foreign investment in Sri Lanka.

In particular, SMEs and journalists face many problems in implementing this new act. Therefore, this research is mainly focused on identifying the implementation issues of SMEs and journalists under the PDPA, critically analysing those issues, and providing recommendations for solving those issues.

Also, Chapter III of the 1978 Constitution of Sri Lanka sets out a range of fundamental rights. Nevertheless, it does not specifically acknowledge privacy as a constitutionally guaranteed right.

Therefore, I intend to examine why the current data protection legal regime in Sri Lanka is not sufficient to solve emerging issues on data protection and privacy regarding SMEs and journalistic purposes and analyse how Sri Lanka can learn lessons from the EU and the UK's data protection laws to solve those issues for creating an effective data protection and privacy regime.

[14] ibid.

1.3 Research Questions

1. What is the current legal framework governing data protection and privacy in Sri Lanka?
2. To what extent is the current legal framework sufficient for protecting the right to privacy?
3. What challenges have been faced by the SMEs and journalists under the PDPA?
4. What best practices from the GDPR of the EU and the Data Protection Laws of the UK could be adopted or adapted to strengthen data protection laws in Sri Lanka, and what recommendations can be made to solve the above-mentioned issues?

1.4 Objectives of the Study

The primary objectives of this research are outlined as follows.

- To analyse the current legal framework governing data protection and privacy in Sri Lanka.
- To evaluate the adequacy of the current legal framework to address the right to privacy in Sri Lanka.
- To appraise the challenges that have been faced by SMEs and journalists under the PDPA.
- To appraise the experience of the selected jurisdictions regarding the above-mentioned issues and make recommendations to solve those issues to create an effective legal framework in Sri Lanka.

1.5 Research Methodology

This research primarily adopts a doctrinal research methodology, complemented by a comparative legal analysis of selected jurisdictions. Additionally, a qualitative research paradigm is employed to critically and analytically examine the data.

Doctrinal research is characterised as 'a comprehensive and highly technical commentary on and methodical explication of the context of legal doctrine.' [15] Accordingly, by using the doctrinal research methodology, I intend to analyse the existing legal materials and aim to identify the deficiencies and gaps within Sri Lanka's data protection and privacy regime.

Also, I intend to do a comparative study under this research. I aim to examine the sufficiency and practical effectiveness of Sri Lanka's current legal framework governing data protection and privacy, with special reference to SMEs and journalistic purposes, compared with the EU and the UK data protection laws. Employing a comparative research methodology is advantageous for understanding the distinctions between various legal systems on a given issue, while also helping to identify knowledge gaps and offer fresh insights.

From my perspective, the EU was selected because it has the GDPR model that is the strongest and most effective worldwide[16] for a third country like Sri Lanka. It is recognised as the world's most powerful and comprehensive legal instrument for data protection and privacy. Also, the 'European Union's Charter of Fundamental Rights' (EU

[15] Michael Crotty, *The Foundations of Social Research: Meaning and Perspectives in the Research Process* (3rd edn, Sage Publications 2003) 1-233, 10.

[16] Council of the European Union, 'The general data protection regulation', < https://www.consilium.europa.eu/en/policies/data-protection-regulation/> Accessed 18 December 2024.

Charter)[17] represents the first legal instrument to enshrine data protection as a fundamental right.

The UK was selected because many former colonies still rely on the legal systems in the UK and Europe. Sri Lanka has a mixed legal system, and it is primarily based on the Roman-Dutch law. However, English Common Law has had a profound influence on the development of the Sri Lankan legal system, particularly during the period of British colonial rule. For instance, the *Sirimane vs. New Indian Assurance Company Limited* case[18] illustrates the importance of Sri Lankan lawyers in studying English Law. This is because most statutory laws are based on English Law principles, and even when statutory regulations are silent, the Sri Lankan legal system still follows and adopts English Law. Also, the UK has decided to leave the EU and passed a new data privacy law suited to its political, economic, cultural, and social needs. Therefore, Sri Lanka will be able to learn lessons from these laws to solve emerging issues relating to SMEs and journalistic purposes.

This study will utilise both primary and secondary sources to accomplish its objectives. Primary sources include relevant legislative enactments, international conventions, and case laws. Additionally, secondary sources such as textbooks, scholarly articles, journal publications, and other academic materials will be utilised to provide comprehensive analysis and support for the research.

1.6 Hypothesis

The present legislative framework does not provide adequate protection for the right to privacy in Sri Lanka. It is a great risk to individuals' personal data and privacy. Also, there

[17] European Union, Charter of Fundamental Rights of the European Union, 18 December 2000 (2000/C 364/01) (EU Charter).

.

[18] 35 NLR 413.

are some implementation issues of the PDPA regarding SMEs. It will affect the country's economy. The Sri Lankan data protection legal regime has not introduced exceptions for journalistic purposes under the PDPA. Therefore, the imbalance between the right to privacy and the right to information will negatively affect the protection of peace and human well-being of people and the country's development.

1.7 Significance of the Study

Currently, Sri Lanka is at a very early stage regarding this subject. Although the parliament passed the PDPA, the regulatory body, the DPA, is not yet fully functional. Section 1 of this Act specifies the procedure and time frames for coming into operation.[19] Accordingly, in August 2023, the DPA commenced operations as a government body. However, the implementation process of this act has not yet started. Therefore, this research is particularly crucial in the present context of Sri Lanka

As there are few comparative legal studies in this field in Sri Lanka, and there are no in-depth studies with special reference to SMEs and journalistic purposes. A comparative analysis with the legal systems of the UK and the EU will undoubtedly yield valuable insights and lead to well-founded recommendations for the Sri Lankan legal system.

The findings and proposals emerging from this research are expected to illuminate the potential pathways for legal reform. Consequently, the study will be of particular relevance and utility to Sri Lankan policymakers, legal reform committees, and other stakeholders engaged in shaping and modernising the country's data protection and privacy framework. Therefore, this research will play a valuable role in the advancement of Sri Lanka's legal framework.

[19] The Personal Data Protection Act No. 09 of 2022, s 1.

1.8 Limitations

In the world, data protection and privacy span a vast area and different angles. The safeguarding of personal data relies on both legal instruments and technological solutions. This research mainly focuses on the legal framework. Many countries around the world have enacted many laws to protect personal data. This research especially focuses on the EU and the UK's legal frameworks regarding data protection and privacy, specifically identifying issues about SMEs and journalistic purposes, and providing recommendations for solving those issues.

1.9 Chapter Outline

This thesis is composed of five chapters. The first chapter serves as the introduction and intends to give an overview of the study. The literature review is listed in the second chapter. Chapter three discusses Sri Lanka’s existing data protection and privacy law regime. Also, it will assess the challenges SMEs and journalists face under the current legal framework in Sri Lanka. Chapter four focuses on a comprehensive analysis of current legislation regarding data protection and privacy in the EU and the UK, and aims to identify best practices regarding SMEs and journalistic purposes. Chapter Five presents the recommendations and conclusions drawn from the research findings. Ultimately, it will offer guidance for implementing a robust legal regime to ensure data protection and privacy in Sri Lanka.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

This Chapter summarises the pertinent and valuable international and local literature published on the concepts in connection with the research. The review of the existing literature primarily aims to increase understanding of Sri Lanka's legal framework and create a theoretical foundation for the research. Therefore, this review commences with identifying the origins and evolution of data protection and the right to privacy. Secondly, I intend to outline the numerous definitions of data protection given by selected jurisdictions with the different branches of law, including the concept of privacy. Then, I intend to analyse Sri Lankan and international literature regarding personal data protection law and privacy with special reference to SMEs and journalism perspectives. By analysing international and domestic literature, I expect to highlight the current literature gaps and emphasise the significance of filling those gaps. Therefore, future researchers on this topic may benefit from this literature review.

2.2 Origins and Evolutions of Data Protection and Privacy

The fundamental basis of data protection laws is the right to privacy. The concept of privacy is expansive and includes various aspects. One such aspect is the protection of personal data. Thusitha B. Abeysekara and Amali E. Ranasinghe state: 'One of the main significances of the right to privacy is that it can automatically protect the data of persons

and organisations as no one can arbitrarily interface or collect the data of others without authority.'[20] It is thus crucial to explore the foundational origins of the right to privacy.

When the United States (US) Constitution was enacted in 1789, it contained no explicit provision for the right to privacy. Nevertheless, the Fourth Amendment stipulates: 'The right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated and no warrant shall issue…' [21] In addition to that, the case of *Katz v. United States*[22] extended the Fourth Amendment's safeguards beyond individual homes and property to any context in which an individual's expectation of privacy is deemed reasonable. Thus, it is recognised as a foundational element in developing the right to privacy within the 17th century.

The publication of the scholarly article, 'The Right to Privacy' in 1890, which described privacy as the 'right to be let alone,' was a landmark contribution to the legal and scholarly discussion of privacy.[23] Those Scholars state: 'The same protection is accorded to a casual letter or an entry in a diary and to the most valuable poem or essay, to a botch or daub and a masterpiece. In every such case, the individual is entitled to decide whether that which is his shall be given to the public.'[24] Accordingly, it can be argued that those scholars have emphasised the concept of privacy and the importance of protecting personal data.

---

[20] Thusitha B. Abeysekara and Amali E. Ranasighe, 'Holistic Approach in Introducing Proper Legal Framework to regulate data protection and privacy in Sri Lanka', Vidyodaya Journal of Management, 2022 vol 8(1) 169-200 Accessed 04 November 2024.

[21] United States Constitution, fourth amendment.

[22] [1967] 389 U.S.347.

[23] Samuel D Warren and Louis D Brandeis, 'The Right to Privacy' (1890) IV (5) Harvard Law Review 193 accessed 20 October 2024.

[24] ibid.

In 1967, Alan F. Westin laid the foundation for discussions on technology and individual liberty through his book, *Privacy and Freedom*.[25] This book examines the conflict between privacy and surveillance in modern society. However, it was written before the advent of the technological era. Therefore, it can be argued that the author lacks practical experience compared to today's digital age.

The 'Universal Declaration of Human Rights' (UDHR) is a landmark document, and its Article 12 explicitly enshrines the right to privacy.[26] Moreover, the 'European Convention on Human Rights' (ECHR), through Article 8, provides comprehensive protection for individual privacy. [27]

The above-mentioned literature has discussed the whole concept of the right to privacy. However, it is pivotal to understand the whole concept because data privacy is also derived from the overarching concept of the right to privacy. '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.'[28]

Juliane Kokott and Christoph Sobotta evaluate the difference between privacy and data protection through the lens of relevant jurisprudence from 'the European Court of Human

---

[25] Alan F Westin, *Privacy and Freedom*, 25 Wash. & Lee L. Rev. 166 (1968). accessed 20 October 2024.

[26] The Universal Declaration of Human Rights, art.12.

[27] Council of Europe, European Convention on Human Rights and Fundamental Freedoms, 3 September 1953, ETS 5, 213 UNTS 221, art 8.

[28] See n 20.

Rights' (ECtHR) and 'the Court of Justice of the European Union' (CJEU).[29] They emphasise that according to CJEU and ECtHR, the concept of 'private life' should not be interpreted narrowly and state: "[P]rivate life includes the protection of personal data….."[30]

Moreover, they examine the distinct provisions relating to data protection and privacy within the ECHR and the EU Charter. They point out Article 8 of the ECHR and Article 7 of the EU Charter, both of which enshrine the right to privacy.[31] Nevertheless, Data protection is clearly enshrined as a fundamental right in Article 8 of the EU Charter; the ECHR does not contain an explicit provision in this regard. They state that: 'In spite of the distinction between privacy and data protection laid down in the Charter, jurisprudence has justifiably considered privacy to be at the core of data protection.'[32]

Furthermore, they highlight the importance of identifying the difference between data protection and privacy by referring to *the Google Spain* case.[33] However, they do not provide explicit definitions of either term.

The evolution of data protection laws dates back to the 1970s.[34] The German federal state of Hesse pioneered the enactment of modern data protection legislation, prompted by

---

[29] Juliane Kokott & Christoph Sobotta, 'The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECHR' (2013) vol 3\4 International Data Privacy Law 222–228. accessed on 01 December 2024.

[30] ibid.

[31] ibid.

[32] ibid.

[33] *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* C-131/12 [2012] OJ C165/11.

[34] United Nations Conference on Trade and Development. *Data protecting regulations and international data flaws: Implications for Trade and Development* (New York and Geneva, 2016) <https://unctad.org/system/files/official-document/dtistict2016d1_en.pdf> accessed 25th October 2024.

growing concerns over advancements in computing and the privacy implications of processing personal data.[35] Hesse announced its 'Hessisches Datenschutzgesetz' in October 1970.[36] However, the scope of the Act was confined to regulating personal data usage in relation to land-related purposes.[37]

The first national privacy regulation, the Swedish Data Act, was established in Sweden in 1973.[38] The primary objective of this Act was to safeguard individuals against unwarranted intrusions into their privacy.[39] While the 'Hessisches Datenschutzgesetz' was limited to regulating data processing within the public sector, the 'Swedish Data Act' extended its scope to the private sector's use of computer technologies.[40]

The Privacy Act, enacted in the US in 1974, establishes comprehensive rules governing how federal agencies, including law enforcement bodies, collect, use, and disclose all categories of personal information.

After seven years of Hesse, Germany, also enacted a 'Federal Act on Protection against the Misuse of Personal Data in Data Processing' on 27th January 1977. According to Jef Ausloos, this Act reflects a strong influence from American academic thought.[41] However, this act was contrary to state-level legislation. Although the legislation mentioned above

35 'Data Privacy Act; A brief history of Modern Data Privacy Laws', (10th April 2018) <https://blog.eperi.com/en/data-privacy-act-a-brief-history-of-modern-data-privacy-laws> Accessed 20th October 2024.

36 Jef Ausloos, *The Right to Erasure in EU Data Protection: From Individual Rights to Effective Protection* (7th edn, Oxford University Press USA 2020) p 1-560.

37 ibid.

38 See n 35.

39 See n 36.

40 ibid.

41 ibid.

was emerging at the national level, discussions concerning data protection laws have taken place at the international level.

In 1980, the 'Organisation for Economic Co-operation and Development' (OECD) promulgated guidelines to establish foundational principles for data protection.[42] The OECD Guidelines laid down fundamental data protection and privacy principles that have significantly influenced contemporary legal frameworks.

In 1981, the Council of Europe passed the 'Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data' (Treaty 108). The convention's primary purpose is to ensure the protection of individuals' personal data.[43] The modernised version of this convention was published in May 2018.[44]

In 1989, the introduction of the World Wide Web (WWW) marked a transformative moment in the evolution of digital communication and information sharing.[45] The introduction of this technology broke every limitation and geographic boundary. Although this has increased people's ability to express themselves freely, it has also raised new concerns about people's privacy, autonomy, and data integrity.

With the emergence of technology, in 1990, a proposal for a Council Directive titled 'Concerning the Protection of Individuals in Relation to the Processing of Personal Data' was presented by the European Commission, marking an early step towards harmonising

---

[42] 'OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.', 12 February 2002 <https://www.oecd.org/en/publications/2002/02/oecd-guidelines-on-the-protection-of-privacy-and-transborder-flows-of-personal-data_g1gh255f.html> accessed 02 January 2025.

[43] 'Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data' (Treaty 108).

[44] Council of Europe, 'Modernisation of the Data Protection "Convention 108"' (May 2018) <https://www.coe.int/en/web/portal/28-january-data-protection-day-factsheet> Accessed on 11 May 2025.

[45] Tim Berners-Lee, 'The World Wide Web: A very short personal history' (*w3.org*, 07 May 1998), accessed 21 October 2024.

data protection laws across member states. On 24 October 1995, the EU formally adopted the 'Data Protection Directive' (DPD).[46]

Also, the signing of the EU Charter in December 2000 affirmed the protection of personal data as a fundamental right.[47] This is regarded as a benchmark in the data protection law regime. With this identification and following the identification of key shortcomings and a series of communications concerning the implementation of DPD, the European Commission presented a proposal for the 'General Data Protection Regulation' (GDPR) on 25 January 2012.[48] The European Union officially enacted the GDPR on 27 April 2016, with its provisions becoming enforceable on 25 May 2018.[49] I intend to analyse the above-mentioned laws thoroughly in a further chapter.

2.3 Definitions for Data Protection and Privacy

Sri Lankan Scholar Altaff Marsoof states that: 'Privacy is a difficult term to define as its definition and scope are largely shaped by the culture and social norms of a country or region.'[50] Jef Ausloos states that: 'Privacy is a notoriously elusive concept with variable content which touches all aspects of life linked to individual freedom, the relationship between privacy and right to data protection is equally hard to define.'[51] Sunil D. B.

[46] See n 45.

[47] EU Charter art.8. (n 17).

[48] See n 35

[49] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of natural Persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1 (came into force on 25th May 2018) (EU GDPR).

[50] Althaf Marsoof, 'The Right to Privacy in the Information Era: A South Asian Perspective' (2008) 5/3SCRIPTed accessed 22 October 2024.

[51] See n 36.

Abeyratne also states, 'The concept of privacy is not uniform. It differs from various countries and jurisdictions.' [52]

Ian J Lloyd states that: 'The General Data Protection Regulation adopted by the European Union in 2016 is a little more specific, referring on 2 occasions to 'the rights of privacy' and to 'respect of private life', but without attempting to define this."[53] Accordingly, it can be identified that the difficulty lies in defining the term privacy.

Also, Dr Prathibha Mahanamahewa has mentioned the difficulty of defining the term 'data protection.' [54] Peter Carey and Damien Welfare define data protection as a system that safeguards individuals' rights to their personal data by placing restrictions on how businesses can use it.[55]

According to IT Governance, Data protection is 'the protection of a person's personal information against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access, as well as the assurance that it is processed fairly.'[56]

Swire, Ahmad, and McQuay, data protection refers to a legal framework designed to safeguard individuals' personal data from unauthorised access and misuse by third parties.[57]

---

[52] Sunil D.B. Abeyratne, *Introduction to Information and Communication Technology Law* (Author Publication 2008)1-297.

[53] Ian J Lloyd, *Information Technology Law* (9th edn, OUP 2020).

[54] Prathiba Mahanamahewa, 'Data Protection Law an E-Business and E-Government Perception' (2003) Ph.D. Research Scholar in IT Law accessed 22 October 2024.

[55] Damien Welfare and Peter Carey, '*Territorial Scope and Terminology' in Peter Carey (ed), Data Protection: A Practical Guide to UK and EU Law* (5th edn, OUP 2018) 1-31, 2.

[56] IT Governance, 'An Overview of UK Data Protection Law: The UK GDPR, DPA 2018 and EU GDPR, and the ePR and PECR' (*IT Governance*) <https://www.itgovernance.co.uk/data-protection> accessed 13 October 2024.

[57] Peter P Swire, Kenesa Ahmad and Terry McQuay, *Foundations of Information Privacy and Data Protection: A Survey of Global Concepts, Laws and Practices* (N.H. International Association of Privacy Professionals, UK 2012).

Accordingly, it can be identified that there is currently no globally recognised definition for the terms 'privacy' and 'data protection'. Although the EU GDPR and DPA 2018 define the term 'personal data', neither law defines 'Data Protection' and 'Privacy'. Ultimately, data protection may be understood as an extension of the broader right to privacy, encompassing multiple dimensions and applications.

2.4 International Literature

Considering international literature on this subject area, much literature can be found regarding the data protection laws of the EU and the UK. Nevertheless, I intend to focus mainly on literature regarding SMEs, and the literature highlighted the exception of journalism in the EU and the UK's data protection laws.

Benjamin Wong, in his article 'The Journalism Exemption in UK Data Protection Law,'[58] examines the implementation of the journalism exemption under the data protection law in the UK. The author primarily concentrates on three core aspects of the journalism exception, which are 'the interpretation of journalistic purposes, the substantive exemption from liability, and the procedural authority to seek a stay of proceedings.'[59] He offers a contextual overview of the journalism exception as it is framed within the UK's data protection legal framework. Further discusses the uncertainties that have emerged regarding journalism exceptions. He analyses the interpretation of what constitutes a journalistic purpose and uncertainties about the meaning of journalistic purpose by referring to the case laws of the EU and the UK, such as the *Satamedia* case[60], the case of

[58] Benjamin Wong, "The Journalism Exemption in UK Data Protection Law", Journal of Media Law, 2020, vol 12. No 2, 216-236, https://doi.org/10.1080/17577632.2020.1843326 accessed 24 December 2024.

[59] ibid.

[60] *Satakunnan Markkinaporssi and Satamedia* [2008] ECLI: EU: C: 2008:727.

Buivids[61], *Suger v. British Broadcasting Corporation*,[62] etc. Although the author provides some suggestions to solve these uncertainties in the discussion, in the conclusion, he does not provide proper solutions for solving those problems.

David Erdos examines the evolving relationship between data protection and freedom of expression within the framework of the EU GDPR through his article.[63] The Author has structured this article into seven parts. He mainly discusses the nature and progressive development of data protection law across the EU, with special reference to the exceptions and derogations regarding freedom of expression. Then, he discusses the special types of freedom of expression guaranteed by the GDPR. In line with this, the author explores how the GDPR addresses journalism and other special expressions. Further, he provides a detailed analysis of journalism and special expressions recognised under Article 85(2) and broad expressions guaranteed under Article 85(1) of the GDPR.[64] Although the author does not critically analyse the issues or uncertainties about these exceptions, this article is fruitful in obtaining a clear understanding of the journalism exception under the GDPR.

Yelena Smirnova and Victoriano Travieso-Morales' article mainly focuses on examining the key challenges confronting commercial organisations in implementing GDPR.[65] The review exclusively considers scholarly work published after 2016, with the challenges

[61] *Sergejs Buivids v. Datu Valsts Inspekcija*[2019] ECLI: EU: C: 2019:122

[62] [2012] UKSC 4, [2012] 1 WLR 439.

[63] David Erodes, 'Special, Personal and Broad Expression: Exploring Freedom of Expression Norms under the General Data Protection Regulation' Yearbook of European Law, Vol.40, No 1 (2021), pp. 398-430, doi:10.1093/yel/ yeab004, accessed 03 December 2024.

[64] ibid.

[65] Yelena Smirnova and Victoriano Travieso-Morals, "Understanding Challenges of GDPR Implementation in Business Enterprises: A Systemic Literature Review", January 2024, International Journal of Law and Management 66 (3): 326-344, doi:10.1108/IJLMA-08-2023-0170, accessed 03rd December 2024.

systematically analysed across four dimensions, which are technical, legal, organisational, and regulatory. Accordingly, they have identified different issues in implementing GDPR, such as 'complexities in data processing, resource limitations, shifts in company culture, difficulties in managing vendors and complexity in interpreting and understanding regulations',[66] etc.

The findings of the systematic literature review reveal that previous studies have mainly addressed privacy and data protection concerns in the fields of public health, education, and public administration. In contrast, limited scholarly attention has been given to the challenges associated with GDPR implementation in business enterprises. This lack of focus represents a significant gap in the existing literature.

The article titled 'GDPR Compliance in SMEs: There is much to be done'[67], which presents empirical research based on interviews conducted with ten industrial SMEs. This literature primarily underscores the limited awareness among these companies concerning their responsibilities and legal obligations under personal data protection laws and the requirements of GDPR compliance.[68] However, their findings are mainly based on a lack of awareness, and they do not critically evaluate other issues of SMEs in implementing GDPR.

[66] See n 65.

[67] Maria da Conceicao Freitas and Miguel Mira da Silva, 'GDPR Compliance in SMEs: There is much to be done', Journal of Information Systems Engineering and Management, Vol. 3 No.4, 30. https:// doi .org/ 10.20897/ jisem/ 3941 accessed 30th January 2025.

[68] ibid.

The research 'Data Protection Authorities and their Awareness-raising Duties under the GDPR'[69] mainly discusses the duty of EU DPAs to provide awareness for SMEs about the GDPR. The authors have used 52-60 SME representatives for their online survey. The authors identified several existing challenges in fostering collaboration between DPAs and SMEs. They argued that practical guidance is essential for the SMEs. Further, the authors recommend that the DPAs should work more closely with SME Associations. In this article, the authors only discuss the duties of DPAs in raising awareness about GDPR. They do not analyse how to address other compliance and implementation issues regarding SMEs under the GDPR.

Looking at the international literature in this field, it seems that the research has been written with a stronger emphasis on data protection law in the EU and that the literature is essentially self-sufficient in that regard. However, it can be identified that most of the literature has focused on the overview of the EU and the UK's data protection laws and few literature analyses about the journalism exception and the issues regarding SMEs under these laws.

2.5 Sri Lankan Literature

Data protection law represents an emerging legal domain within the Sri Lankan legal framework, and little literature has been published about this law. Sunil D.B. Abeyrathne

[69] Leanne Cochrane, Lina Jasmonataite- Zaniewicz and David Barnard-Wills,"Data Protection Authorities and their Awareness- raising Duties under the GDPR: The Case for Engaging Umbrella Organizations to Disseminate Guidance for Small and Medium-Size Enterprises", European Data Protection Law review, Volume 6 (2020) issue 3, page 352-364, DOI: https://doi.org/10.21552/edpl/2020/3/6, accessed 5th December 2024.

emphasises that Sri Lankan data protection policy is not sufficient for strengthening international trade and commerce and needs a law that complies with the EU GDPR.[70]

Dr Prathibha Mahanamahewa underscores the challenges associated with defining data protection and examines the differing approaches adopted by the US and the EU. He further contends that in the Sri Lankan context, informational privacy ought to be recognised as a constitutional right, and that the development of data protection legislation should be modelled on the EU framework. [71]

Jayantha Fernando and Sanduni Wickramasinghe, in their article 'Sri Lanka Data Protection Legislation – An Overview', provide an overview of the PDPA. This article mainly discusses the background of the PDPA and the legislative drafting process.[72] The authors further discuss the application of the PDPA. Also, they discuss the definitions of 'Personal Data', 'Data Subject', 'Controller', and 'Processor' mentioned in the PDPA. However, they have not critically analysed those definitions compared with other jurisdictions.

Moreover, the authors have given a brief introduction to the data processing principles and rights of the data subjects, but they have not critically analysed those principles. And also, they explain the powers and functions of the DPA. At the end of this article, they compare the PDPA with international standards and discuss the benefits of this act for the country.[73] However, the authors have not discussed the challenges of this act.

---

[70] See n 53.

[71] See n 54.

[72] Jayantha Fernando and Sanduni Wickramasinhe, 'Sri Lanka Data Protection Legislation- An Overview' (3 August 2022), accessed 5 November 2024.

[73] ibid.

Dr Thusitha B. Abeysekara and Amali E. Ranasinghe comprehensively analyse Sri Lanka's existing legal framework on data protection.[74] Drawing comparative insights from the UK and Singapore legal systems, they propose the establishment of a more robust and effective data protection and privacy framework in Sri Lanka.[75] The authors emphasise that Sri Lanka's Constitution does not explicitly safeguard the right to privacy. They further draw attention to the prevailing imbalance between the right to privacy and the right to information within the Sri Lankan legal context. However, the authors do not discuss the implementation issues regarding the PDPA. Although they mentioned the challenges faced by the journalists, they do not discuss the challenges faced by the SMEs under this new law.

The Centre for Policy Alternatives (CPA), in its discussion paper, highlights the significance of the right to privacy and makes recommendations for many developments in the Sri Lankan legal system.[76] The authors mainly discuss the necessity and the scope of privacy rights. Also, they suggest a framework for protecting privacy by using international best practices.[77]

The Article published by Transparency International Sri Lanka, 'Legislative Brief, Personal Data Protection Bill 2021'[78] argues that processing personal data for journalistic purposes should be acknowledged as a legitimate ground under data protection law. The author highlights the exception of journalism under Article 85 of the EU GDPR. She

---

[74] See n 20.

[75] ibid.

[76] Centre for Policy Alternatives CPA in Sri Lanka, 'Right to Privacy in Sri Lanka' (cpalanka.org. 21 September 2020) <http://www.cpalanka.org/right-to-privacy-in-srilaka/>Accessed 21 November 2024.

[77] ibid.

[78] T.Piumi Madushani, "Legislative Brief, Personal Data Protection Bill 2021", accessed 05 December 2024.

further proposes the harmonisation of the concept of 'personal data' across the Personal Data Protection Bill and the RTI Act, and advocates for the establishment of an independent DPA, among other reforms.[79]

Prof. Rohan Samarajeewa also emphasises the flexibility of the EU and UK GDPR in adopting the journalism exemption.[80] He states that: 'The contact list that is saved on a person's phone is …. not covered by the law if it is used purely for a person, domestic or household purposes…..nevertheless, that a journalist's use of such a list for professional reasons is beyond the limits of the law.'[81]

U.M. Sapukotana, for her research titled 'Protecting eHealth Information Privacy', specifically examined whether Sri Lanka has the necessary legal framework to protect the privacy of electronic health records, comparing it to the legal systems of India and the UK.[82]

According to the above-mentioned Sri Lankan literature, a few instances can be identified in the discussion about SMEs and Journalistic purposes. Most of the literature focuses on an overview of the data protection law in Sri Lanka, and some literature mainly focuses on other sectors, such as health, consumer protection, etc.

2.6 The Literature Gap

According to this literature review, the main literature gap is that there is no unified definition of data protection and privacy. The scholarly publications described

[79] ibid.

[80] Rohan Samarajeewa, 'Personal Data Protection Act Passed; what will it mean', (22 March 2023) accessed 5 November 2024.

[81] ibid.

[82] Upeksha Madukalpani Sapukotana, 'Protecting eHealth Information Privacy: A Proposal for a Legal Framework for Sri Lanka' (PhD Thesis, General Sir John Kotelawala Defence University, Rathmalana, Colombo, Sri Lanka 2019).

above indicate that data protection is a challenging concept. Because of this, it is uncertain whether data protection should be regarded as a civil, criminal, constitutional, or special right that includes all of these.

Another notable issue in this context is the difficulty in distinguishing between the concepts of ‘data protection’ and ‘privacy’. As highlighted in the literature reviewed, this distinction remains ambiguous and lacks a universally accepted definition. The absence of a clear conceptual demarcation between data protection and privacy represents a significant gap in the existing legal and academic discourse on data protection and privacy frameworks.

Previous scholarly surveys reveal that extensive international literature exists on various aspects of data privacy and protection, particularly in relation to the EU and UK Data Protection Laws. In contrast, when examining Sri Lankan scholarship, only a limited body of work can be identified that specifically addresses issues of data protection and privacy.

Moreover, most of the existing studies have primarily focused on privacy and data protection concerns in areas like public health and education, and consumer protection, as well as general overviews of data protection legislation. Consequently, the lack of focused studies on other critical areas constitutes a significant gap in the current body of literature.

In considering international literature, it can be identified that some literature has addressed the compliance and implementation issues regarding SMEs and uncertainties that arise in journalism exceptions under the EU and the UK’s data protection laws. However, depth studies were not found to address these issues in Sri Lankan literature.

In the UK, numerous studies have examined the country’s data protection framework in comparison with the EU’s legal regime, often highlighting national needs that informed the development of its current legislation. In contrast, Sri Lanka lacks comprehensive

research that analyses the data protection and privacy laws of the EU and the UK in the context of Sri Lanka's specific economic, social, and technological requirements. This absence reflects a significant gap in the domestic academic and legal discourse.

According to the aforementioned study, the concept of data protection is still largely unexplored in Sri Lanka, and no research has been done to address issues regarding SMEs and journalistic purposes under the data protection law in Sri Lanka. Accordingly, there is a significant gap in Sri Lankan literature in this area of study. Therefore, the goal of this study is to address the identified knowledge gap and enhance the legal literature on this topic.

CHAPTER 3

THE CURRENT LEGAL FRAMEWORK ON DATA PROTECTION AND PRIVACY IN SRI LANKA

3.1. Introduction

This chapter primarily seeks to explore the importance of data protection and privacy in the context of Sri Lanka's digital transformation. It also assesses the sufficiency and effectiveness of the current legal framework, focusing specifically on its impact on SMEs and the field of journalism.

To achieve this objective, the chapter initially outlines the impact of rapid technological advancements on personal data and privacy in Sri Lanka, highlighting the need for a comprehensive and robust legal framework. It then evaluates the current legal regime governing data protection and privacy in Sri Lanka, structured under three key areas: constitutional provisions, common law principles, and relevant statutory enactments.

Finally, I intend to critically analyse the implementation issues which can be identified under the PDPA with special reference to SMEs and journalistic purposes. For that purpose, I intend to critically evaluate the challenges that will have to be faced by SMEs and Journalists in implementing the act.

3.2. The Concept of Data Protection and Privacy in Sri Lanka

Sri Lanka has become an open market economy since 1977. As a result of this, all geographical and economic barriers were removed and opened to the international digital market. Then, the country began implementing digital technology in the late 1980s.[83] In

[83] Nalaka Gunawardena, *Digital Transformation in Sri Lanka; Opportunities and Challenges in Pursuit of Liberal Policies*, (Friendrich Naumann Foundation (FNF) Sri Lanka, 2017) 1- 101, 22.

1989, the country commenced mobile phone services.[84] After introducing mobile phone services and internet connectivity, the country's Information and Communication Technology (ICT) increased rapidly. Therefore, personal data has become a significant asset in many fields in Sri Lanka.

'Electronic Transactions Act, No.19 of 2006' [85](ETA) was adopted on 19th May 2006. It is the most important legislation controlling the implementation of e-government services and the integration of ICT into public sector operations. Then, the 'Electronic Transactions (Amendment) Act, No.25 of 2017', introduced additional objectives to the main statute. 'Legal Recognition of Electronic Signatures' is a very important feature under the amendment to this act. Also, 'Data messages', 'electronic documents', 'electronic record or other communications' have legal recognition under this act.[86] Consequently, the rise in electronic transactions in Sri Lanka has underscored the growing importance of establishing a comprehensive legal framework for cybersecurity and the protection of personal data and privacy.

Also, there is the rapid growth of online services in Sri Lanka. As of early 2025, Sri Lanka recorded approximately 12.4 million internet users, and the number of social media users reached 8.2 million, representing 35.4% of the total population. [87] The ongoing expansion of digitalisation has significantly intensified the demand for comprehensive data protection and privacy legislation.

The usage of modern technology is always evolving, opening up more and more opportunities for third parties to gather personal data without the owner's knowledge or

---

[84] ibid.

[85] Electronic Transactions Act, No. 19 of 2006.

[86] ibid s 3.

[87] Simon Kemp, 'Digital; 2025 Sri Lanka' (03 March 2025), accessed 10 April 2025.

agreement, making it more susceptible to being misused. The loss of personally identifiable information may have negative effects on people. Consequently, these emerging trends often jeopardise individuals' data and privacy, undermining public trust in e-commerce and digital information networks. Moreover, the absence of an effective legal framework for data protection and privacy may have adverse implications for attracting international investments.

The aforementioned findings indicate the need for a robust legal framework governing data protection and privacy in Sri Lanka. However, while safeguarding individual data and privacy, corporate entities should be able to process data without excessive barriers. Additionally, these data protection and privacy laws must not adversely impact other sectors, including the national economy and people's right to information. Accordingly, I will evaluate the current legal framework of privacy and data protection in the following subchapters.

3.3 Current Legal Framework in Sri Lanka

3.3.1. Constitutional Status of Data Protection and Privacy in Sri Lanka

Although Chapter III of the 'Constitution of Sri Lanka' incorporates a range of fundamental rights, it does not expressly acknowledge privacy as a constitutionally guaranteed right.[88] Nevertheless, the 19th Amendment to the Constitution introduced the right to information as a fundamental right.[89] Article 14 A (1) states that 'every citizen

[88] The Constitution of the Democratic Socialist Republic of Sri Lanka, 1978 Chapter III. (Sri Lankan Constitution)

[89] ibid. 19th Amendment.

shall have the right of access to any information as provided by law…' [90] Accordingly, the RTI Act was passed by the Sri Lankan Parliament.[91]

However, article 14 A (2) has given restrictions for article 14 A (1), which states that: "No restrictions shall be placed on the right declared and recognized by this Article, other than such restrictions prescribed by law as are necessary in a democratic society, ……for the protection of health or morals and of the reputation or the rights of others, privacy……." [92] Accordingly, it can be argued that the right to privacy is impliedly safeguarded under the Constitution.

Althaf Marsoof also states that '[T]he right to privacy is not recognised as a fundamental right under the Sri Lankan Constitution and it is only acknowledged as an exception to the right to information.' [93]

The UDHR was the pioneering international document that sought to establish the right to privacy as an independent and fundamental human right.[94] Also, the rights to privacy and information have been recognised simultaneously by over ninety countries across the globe. [95] The UK has affirmed privacy as a fundamental human right through the incorporation of the 'Human Rights Act 1998'. [96] Similarly, Thailand recognises privacy as a fundamental right under Section 32 of its Constitution.[97] In both Sri Lanka and India,

---

[90] ibid, Chapter III, art 14 A (1)

[91] The Right to Information Act, No. 12 of 2016.

[92] Sri Lankan Constitution, 19th Amendment, Chapter III, art 14 A (2).

[93] See n 50.

[94] ibid.

[95] See n 20.

[96] Human Rights Act 1998 (UK) Art. 08.

[97] Constitution of Thailand 2017, s 32.

the right to privacy is not expressly guaranteed as a constitutional right. Nonetheless, the Supreme Court of India has ruled that privacy is inherent within the scope of Article 21 of its Constitution, thereby affirming it as a fundamental right.[98]

The 'International Covenant on Civil and Political Rights' (ICCPR) explicitly recognises the right to privacy.[99] This recognition affirms the global consensus on privacy as a fundamental human right that must be safeguarded through legal mechanisms. Although Sri Lanka has ratified the ICCPR, the domestic enactment, ICCPR Act No. 56 of 2007[100], does not incorporate several key provisions of the Covenant, including Article 17, which guarantees the right to privacy. As a result, the right to privacy is not expressly identified or enforceable under Sri Lankan domestic law, and individuals lack a clear legal remedy for violations of their privacy. Consequently, this legislative gap poses a significant risk to personal data.

3.3.2. Common Law Principles regarding the Right to Privacy in Sri Lanka

In Sri Lanka, privacy protection falls under the realm of *delictual liability*, specifically through the Roman-Dutch law concept of '*actio injuriarum'*. However, *Actio injuriarum* may not be adequate to solve current aspects of data protection and privacy issues. It is a stand-alone remedy available for wrongful assault on people, their reputation, or their dignity. This principle has evolved through judicial decisions. In the case of *Nadaraja v. Obeysekara*[101] the judiciary addressed and examined the concept of 'invasion of privacy'.

---

[98] *Justice K.S. Puttaswamy (Retd.) and Anr. v. Union of India and Ors.* [(2017) 10 SCC 1].

[99] International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR), art 17.

[100] International Covenant on Civil and Political Rights (ICCPR) Act No. 56 of 2007.

[101] *Nadaraja* n 10.

Since this action has limitations and several elements have to be satisfied for claims, this law is not used widely.

Also, in the *Sinha Rathnathunga V. State*[102] the court accepted the concept of privacy. In this case, Hector Yapa J stated that: 'The press should not think they are free to invade the privacy of individuals in the exercise of their constitutional right to freedom of speech and expression, merely because the right to privacy is not declared a fundamental right of the individual.'[103] He emphasises that the Sri Lankan constitution places a strong emphasis on personal autonomy through its guarantees of fundamental human rights.[104]

3.3.3. Statutory Law relating to the Data Protection and Privacy.

Considering statutory law regarding data protection and privacy, there are a few provisions in various statutes. 'The post office ordinance No.11 of 1908'[105] can be recognised as the first statute to give positive protection for personnel information. This Ordinance has several provisions penalising violations of privacy.[106]

Also, the 'Telecommunication Act, No. 25 of 1991',[107] mentions a penalty for intrusion into the content of a message under Section 52.[108] Section 53 sets out the punishment for

[102] [2001] 2 SLR 172.

[103] ibid.

[104] ibid.

[105] The Post Office Ordinance No 11 of 1908.

[106] ibid, s75.

[107] Sri Lanka Telecommunications Act, No. 25 of 1991.

[108] ibid, s 52.

communication officers who intercept and disclose the contents of a message.[109] Also, this is the first legislation in Sri Lanka to identify electronic data as a crime.

The ETA[110] is the most important legislation controlling the implementation of e-government services. The electronic version of any 'data' or 'information' is covered under this act. However, there are no provisions relating to the protection of data under this act. And also, it does not define what would be considered as 'data'.

The 'Payment Devices and Frauds Act, No.30 of 2006', [111] is another important act in this regard. This act has a legal framework for credit cards, debit cards, and other electronic payment devices. According to section 03 (d) of this act, providing cardholders' information to a third party without the cardholder's permission is an offence. [112]

The CCA [113] is particularly significant for data protection and privacy. This Act contains a few provisions aimed at the protection of personal data confidentiality. Accordingly, gaining access to a computer system without authorisation constitutes a criminal offence.[114] Section 08 of the Act stipulates that the unlawful interception of data constitutes a criminal offence.[115] Also, unauthorised disclosure of information is an offence.[116] These crimes are punishable by criminal penalties and restitution to the victim.[117] However, this act does not define what would qualify as 'data'.

---

[109] ibid, s 53.

[110] The Electronic Transaction Act, No.19 of 2006.

[111] Payment Devices Frauds Act No 30 of 2006.

[112] ibid, s 3(d).

[113] The Computer Crimes Act No. 24 of 2007.

[114] ibid, s3.

[115] ibid, s8.

[116] ibid, s10.

[117] ibid, s14.

The RTI Act was enacted to ensure the fundamental right to information. Part II of this act describes the denial of access to the information.[118] Hence, public authorities are permitted to withhold information where its disclosure would result in a breach of personal privacy.[119]

Accordingly, it is revealed that the Sri Lankan legal system contains a limited number of provisions on data protection in various statutes, and lacks a clear definition of the term 'personal data' until very recently.

3.3.4. The 'Personal Data Protection Act, No.09 of 2022' (PDPA)

The enactment of PDPA represents a significant effort to address the longstanding absence of a dedicated legal framework for personal data protection in the country. The main objectives of this act are established in the preamble. [120] Accordingly, three main aspects can be identified under this act, which are establishing rules for how personal data is processed, identifying and strengthening the data subjects' rights and establishing the DPA, including its powers, functions and duties of that authority.[121]

Part I of this act specifies the legal obligations concerning the 'processing of personal data'.[122] The second part of the Act deals with the rights of individuals regarding their personal data. [123] Part III sets out obligations on data 'controllers' and 'processors'.[124] Part IV outlines the legal provisions regarding the processing of personal data for sending

---

[118] Right to Information Act, No. 12 of 2016, Part II.

[119] ibid, section 5(1) (a).

[120] The Personal Data Protection Act, No. 9 of 2022, Preamble.

[121] See n 72.

[122] The Personal Data Protection Act, No. 9 of 2022, Part I.

[123] ibid, Part II.

[124] ibid, Part III.

solicited messages.[125]. The DPA is specifically discussed in Part V of the Act concerning its establishment, goals, and other responsibilities. [126]

According to Section 1 of the Act, Part V came into operation on 17th July 2023 under the 'Extraordinary Gazette No. 2341/59' dated 21st July 2023.[127] Then, DPA was established in August 2023. Under the 'Extraordinary Gazette No. 2366/08', dated 8th January 2024, Parts VI, VIII, IX, and X of the Act came into effect on 1st December 2023. The remaining provisions—Part I, Part II, Part III, and Part VII were scheduled to come into operation on 18th March 2025.[128]

Nevertheless, a memorandum was submitted to amend the PDPA. Consequently, the enforcement date of 18th March 2025 was revised through 'Extraordinary Gazette No. 2427/34', dated 14th March 2025, and a new date will be published after enacting the Amendment Bill.[129] Although the PDPA is not fully enforced when I am conducting this research, I intend to describe important parts of this act to get an overall idea about the PDPA.

Section 2 deals with the application of this act.[130] However, the processing of personal data for domestic or household reasons is exempt from this act, and also, this act does not apply to any data other than personal data.[131]

---

[125] The Personal Data Protection Act No. 09 of 2022, Part IV.

[126] ibid., Part V.

[127] "Application of the Personal Data Protection Act No. 09 of 2022 in the Public Sector and Introduction to the Data Protection Authority", Circular No. 01/2024 issued by the Data Protection Authority. < https://www.dpa.gov.lk> Accessed 20th April 2025.

[128] ibid.

[129] "Cabinet Endorses PDPA Amendments to strengthen Stakeholder Alignment and Regulatory Capacity Prior to Enforcement" Media Release, 24 February 2025, Ministry of Digital Economy < https://www.dpa.gov.lk > Accessed 20th April 2025.

[130] The Personal Data Protection Act, No. 9 of 2022, s.2.

[131] ibid s3 (1).

Section 4 obliges data controllers to process personal data in line with the defined responsibilities set out under the Act.[132] Those obligations are mentioned under sections 5 to 12 of this Act. Accordingly, the controllers have obligations to 'process personal data lawfully'[133], 'define a purpose for personal data processing' ,[134] 'confine personal data processing to the defined purpose'[135], 'ensure accuracy' [136], 'limit the period of retention' [137] , 'maintain integrity and confidentiality' [138], 'process personal data in transparent manner' [139], and 'accountability in processing of personal data.' [140]

The PDPA guarantees several rights concerning the data subjects, which are described under part II of the act as follows: 'right of access to personal data'[141], 'right to withdrawal of the consent and the right to object to processing'[142], 'right to rectification of completion'[143], 'right to ensure'[144], 'the right to request a controller to review a decision

---

[132] The Personal Data Protection Act No. 09 of 2022, s 4.

[133] ibid, s 5.

[134] ibid, s 6.

[135] ibid, s7.

[136] ibid, s 8.

[137] ibid, s 9.

[138] ibid, s 10.

[139] ibid, s11.

[140] ibid, s 12.

[141] ibid, s.13.

[142] ibid, s 14.

[143] ibid, s 15.

[144] ibid, s 16.

of such controller based solely on automated processing' [145] and ensure the 'right of appeal of the data subjects to the DPA.' [146] Also, the decisions made by the DPA can be challenged before the Court of Appeal.[147]

Section 20 of this act deals with the appointment of the DPO[148]. Section 20(1) provides the circumstances of the appointment of the DPO.[149] If the processing is conducted by a 'government ministry, department, or public corporation', the controller or processor shall appoint a DPO. However, there is an exception for the judiciary under this subsection. [150] And also, section 20(1) (b) provides specific activities for the appointment of the DPO. [151]

DPIA is a significant feature under the PDPA. Before engaging in some types of processing operations, controllers are obligated to conduct DPIAs to identify risks and, if necessary, seek the advice of the DPA.[152] Also, the PDPA has established a mechanism for cross-border data transfers in accordance with regional and global protocols.[153] However, there are some limitations for the public authorities. [154]

Provisions in Part V deal with the DPA.[155] The objectives of this Authority are mentioned under section 31 of this Act. It has the authority to conduct inquiries, hear complaints and

---

[145] The Personal Data Protection Act No. 09 of 2022, s 18.

[146] ibid, s 19.

[147] ibid.

[148] ibid, s 20.

[149] ibid, s 20 (1).

[150] ibid, s 20(1) (a)

[151] ibid, s 20(1) (b)

[152] ibid, s 24.

[153] ibid, s 26.

[154] ibid, s 26.

[155] ibid, Part V.

appeals, and give directions to entities that disobey the proposed law's requirements. Those who disobey a directive given by the Authority may be subject to administrative penalties. [156]

The act provides definitions for the 'Personal Data', 'Data Subject', 'Controller', 'Processor', 'Processing', 'Special Categories of personal data', etc.[157] Therefore, it is evident that the committee that drafted this Act adhered to best practices that were incorporated into several international standards.

The PDPA does not specifically mention SMEs. Nevertheless, according to section 2, all SMEs that process personal data should comply with the Act.[158] Also, there are no provisions regarding journalistic purposes, and one exception is addressed for journalistic purposes.[159] However, this exemption is not sufficient for addressing issues relating to journalistic purposes. Accordingly, I intend to critically analyse the challenges faced by SMEs and Journalists under the PDPA.

3.3.5. Challenges Faced by SMEs under the PDPA

SMEs play a vital role in the economies of developing countries like Sri Lanka, as they contribute significantly to the GDP. Moreover, SMEs not only provide job opportunities for a substantial portion of the country's population but also act as a nursery for future

---

[156] The Personal Data Protection Act No. 09 of 2022.

[157] ibid, s.56.

[158] ibid, S.02.

[159] ibid, S.40 (e).

large companies.[160] At the end of 2018, there were approximately 1.3 million active 'Micro, Small, and Medium-sized Enterprises' (MSMEs) operating in the country[161]

There is no standard definition regarding SMEs in Sri Lanka; instead, various agencies apply different criteria depending on their specific goals and mandates.[162] However, the 'National Policy Framework for Small and Medium Enterprises (SME) Development' defines SMEs. According to that report, 'SMEs are made up of enterprises which employ less than 300 employees and which have an annual turnover not exceeding Rs 750 million. In this context, micro-enterprises are also read with SMEs for any policy-related measures.'[163] This has been considered an accepted definition in Sri Lanka.[164]

In considering the distribution of SMEs, large and medium-sized enterprises are mainly established in urban areas, while micro and small businesses are established in rural areas. The 'Department of Census and Statistics' (DCS) states that: '74% of the micro establishments are scattered in the rural areas, whereas around 50% of the medium and 61% of the large-scale establishments were found in the urban areas.'[165]

Moreover, the DCS highlights that micro enterprises in Sri Lanka make up 91.8%, small enterprises 7%, medium enterprises 1%, and large enterprises comprise the remaining

---

[160] 'Non-Agricultural Economic Activities in Sri Lanka, Economic Census 2013/2014', Listing Phase, Department of Census and Statistics, Ministry of Policy and Planning Economic Affairs, Child Youth and Cultural Affairs, < http://www.statistics.gov.lk> Accessed 10 April 2025.

[161] 'Impact of Economic Crisis on MSMEs, Insights and Analysis', 2022, Ministry of Finance, Economic Stabilization and National Policies in Sri Lanka, <https://www.statistics.gov.lk/Resource/en/Industry/Other_Tables_Reports/MSMEs_Report.pdf> Accessed 11 March 2025.

[162] Department of Census and Statistics, "Key indicators of Industry Trade and Services Sector, Economic Census 2013/14", Press Release on 14.07.2015, <http:// www.statistics.gov.lk, chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.statistics.gov.lk/Economic/Non_agri/PRESS%20RELEASEEcoCen_en.pdf > Accessed 10 February 2025.

[163] ibid.

[164] See n 11.

[165] See n 160.

0.2%.[166] Accordingly, it can be observed that MSMEs comprise approximately 99.8% of all businesses in Sri Lanka, whereas large enterprises make up only 0.2%.[167] This clearly highlights the critical role SMEs play in driving the nation's economic growth and development.

However, the effects of the PDPA on SMES in Sri Lanka have not been examined in detail, as the act had not been fully enforced when I conducted this research. Hence, I intend to evaluate the possible effects of the PDPA on SMES in Sri Lanka and the challenges that SMES will have to face in complying with the act. The main challenge is that all business enterprises which process personal data should comply with the act. Accordingly, all MSMEs which process personal data fall within its scope, and there are no exceptions for small businesses except for processing data purely for household purposes. Nevertheless, the EU GDPR provides exemptions for small businesses. Accordingly, an organisation with fewer than 250 employees does not need to follow a record-keeping process.[168]

Since there is no limitation under the PDPA, Sri Lankan SMEs will have to face lots of complexities in data processing. Sri Lanka is a middle-income country, and all SMEs are mainly established in rural areas. In considering regular work culture, insufficient human resources and budget limitations are the main challenges that are faced by SMEs.

According to the DCS, the percentages of temporarily or permanently closed MSMEs from 2018-2023 are as follows:'2019- 9.9%, 2020- 33.4%, 2021- 27.4%, and 2022-29.3%.'[169] Moreover, that report states that 'due to the Covid-19 epidemic and economic

[166] See n 160.

[167] ibid.

[168] EU GDPR, Art 30 (5).

[169] See n 161.

crisis, there has been a notable increase in the number of Micro, Small and Medium Scale businesses either temporarily or permanently shutting down.'[170] Accordingly, SMEs will have to face additional pressure in complying with the PDPA with their budget limitations.

The above-mentioned report highlights a significant decline in employment within the SME sector between 2018 and 2020.[171] Specifically, the number of employees in the small business sector dropped from 673.3 thousand to 414.6 thousand, while in the medium business sector, it fell from 485.5 thousand to 262.4 thousand.[172] Accordingly, it is clear that SMEs already face an issue of a lack of human resources.

According to the PDPA, controllers and processors should designate DPOs.[173] The Act provides special circumstances for appointing DPOs.[174] Nevertheless, the Act lacks detailed guidance on how to determine when these particular circumstances apply. This may negatively affect the SMES in complying with the Act.

Lack of awareness regarding the PDPA is another challenge that will have to be faced by SMEs. Most of the SMEs are established in rural areas and conduct their business by using minimal resources and technologies. Some unclear wording of the PDPA is difficult to understand, and it will negatively affect the SMEs.

According to Section 35 of the Act, if the controller or processor fails to comply with the Act, the DPA will be able to conduct an inquiry against them.[175] Moreover, section 38

---

[170] See n 161.

[171] ibid.

[172] ibid.

[173] The Personal Data Protection Act No. 09 of 2022, S.20.

[174] ibid, s 20 (b) (i) (ii) and (iii).

[175] ibid, s 35.

states that: '[T]he nature and extent of relevant non-compliance and matters referred to in section 39 of this Act, by notice require such controller or processor to pay a penalty, which shall not exceed a sum of rupees ten million for each non-compliance.'[176] Therefore, it is necessary to conduct awareness programs regularly before the enforcement of the Act. Unless SMEs which conduct their business with minimal resources have to pay too many penalties under the PDPA.

3.3.6. Challenges Faced by Journalists under the PDPA

Reconciling the right to privacy with the right to information is important to ensure transparency and accountability while protecting personal data. The PDPA has tried to protect that balance to a certain extent by imposing an exception to the Act. Section 40 (e) of this Act states that: 'Any exemption, restriction or derogation to the provisions of this Act shall not be allowed except ……. (e) the protection of the rights and fundamental freedoms of persons, particularly the freedom of expression and the right to information.'[177]

Nevertheless, it can be argued that this exception is not sufficient to reconcile the right to privacy with the right to information in comparison with the other sections of the Act. Also, the PDPA does not provide exceptions for journalistic purposes like the EU and the UK's data protection laws.[178] As a result, journalists who are processing personal data have to face lots of problems in the reporting process, and they have to get consent from

[176] The Personal Data Protection Act No. 09 of 2022, s 38.

[177] ibid, s 40 (e).

[178] Data Protection Directive 1995, art9, Data Protection Act 1998, s.32, Data Protection Act 2018, s.176, European Union Data Protection Regulation (GDPR), art.85(1) 85(2).

the data subjects daily. Thus, it becomes apparent that a significant conflict arises between the right to freedom of expression exercised by the press and individuals' data privacy rights within the Sri Lankan legal context.

Dr Thusitha B. Abeyseara also proposed that 'including the specific exception to ensure that the Right to Information Act will not be overridden in any case of inconsistency.'[179]

However, if adopting the journalism exception under the PDPA, there should be a specific definition for journalistic purposes. Sri Lanka lacks a clear and specific definition for 'journalistic purposes' within its legal framework. Therefore, the subsequent chapter will examine the approach adopted by the EU GDPR and the UK's legal framework on data protection and privacy to provide a comparative analysis.

[179] See n.20.

CHAPTER 4

ANALYSIS OF THE DATA PROTECTION AND PRIVACY LAWS IN THE EU AND THE UK

4.1 Introduction

This chapter's main objective is to identify leading trends from the EU and the UK's data protection and privacy laws with special reference to SMEs and journalistic purposes, which can serve as lessons for Sri Lanka's data protection framework. The EU has a globally effective data protection model under the GDPR. The UK was among the first nations to incorporate GDPR into domestic law. Therefore, I intend to analyse key legislation, judicial decisions, and significant literature written in the two aforementioned jurisdictions. Then, I will explore the lessons that can be drawn from the data protection and privacy legal frameworks of the EU and the UK to develop a robust and effective legal regime for data protection and privacy in Sri Lanka.

4.2. Legal framework of the EU's Data Protection and privacy

4.2.1. The Background

Data protection and privacy laws in the EU extend back several decades. By removing trade restrictions, the EU formed a common market across its member states[180] As a result of embracing market liberalisation, new rights emerged, and existing laws related to human rights proved insufficient. Consequently, conflicts arose between market liberalisation and laws designed to protect human rights. Although the EU has long acknowledged privacy as a basic human right, the growth of information technology

[180] 'The Internal Market: General Principles' Fact Sheets on the European Union < https://www.europarl.europa.eu/factsheets/en/sheet/33/the-internal-market-general-principles> accessed 10 April 2025.

compelled the EU to go beyond the traditional understanding of the right to privacy, especially in data processing and protecting personal information.

As discussed in the previous chapter, the development of data protection laws at both national and international levels significantly influenced the development of the EU's data protection framework. Notably, the 'OECD Guidelines'[181] and 'Convention 108'[182] stand out as key international instruments. In particular, the OECD Guidelines set forth the main data protection principles that have had a substantial impact on modern legal frameworks, including the DPD.[183]

Accordingly, a proposal for a 'Council Directive Concerning the Protection of Individuals in Relation to Processing of Personal Data' was issued by the European Commission in 1990.[184] The proposed DPD aimed to achieve several key goals, including (a) 'to protect the fundamental rights of individuals, and in particular the right to privacy' and (b) 'prevent restrictions to the free flow of personal data between member states'.[185] Finally, the DPD was adopted on 24th October 1995.[186]

Nevertheless, the DPD was not applied automatically to the national laws, and required incorporation into national legislation by member states. Accordingly, each member state applied its own interpretations to the DPD. As a result, it was difficult to identify uniform data protection compliance requirements across EU member states, and this affected

---

[181] See n 42.

[182] See n.43.

[183] Asloos n.36.

[184] European Union, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, OJ 1995 L 281/31. (Data Protection Directive).

[185] ibid.

[186] Data Protection Directive.

business organisations. Accordingly, the CJEU provided an interpretation for the DPD through the case laws to solve these issues.[187]

The DPD was drafted in the 1990s when significant changes were emerging in technology, particularly in computing and communications. Consequently, it was essential to adapt to the increasingly changing world and update the DPD to address the emerging issues accordingly.

Also, in December 2000, the EU Charter was signed, and the safeguarding of personal data was acknowledged as a basic human right.[188] With this identification, and after several communications regarding the implementation of the DPD, the European Commission intended to revise the legal framework of the EU and proposed a comprehensive legal reform, including the GDPR on 25th January 2012.[189] Finally, the GDPR received approval from the European Parliament on 27 April 2016 and officially took effect on 25 May 2018.[190]

4.2.2 The EU GDPR

EU GDPR development in 2018 can be identified as an effort to fill the gaps.[191] It developed into a comprehensive law, incorporating new guidelines to allow people more

[187] *Commission v Germany*, [2010] ECR I-01885 case, the Court of Justice held that the requirement of 'complete independence' for a supervisory authority entails freedom from any external influence.

[188] EU Charter art.8. (n 17).

[189] See n 36.

[190] See n 49.

[191] ibid.

control over their personal data and businesses full access to the benefits of the digital economy.[192]

The GDPR seeks to unify data protection laws throughout the EU by eliminating separate national implementation requirements.[193] Accordingly, the EU GDPR directly applies to the member states. It was introduced to respond to the technological and social developments that have arisen over the last twenty years.[194]

Although the aims of the DPD and EU GDPR are closely similar, the GDPR enhances the ability to conduct business in EU member states by reducing inconsistent compliance requirements compared to the DPD. Accordingly, some differences between the DPD and the EU GDPR can be identified. I intend to critically analyse these differences in the following sub-chapters.

My research specifically focuses on SMEs and journalism exemptions under the GDPR. However, I intend to analyse the GDPR under 6 parts to obtain a better understanding, which are key definitions, key data protection principles, Data subjects' rights, duties and responsibilities of data controllers and processors, GDPR compliance for SMEs and Journalism exemption under the GDPR.

---

[192] European Commission, 'Commission report: EU data protection rules empower citizens and are fit for the digital age'(*ec.europa.eu*,24June 2020) <https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1163> Accessed 12 May 2025.

[193] Detlev Gabel, Tim Hickman, "Unlocking the EU General Data Protection Regulation: A practical handbook on the EU's new data protection law" 28 May 2025 accessed 10 June 2025.

[194] ibid.

4.2.3 Key Definitions under the GDPR

The GDPR is a special regulation to strengthen personal data privacy and maintain uniformity within the EU. When analysing the GDPR, it is vital to examine the notions of 'processing' and 'personal data'. In considering 'personal data', which has been defined broadly by the GDPR.[195]

Under the GDPR, personal data is generally defined as any information about a named or distinguishable individual. [196] As a result, even information that indirectly identifies a named person but could be used to do so is protected by the law. The GDPR has added extra compliance requirements, including location data, online identifiers and genetic data within the definition of personal data. However, the DPD did not include these obligations. However, diseased persons are not covered under this definition.[197] The predecessor, the DPD, has not specifically excluded the personal data of deceased persons. Also, the GDPR does not cover legal persons.[198]

In the *Rynes* case[199]states that: 'the image of a person recorded by a camera constitutes 'personal data' within the meaning of Article 2(a) of Directive 95/46.'[200] In the *Buivids*[201]

---

[195] EU GDPR Art.4(1)

[196] ibid.

[197] EU GDPR, Recital 27.

[198] ibid., Recital 14

[199] *Frantisek Rynes v. Urad pro ochranu osobnich udaju*, C-212/13, EU: C: 2014: 2428.

[200] ibid. para 22

[201] Buivids (n 61).

case, also emphasised that the video recordings in question of the police officers and captured images of individuals fall within the scope of 'personal data'.[202]

In the *Nowak v. Data Protection Commissioner*[203] the CJEU held that written answers to the exams and comments of the examiners are considered personal data under EU law. Also, in *Breyer* [204]case, the court decided that an IP address comes under the personal data under the EU law. Accordingly, it is evident that the courts have adopted a broad interpretation of the term 'personal data'.

Also, the GDPR defines the term 'Processing'.[205] This term encompasses any activity that touches the context of personal data. Therefore, its scope is very broad according to the judicial decisions of European courts. In the *Rynes* case, the court held that: 'a video recording of a person, which is stored on a continuous recording device, the hard disk drive of that system, constitutes, Article 2(b) and Article 3(1) of the Directive 95/46, the automatic processing of personal data.'[206]

4.2.4 Key Data Protection Principles under the GDPR

The GDPR establishes key data protection principles that controllers must follow in personal data processing. [207] There are seven key principles which are outlined and briefly discussed below.

---

[202] Buivids (n 61).

[203] 1/1 C- 434/16, ECLI:EU:C:2017:994

[204] *Patrick Breyer v. Bundesrepublik Deutchland* ECLI:EU:C: 2016:779

[205] EU GDPR Art. 4 (2).

[206] *Rynes*, (n 199), para 23 and 25.

[207] EU GDPR, art 5.

- **'Lawfulness, fairness, and transparency'**[208]

According to the DPD, personal data was required to be handled fairly and lawfully.[209] However, the GDPR added a further compliance obligation, which is transparency.[210] According to Article 6(1) of the GDPR, data processing is considered lawful only if it satisfies at least one of several specified conditions.[211]

The principle of fairness obliges controllers and processors to act consistently with the explanations given to data subjects. Simply put, permission from the data owner must be sought before collecting any data. Transparency is essential in data processing, and data subjects must be notified of the purpose, methods, and duration of processing. They also have the right to know about the use of their data and the parties who will have access to it.[212]

- **'Purpose limitations'** [213]

According to this principle, personal information should be processed strictly in keeping with the intent for which the data subject was informed at the moment of its collection. Furthermore, the data subject must have given their informed consent for those particular purposes.[214] This measure allows individuals to retain authority over their personal data while reducing the risk of misuse or exploitation.

---

[208] EU GDPR, art 5(1) (a).

[209] Data Protection Directive, Recital 37, Article 6 (1) (a)

[210] EU GDPR, art 5 (1) (a).

[211] ibid. art. 6(1)

212 Galina Kulakova, '7 principles of the GDPR and what they mean' (amara-marketing.com.co, 2019) accessed 13 May 2025.

[213] ibid, art.5(1) (b).

[214] EU GDPR, art 5(1) (b).

- **'Data minimisation'**[215]

The quantity of data collected should be justified under the GDPR. Accordingly, personal data must be 'adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.' [216]

- **'Accuracy'**[217]

According to this principle, Personal data should be kept accurate and updated as needed. Data controllers are required to implement adequate steps to preserve the accuracy of the information they process. Consequently, data processors are obligated to correct or delete any personal data that is found to be incorrect or outdated.

- **'Storage limitation'**[218]

The 'storage limitation' is related to the principle of 'data minimisation'. This principle requires that personal data be stored in a form that identifies individuals only for as long as necessary to fulfil the purposes for which it was collected. While a reasonable retention period may be permitted, it is essential that the data controller can justify this duration by showing that it is genuinely needed for the specific purposes previously communicated to the data subject. Once the purpose is fulfilled, the data should be either anonymised or securely deleted.[219]

---

[215] EU GDPR, art.5(1) (c).

[216] ibid, art 5(1) (c).

[217] ibid, art.5(1)(d).

[218] ibid, art.5(1) (e).

[219] Data Privacy Manager, 'What are the 7 principles of GDPR (*dataprivacymanager.net*, 01/10/2020), <https://dataprivacymanager.net/what-are-the-7-gdpr-principles/> Accessed 13 May 2025.

- **'Integrity and confidentiality'**[220]

This principle requires that personal data be managed in a manner that guarantees its security and shields it from potential risks. Accordingly, it necessitates implementing adequate technical and organisational safeguards to avert unauthorised access, misuse, or accidental damage to personal data. These measures may include encrypting data, setting access restrictions, conducting regular security audits, and training staff, all of which are aimed at maintaining the confidentiality of personal data.

- **'Accountability'**[221]

Accountability means that the principles of the GDPR must be followed by the controller. Peter Carey states that GDPR introduces this 'accountability' responsibility as a new principle to data protection law.[222] As mentioned in Article 5(2), Controllers must show that they are following the aforementioned six principles. [223]

4.2.5 Data Subject Rights under the GDPR

The GDPR introduces a wide range of rights of data subjects under Chapter III as follows;

- **'Right to be informed'**

Articles 13 and 14 of the GDPR grant data subjects the right to receive clear and detailed information about the collection and use of their personal data. These articles ensure that data processing is carried out transparently by requiring controllers to inform individuals about 'the identity and contact details of the controller or DPO, purpose and legal basis of

[220] EU GDPR, art5(1)(f).

[221] ibid, art 5(2).

[222] Peter Carey, 'Data Protection Principles' in Peter Carey (ed*), Data Protection: A Practical Guide to UK and EU Law* (5th edn, Oxford University Press 2018) 32-41.

[223] EU GDPR, art 5(2).

the processing, the categories of personal data involved, the period for which the data will be stored' etc.[224]

- **'Right to access'**

Right to access is described under Article 15 of the GDPR, which states that: 'The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data.'[225] Also, the data subjects have the right to obtain a copy of the processing of personal data.[226] However, it should not affect others' rights and freedoms.[227]

- **'Right to rectification'**

Article 16 grants the data subject the right to request the correction of any inaccurate personal information promptly. Considering the purposes for which the data is processed, individuals can request that incomplete personal information be completed, including the addition of extra statements. [228]

- **'Right to erasure'**

This article provides grounds for erasing personal data. Situations include the personal data being irrelevant to its intended purpose, withdrawal of consent by the data subject, objection to processing, or unlawful processing of the data, etc.[229]

---

[224] EU GDPR, art 14.

[225] ibid.

[226] ibid art, 15 (3)

[227] ibid art, 15 (4)

[228] ibid, art.16.

[229] ibid art.17.

- **'Right to restriction of processing'**

Under this right, individuals have the right to limit how their personal data is processed or used. Simply defined, the GDPR gives consumers and other natural persons the right to restrict their personal data processing, subject to several guidelines and exceptions.[230]

- **'Right to object to processing'**

This is another right guaranteed under the GDPR.[231] Similar to Article 18, a data subject can object to the processing of personal data based on particular reasons related to their unique circumstances, especially when the information was collected with a marketing view.

- **'Right to data portability'**

According to this right, data subjects have the right to ask the controller to give them their personal data in a 'structured, commonly used and machine-readable format', and they can keep that data themselves or share it with another controller.[232] However, this right applies only in the circumstances in which information is processed automatically.

- **'Right to object and automated individual decision-making'**

This means that data subjects have the right to refuse or revoke permission if their personal data is being used for direct marketing activities, which includes profiling.[233] Consequently, when the data subject expresses opposition, personal data cannot be utilised for direct marketing.[234]

---

[230] EU GDPR, art.18.

[231] ibid, art.19.

[232] ibid, art 20.

[233] ibid, art 21.

[234] ibid, art 21.

4.2.6 Duties and Responsibilities of Data Processors and Controllers under the GDPR

Article 4 of the GDPR defines the term 'controller'[235] and 'processor'.[236] Article 5 (2) provides the responsibilities of the controller. This involves obtaining individuals' consent, securely storing their data, managing consent withdrawals, and providing access when required, etc.[237]

Controllers and processors are obliged to document their data processing operations and must be able to show compliance if asked by the supervisory authority.[238] Furthermore, controllers must implement measures to uphold data protection principles and embed appropriate protections during personal data processing.[239]

Controllers are required to undertake DPIA before processing when data processing utilises developing technologies and is assessed to represent a significant danger to people's privacy.[240]

Under the GDPR, Article 37 outlines three specific circumstances in which a DPO must be appointed by a data controller or processor.[241]Accordingly, DPOs should not be appointed in every circumstance, and it can be identified as a solution for the budget limitations of the SMEs.

---

[235] EU GDPR, Art. 4.

[236] ibid.

[237] ibid, art 5(2).

[238] ibid art.30.

[239] ibid, art.25(1).

[240] ibid art.35.

[241]ibid, art 37.

The Data Supervisory Authority plays a vital role in ensuring GDPR compliance in the EU. The GDPR requires that member states create a Data Supervisory Authority, an independent organisation with the authority to oversee and ensure adherence with the GDPR and defend the rights and liberties of individuals regarding data processing inside the EU.[242] National Data Supervisory Authorities are also given investigative[243], corrective[244], authorisation, and advisory[245] capabilities, as well as the authority to levy administrative fines on controllers and processors for violations.

4.2.7 Compliance of SMEs under the EU GDPR

GDPR pays special attention to SMEs throughout the regulation. My research mainly focuses on analysing how GDPR concerns SMEs in the EU and what implementation process they have followed regarding SME compliance with GDPR. Additionally, I intend to evaluate the key lessons that can be drawn from the EU GDPR to strengthen and improve the data protection legal framework in Sri Lanka, particularly the legal framework, implementation process, and SMEs compliance with the PDPA.

The GDPR states that: 'To take account of the specific situation of micro, small and medium-sized enterprises, this Regulation includes a derogation for organizations with fewer than 250 employees with regard to record-keeping.'[246] Further states that: '[T]he Union institutions and bodies, and Member States and their supervisory authorities, are

[242] EU GDPR, art 58(1).

[243] ibid art.58(2).

[244] ibid, art.58(3).

[245] ibid art.83.

[246] ibid, Recital 13.

encouraged to take account of the specific needs of micro, small and medium-sized enterprises in the application of this Regulation.'[247]

Accordingly, Article 30 (5) of the GDPR provides an exemption for SMEs with fewer than 250 employees for the record-keeping process.[248]Article 2 (1) of the Commission Recommendation defines MSMEs as: '[E]nterprises which employ fewer than 250 persons and which have an annual turnover not exceeding EUR 50 million, and/or an annual balance sheet total not exceeding EUR 43 million.'[249] The GDPR especially mention that MSMEs should take guidance from Article 2 of this Commission Recommendation.[250]

Also, the GDPR encourages associations and relevant bodies involved in personal data processing to develop codes of conduct that align with the regulation, while also taking into account the particular needs of MSMEs to ensure their effective implementation.[251] Furthermore, Article 42 of the GDPR outlines the creation of a certification mechanism to guarantee adherence with the regulation. It explicitly states that this mechanism should consider the particular requirements of MSMEs.[252] Based on the findings discussed above, it is evident that the GDPR has given particular consideration to the needs of SMEs from the initial stages of its formulation.

Moreover, the EU has published two reports on the application of the GDPR until now. The first report on the evolution and review of the GDPR under Article 97 of the GDPR

---

[247] EU GDPR.

[248] ibid, art 30(5).

[249] Commission Recommendation concerning the definition of micro, small, and medium-sized enterprises on 06 May 2003 (C(2003)1422), 2003/361/EC, Official Journal of the European Union L 124/16 dated 20.05.2003.

[250] EU GDPR.

[251] ibid, Rec 98 and Art 40.

[252] ibid., Article 42.

was published on 24.06.2020, and the second report was adopted on 25.07.2024.[253] Both reports have highlighted challenges for organisations, in particular SMEs, in the implementation process. Second report emphasises that: 'The GDPR provides a toolbox of instruments to enable organizations to flexibility manage and demonstrate their compliance, including codes of conduct, certification mechanisms and standard contractual clauses.'[254] According to the second report, this guidance for SMEs should be easy to understand without any legal training, since most of them do not possess internal knowledge or specialised staff for handling data protection.[255]

Also, the 'European Data Protection Board' (EDPB) launched guidelines for small businesses to easily understand the GDPR and ensure compliance with the GDPR on 27th April 2023.[256] These guidelines cover various aspects of the GDPR, including understanding the data protection basics, rights of the data subjects, compliance with the GDPR and how to secure personal data, etc. It includes videos, flowcharts, infographics and interactive materials to easily understand the GDPR.

According to the second report, SMEs are carrying out low-risk processing activities.[257] Accordingly, it can be identified how the GDPR pays special attention to SMEs.

---

[253] Communication from the Commission to the European Parliament and the Council, Second Report on the application of the General Data Protection Regulation, European Commission, Brussels COM (2024) 357 final. < https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52024DC0357> Accessed 15 May 2025.

[254] ibid.

[255] ibid.

[256] EDPB Launches Data Protection Guide for Small Businesses, 27 April 2023, < https://www.edpb.europa.eu/news/news/2023/edpb-launches-data-protection-guide-small-business > Accessed 15 May 2025.

[257] See n 253.

4.2.8 Journalistic Exemptions under the GDPR

The GDPR specifically mention that: "Member States' law should reconcile the rules governing freedom of expression and information, including journalistic, academic, artistic and or literary expression with the right to the personal data pursuant to this Regulation."[258] Further, it emphasises that processing personal data for journalistic purposes should allow certain derogations or exemptions to balance the right to data protection with the right to freedom of expression[259]

Also, in the *Satamedia case,* the CJEU states that;

'In order to take account of the importance of the right to freedom of expression in every democratic society, it is necessary, first, to interpret notions relating to that freedom, such as journalism, broadly.'[260] This concept has been emphasised under the EU GDPR.[261]

Accordingly, Article 85(1) and Article 85 (2) of the GDPR provide exemptions and derogations for 'journalistic purposes' and 'purposes of academic, artistic, and literary expression'. Article 85(1) states: 'Member states shall by law reconcile the right to protection of personal data pursuant to this Regulation with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression.'[262]

David Erdos categorises Article 85 (1) of the GDPR as a broad expression and Article 85 (2) of the GDPR as a special expression regime.[263] He emphasises that the majority of EU

---

[258] EU GDPR, Recital 153.

[259] ibid.

[260] *satamedia* (n 60).

[261] EU GDPR, Recital 153.

[262] EU GDPR, Article 85 (1).

[263] See n 63.

member states, around 80%, have refrained from enacting broad derogations under this provision, considering that six countries have adopted such measures, which is problematic.[264] He provides the details of these countries, which are 'Denmark, Greece, Ireland, Malta, Portugal and Sweden'.[265] Accordingly, it can be identified that there is a debate regarding Article 85 (1) of the GDPR in member states, and they do not like to imply that broad expression to their local legislations.

However, in *Buivids'* case, the court of justice emphasised that in the lack of relevant domestic legislation, the 'special purposes derogation' should be regarded as self-executing.[266] This case also establishes 'relevant criteria' to be taken into account when balancing the right to privacy with the right to freedom of expression which are '[the] contribution to a debate of public interest, the degree of notoriety of the person affected, the subject of the news report, the prior conduct of the person concerned, the content form and consequences of the public, and the manner and circumstances in which information was obtained and its veracity.'[267]

Accordingly, it can be identified that the court has given direction for the reconciliation of the right to privacy and the right to freedom of expression for member states.

Also, in the *Buivids* and *Satamedia* cases emphasised that the journalism exemption covers not just media organisations but extends to all individuals engaged in journalism.[268] Specifically, in the *Buivids* case states that 'Mr Buivids uploaded the recorded video

---

[264] See n 63.

[265] ibid.

[266] *Buivids* (n 61).

[267] ibid.

[268] *satamedia* [2008] (n 60) para 58, *Buivids* (n 61) para 52.

online on such an internet site, in this case www.youtube.com, cannot in itself preclude the classification of that personal data as having been carried out 'solely for journalistic purposes' within the meaning of Directive 95/46.'[269]

Also, the above-mentioned cases highlighted that 'journalistic activities are those which have as their purpose the disclosure to the public of information, opinions or ideas, irrespective of the medium which is used to transmit them.'[270] Accordingly, all publishing methods, such as newspapers, radio, and the internet, can be used, and the publishing method is neutral. Nevertheless, in the *Buivids* case emphasised that all the information published on the internet cannot be considered as journalistic activities.[271]

Also in 2018, *NTI v. Google LLC,*[272] the court ruled that Google was not entitled to use the journalism exception to refuse a de- referencing request. Accordingly, it can be identified that there are some uncertainties when analysing case laws regarding the journalism exception. Nevertheless, the courts of justice have given directions for the execution of the journalism exception.

4.3 Data Protection Framework in the United Kingdom

4.3.1 Introduction

The evolution of data protection and privacy laws in the UK dates back to the 1970s. The 'Younger Committee's Report' on Privacy in 1972, the 'Lindop report on data protection' in 1978, can be identified as the main reports concerned about data protection in the

[269] *Buivids (n 61)* para 56.

[270] *Satamedia* (n 60) para 61, *Buivids* (n 61) para 53.

[271] *Buivids* (n 61) para 58.

[272](2018) EWHC 799 (QB) (2018) 3 WLR 1165 (99).

UK.[273] This sets out ten key principles for managing personal data. These principles influenced the current data protection legislation in Europe.[274]

The Conservative Administration of the UK introduced the Data Protection Bill in 1982, and it was adopted as statute in 1984.[275] However, this act was applied only to data stored on computers.[276]

Subsequently, the UK Parliament enacted the 'Data Protection Act 1998' to give effect to DPD within the UK.[277] Also, the 'Data Protection Act 1984' was replaced by this act. This Act covers personal data that is either stored digitally on a computer or maintained in a structured physical document system.

In line with the EU GDPR, the UK integrated its provisions into domestic legislation via the 'Data Protection Act 2018' by replacing the 'Data Protection Act 1998'.[278] Accordingly, the UK was the first country to incorporate GDPR into domestic law.[279] It offers a fresh and comprehensive foundation for safeguarding personal data by establishing new standards. However, after Brexit, the UK introduced its own framework based on the EU GDPR, referred to as the UK GDPR. [280]According to Carey and Treacy,

---

[273] Adam Warren & James Dearnley, "Data Protection Legislation in the United Kingdom, from development to statute 1969-84, 12 April 2011, page 238-263, https://doi.org/10.1080/13691180500146383 accessed 13 June 2025.

[274] ibid.

[275] "What is the freedom of information and data protection?", University College of London, < https://www.ucl.ac.uk/constitution-unit/research-areas/research-archive/freedom-information-and-data-protection-archive/what-freedom> Accessed 13 June 2025

[276] ibid.

[277] ibid.

[278] Cynthia O'Donoghue and John O'Brien, 'Data Protection Act 2018 Comes into Force' (*technology law dispatch.com*, 15 June 2018), accessed 22 May 2025.

[279] See n 20.

[280] ibid.

the post-Brexit version of GDPR in the UK bears many similarities to the EU rule and imposes similar duties on data controllers and processors.[281] Further, they state that the GDPR in the UK is supplemented by the DPA 2018.[282]

The EU GDPR and UK GDPR are largely similar in nature. Therefore, this section will not address concepts that are virtually identical, such as data protection principles and data subject rights, etc. Instead, the focus will be on highlighting the key differences between the two regimes, with particular attention to the treatment of SMEs and journalistic purposes under the UK GDPR and the DPA 2018.

4.3.2 Compliance of SMEs under the UK GDPR and DPA 2018

The EU GDPR and UK GDPR share a similar framework, facilitating easier compliance for organisations under both regulations. Both regulations follow the same compliance requirements. Nevertheless, there is a difference in the territorial and extraterritorial coverage. The EU GDPR applies uniformly to all EU member states, whereas the UK GDPR is specifically enforceable within the United Kingdom.

The UK GDPR applies to all businesses regardless of their size. Nevertheless, it provides that enterprises with fewer than 250 employees are not obligated to maintain records.[283] According to the 'Procurement Act 2023' in the UK, SMEs mean: '[H]ave fewer than 250 staff and have a turnover of an amount less than or equal to £ 44 million, or a balance sheet total of an amount less than or equal to £ 38 million.'[284]

---

[281] See n 20.

[282] ibid.

[283] ibid, Article 30(5).

[284] The Procurement Act 2023, s 123.

Additionally, the UK GDPR promotes the development of codes of conduct that take into account the unique requirements of MSMEs, aiming to support their effective and practical adherence with the regulation.[285]

Similarly, Article 42 of the GDPR promotes the creation of certification mechanisms to support compliance with the regulation. This provision explicitly states that the particular needs of MSMEs must be considered in the design and implementation of such certification processes.[286]

Accordingly, UK-based businesses are required to pay a data protection fee to the 'Information Commissioner's Office' (ICO).[287] The amount of the fee depends on the business's size or scale. If the payment has not been paid by the business enterprises, warning letters are issued, and fines are imposed by the ICO. Nevertheless, business enterprises that have already paid the annual fee are added to the ICO register.

Accordingly, the ICO is a highly independent body, exempt from political interference. The ICO has extensive investigative and corrective powers.[288] Also, it has the power to perform a consensual audit of a controller or processor to check whether companies are adhering to acceptable data processing procedures.[289]

Under the UK GDPR, the appointment of DPOs is not compulsory. Article 37 provides requirements for designating DPOs. Hence, the appointment of DPOs is required only under specific circumstances.[290] It is acknowledged as a solution to the financial and

---

[285] UK GDPR, Art 40.

[286] ibid., Art 42.

[287] "GDPR for Small Businesses, why is it important and how to comply" < dataguard.com/blog/gdpr-for-small-businesses > Accessed 15 June 2025.

[288] UK GDPR, Art 58.

[289] ibid.

[290] ibid, Art 37.

human resource challenges faced by SMEs. The foregoing findings demonstrate the special consideration given to SMEs under the UK GDPR.

4.3.3 Journalistic Exemptions under the DPA 2018 and UK GDPR

The UK has incorporated Article 85 of the GDPR into its domestic legal framework through the DPA 2018 by introducing a 'special purposes' exemption.[291] A substantive exemption is outlined under Section 15(2)(e), and the procedural authority to stay proceedings related to this exemption is explained in Sections 174 to 179 of the Act.[292]

'Special purposes' exemption seeks to balance the right to data protection with the right to freedom of expression, particularly in contexts where public interest considerations are paramount. Additionally, the data processor has the right to request a stay of legal proceedings if the personal data in question is being processed solely for special purposes and the publication has not yet been made.[293] Nevertheless, according to section 176(2) of the DPA 2018, although the material has been published previously, publication within the first 24 hours can be ignored.[294]

In *Sugar v. British Broadcasting Corporation*[295] case, the Supreme Court determined that what journalism involves, Lord Wilson provided three classifications of journalistic activity, which are 'first, the collecting, writing and verifying of material for publication,

---

[291] Data Protection Act 2018, Schedule 2 para 26.

[292] ibid S. 15(2) (e) and S. 174- 179.

[293] Data Protection Act 2018 S.176 (1) (a).

[294] ibid.S.176 (2).

[295] *Sugar* (n 62).

second, the editing of the material…….., and third, the maintenance and enhancement of the standards of the output by reviews of its quality.'[296]

According to the above-mentioned findings, it can be identified that there are provisions for journalism exception under the UK GDPR and DPA 2018, and these provisions are interpreted by the courts, which can be learn valuable lessons for Sri Lanka.

4.4 Comparative Analysis of the EU and UK Legal Frameworks with the Sri Lankan Legal Regime

As a Union that upholds one of the world's most robust and valuable data protection frameworks, the EU has established the strongest safeguards for the right to privacy and data protection through the GDPR. Also, the EU Charter explicitly guaranteed data protection as a fundamental human right.[297] Accordingly, the EU's data protection framework, along with its effective elements, can be used as a model to develop a new data protection legal regime in Sri Lanka.

Also, the UK-GDPR is closely similar to the EU GDPR, with the difference that it has been updated to fit domestic legal requirements.[298] Privacy is strongly upheld within the UK's data protection framework, reflected in the data privacy principles outlined in the DPA 2018, which align with the standards of the GDPR. Accordingly, I intend to do a comparative analysis of both the EU and the UK's data protection laws with the Sri Lankan data protection and privacy legal regime.

According to the above-mentioned findings, many case laws are addressed to the data protection principles and emerging issues in this regard. Also, there are several case laws

---

[296] *Sugar* (n 62).

[297] EU Charter (n 17), Article 8.

[298] Cookiebot, 'New UK-GDPR law after Brexitl Compliance with Cookiebot CMP' (*Cookiebot*, 01 July 2021) <https://www.cookibot.com/en/uk-gdpr/>Accessed 28 May 2025.

regarding the definitions of 'personal data' and 'data processing'. Hence, Sri Lanka can learn important lessons from the EU GDPR and case laws regarding data protection to resolve issues.

Additionally, Sri Lanka can greatly benefit from understanding the entitlements of data subjects alongside the responsibilities of data controllers and processors under the GDPR. Accordingly, controllers or processors do not need to designate data protection officers at all times.[299] This Article provides the requirements and situations for appointing data protection officers. This can be identified as the solution for the cost effects of the SMEs.

In Sri Lanka, the 'Personal Data Protection Amendment Bill' was published by the Minister of Digital Economy, by way of a gazette notification, on 27th March 2025.[300] Currently, it is in the parliamentary debating stage. It includes the amendments for sections 1, 12, 17, 20, 24, 25, 26 and 56. The meaning of the 'Public Authority' has changed under the new bill, which tries to reduce the designation of DPOs. Accordingly, Public Corporations or a company incorporated under the 'Companies Act, No. 07 of 2007', does not include the meaning of the 'public authority.'[301]

One of the main issues under the DPA is that it is not an independent body. According to the EU GDPR, the Supervisory Authority must be independent. In the parliamentary debate regarding the Personal Data Protection Bill held on 03rd June 2025, this issue was questioned.[302] However, this issue has not been amended under the new Bill. Accordingly, Sri Lanka can learn a lesson from the GDPR on how to establish an independent supervisory authority.

---

[299] UK GDPR, Article 37.

[300] "Cabinet Endorses PDPA Amendments to strengthen Stakeholder Alignment and Regulatory Capacity Prior to Enforcement" Media Release, 24 February 2025, Ministry of Digital Economy < https://www.dpa.gov.lk > Accessed 20th April 2025.

[301] Personal Data Protection Amendment Bill, Sri Lanka.

[302] Hansards of 03 June 2025 < https://www.parliament.lk/en/business-of-parliament/hansards?start=20> accessed 10 August 2025.

In considering SMEs, both the EU GDPR and the UK GDPR have given special attention to the implementation issues from the drafting level. Nevertheless, in Sri Lanka, the PDPA or the new Amendment Bill to the PDPA does not concern SMEs and does not mention any provision regarding SMEs.

Also, the PDPA does not provide exceptions for journalistic purposes like the EU and the UK's data protection laws.[303] As I discussed earlier, both the EU and UK data protection legal regimes try to maintain an equilibrium between the right to access information and the right to privacy and data protection. Also, there were many case laws in the EU and the UK regarding the journalism exemption. Sri Lanka can learn lessons from both jurisdictions on how to protect the freedom of expression while protecting personal data and privacy.

According to the findings of this research, Multiple international covenants of human rights acknowledge privacy as an essential basic right. Nonetheless, it is not explicitly protected as a constitutional right in Sri Lanka.

It has also been noted that selected jurisdictions have developed their own data protection regimes by passing legislation that is specifically suited to their requirements and aims to give citizens better control and protection over their personal data. Accordingly, these selected countries were able to get benefits from the digital market economy. Therefore, these optimal methods provide practical lessons for Sri Lanka for developing its own data protection regime.

[303] Data Protection Directive 1995, art9, Data Protection Act 1998, s.32, Data Protection Act 2018, s.176, EU GDPR, art.85(1) 85(2).

CHAPTER 5

CONCLUSION AND RECOMMENDATIONS

5.1 Introduction

The first section of this Chapter presents the study's findings. The second section of this Chapter contains recommendations for creating an effective legal framework for Sri Lankan data protection and privacy with special reference to SMEs and journalistic purposes, in keeping with the study's primary goal.

5.2 Conclusion

The key findings discussed in the previous chapters indicate that data collection through digital devices and its processing by public and private sector entities have significantly increased in the Sri Lankan digital landscape. Today, personal data can be regarded as the lifeblood of the commercial sector, and through their daily operations, both sectors store, collect, and share large amounts of personal data. Due to these technological developments, the issue of data protection has garnered attention, and Sri Lanka is not well-equipped to prevent data breaches as it lacks proper legislation and regulations in this area.

According to the findings of this research, it was revealed that, apart from the minimal safeguards offered through the common law remedy of *actio injuriarum* and a few statutory provisions, Sri Lanka lacked substantive legislation to regulate data protection until very recently. Although the Sri Lankan parliament passed the PDPA, the

effectiveness of this legislation has not yet been determined. Limited scholarship assesses the effectiveness of this act because it is the latest enactment.

As mentioned earlier, Data protection and privacy can be identified as inextricably connected concepts. Privacy is necessary for protecting personal and business data from unauthorised access. Many international covenants on human rights recognise privacy as a basic human right.[304] Also, Various countries have guaranteed privacy as a basic right under their constitutions.[305] However, the Sri Lankan situation is totally different, and the Constitution does not expressly recognise the right to privacy. As previously mentioned, the balance between privacy rights and the right to information remains unresolved.

However, creating a universal legal regime for privacy and data protection is a difficult endeavour. Nonetheless, establishing at least the fundamental requirements for data protection and privacy is essential. Accordingly, the PDPA can be recognised as a fulfilment of the gap regarding the legal framework of data protection and privacy to some extent.

Nevertheless, the PDPA does not fully align with international standards when compared to the data protection and privacy frameworks of the EU and the UK. As a result of the lack of international consistency, numerous problems may arise. It might result in limitations on foreign investment and trade. Furthermore, it may influence the confidence of individuals, direct and indirect investors, online consumers, etc.

---

[304] UDHR (n 26) Art 12, ICCPR (n 99) Art 17.

[305] Constitution of Thailand 2017, s 32.

According to the findings of this research, it was revealed that under the GDPR, member states are obliged to set up an independent Data Supervisory Authority.[306] However, under the PDPA, the DPA in Sri Lanka is not an independent body.[307] Nevertheless, the UK ICO functions with substantial autonomy. Both the UK GDPR and the DPA 2018 legally guarantee the Commissioner's independence.[308] As such, the Information Commissioner is accountable directly to Parliament rather than the government. This structure ensures regulatory oversight free from direct political influence. Also, the ICO operates independently, free from external instruction in the execution of its duties. Its internal decision-making framework safeguards impartiality and autonomy. Moreover, the ICO is vested with broad discretionary powers to oversee and enforce compliance with the UK GDPR and DPA 2018. These powers include issuing guidance, providing advice, conducting audits and assessments, addressing systemic violations, issuing warnings, and initiating prosecutions. Although in Sri Lanka, the PDPA provides discretionary powers for monitoring and enforcement of the act, it can be identified that there is a political interference in the recruitment process of the higher-level positions, which are the chairman and Board members.

Also, GDPR pays special attention to SMEs throughout the regulation. Accordingly, SMEs with fewer than 250 employees do not need to follow a record-keeping process under the GDPR.[309] Also, the GDPR encourages the formulation of a code of conduct for organisations that process personal data for the proper execution of this regulation and considers the specific needs of MSMEs.[310] Furthermore, the GDPR demonstrates the

---

[306] EU GDPR, art 58(1).

[307] The Personal Data Protection Act, No. 9 of 2022, s.29(3).

[308] UK GDPR art.52, DPA 2018 Part V.

[309] ibid, art 30(5).

[310] EU GDPR (n 49), Rec 98 and Art 40.

establishment of a certification mechanism for compliance with the GDPR, and the specific needs of MSMEs should be taken into account in this certification mechanism.[311] Moreover, the EDPB launched guidelines for small businesses to easily understand the GDPR and ensure compliance with the GDPR.[312] Nevertheless, in Sri Lanka, the PDPA or the new Amendment Bill to the PDPA does not concern SMEs and does not mention any provision regarding SMEs.

Also, it can be identified that the PDPA does not provide exceptions for journalistic purposes like the EU and the UK's data protection laws. Article 85(1) and Article 85 (2) of the GDPR provide exceptions and derogations for 'journalistic purposes and purposes of academic, artistic, and literary expression'. Also, the GDPR emphasises the importance of interpreting the term 'Journalism' broadly.[313]

Additionally, the ICO has issued a Code of Practice on Data Protection and Journalism to assist journalists in navigating their responsibilities under data protection law while safeguarding freedom of expression.[314] This code seeks to strike a balance between the public's right to information and the protection of individuals' personal data. The code primarily targets media organisations and journalists, including those working in the press, broadcast media, and online news platforms. It also applies to press agencies and freelance journalists who supply content to these outlets. The code underscores that journalists are generally expected to comply with data protection laws when handling personal

---

[311] ibid., Article 42.

[312] EDPB Launches Data Protection Guide for Small Businesses, 27 April 2023, < https://www.edpb.europa.eu/news/news/2023/edpb-launches-data-protection-guide-small-business > Accessed 15 May 2025.

[313] EU GDPR, Rec 153.

[314] 'Data Protection and Journalism Code of Practice', issued by the Information Commissioner's Office in 2023. < https://ico.org.uk/media2/migrated/4025760/data-protection-and-journalism-code-202307.pdf> Accessed 30 July 2025.

information for journalistic purposes. However, it also outlines specific criteria for invoking the journalism exemption. This exemption applies when personal data is used for journalistic activities, the journalist acts with the intention or expectation of publishing it, plausibly believes that the publication serves the 'public interest', and considers that adhering to a specific requirement of data protection law would be agreeable with journalistic objectives.[315] Further, it highlights the interpretation of journalism broadly encompassing all content published in newspapers or magazines, or broadcast via radio or television, excluding paid advertisements. It also includes content produced by non-professional journalists, such as members of the public engaging in citizen journalism, such as bloggers, eyewitnesses, or social media users, as well as material that serves both journalistic and additional purposes, such as campaigning.[316]

In the Sri Lankan context, there is currently no comprehensive legislation that safeguards the rights of journalism, nor is there a clear definition of the term 'journalism'. The Press Council Law, enacted in 1973, remains old and has not undergone any significant amendments. While it defines the term 'newspaper,' it fails to define journalism. Similarly, the Online Safety Act, No. 9 of 2024, recently enacted by Parliament, defines 'social media platform' but does not define 'journalism.' Therefore, if a journalism exemption is to be introduced into PDPA, it is essential to establish a clear definition of journalistic activities. Moreover, there should be consistent and well-defined criteria for applying the journalism exemption, similar to the approach taken in the UK.

It can be noted that the UK has developed its data protection regimes by passing legislation that is specifically suited to its requirements and aims to give citizens better control and protection over their personal data. Accordingly, the UK has been able to get

[315] See n 314.

[316] ibid.

benefits from the digital market economy. Therefore, these optimal methods provide practical lessons for Sri Lanka for developing its data protection regime to address serious issues about the data protection and privacy of the country.

Based on the findings, this study concludes that Sri Lanka lacks sufficient legal safeguards for personal data in comparison to international legal advancements. As a result, Sri Lanka must immediately take the required steps to build a thorough, effective data privacy framework that provides proactive protection in line with globally accepted standards and practices to win the faith and confidence of both investors and individuals while protecting other rights. Also, as a middle-income country, Sri Lanka should pay special attention to SMEs, which contribute a considerable percentage to the country's economic growth, in adhering to the personal data protection laws.

5.3 Recommendations

Based on the above-mentioned findings, the following recommendations are put forward to create a new effective data protection regime in Sri Lanka in accordance with the research objectives:

5.3.1 Specific Recommendations

I. Proposed amendments to the Constitution of Sri Lanka

- Ensure the right to privacy as a fundamental right under the Sri Lankan Constitution. Accordingly, Chapter III of the Constitution should be amended by incorporating a new article on the right to privacy.

- Enhancing the proposed fundamental rights by revising Article 28 of the Constitution on 'fundamental duties' to explicitly mandate respecting the right to privacy of others.
- Introducing comparable amendments to Chapter VI of the Constitution, 'Directive Principles of State Policy and Fundamental Duties,' for strengthening the fundamental duty to respect the rights of others' privacy.

II. Proposed Amendments to the 'Personal Data Protection Act, No. 09 of 2022'

- To ensure the DPA's independence, its members should be designated by an autonomous body instead of the government. According to the EU GDPR, the Supervisory Authority must be independent. I recommend that these appointments be done through the Constitutional Council of Sri Lanka, which is an independent body. Accordingly, section 29 (3) of this Act should be amended.
- PDPA should pay special attention to SMEs, like the GDPR. Although all sizes of business entities are subject to data protection obligations, in considering a country's economic situation, SMEs cannot bear the extra cost for the recruitment process and getting technical and informational support for complying with the PDPA. Also, most of the SMEs are located in rural areas and are unaware of how to comply with the PDPA. Some MSMEs are run by one or two employees. Practically, they have to face difficulties in complying with the Act. Accordingly, I proposed an amendment to the PDPA to include a specific section for SMEs, as 'SMEs with fewer than 300 employees do not need to follow the record-keeping process.' At the same time, micro-enterprises with fewer than ten employees should be exempted from compliance with this act. However, micro enterprises

that process special categories of personal data should not be exempted in this regard.

- Additionally, I propose amending the PDPA to include an exemption for journalistic purposes. I also suggest defining what constitutes journalistic purposes. Furthermore, I propose to establish a code of conduct for journalistic purposes and data protection. It should specifically mention the consistent criteria for applying the journalism exception. Sri Lanka can draw lessons from the EU GDPR and the UK GDPR, particularly from the case law of the EU and the UK.
- Section 20 (1) (a) of the PDPA provides that the government bodies need to appoint DPOs. However, Public Corporations have been excluded by the new amendment to the PDPA to reduce the cost of appointing new data protection officers. It can be identified as a good trend. Section 20 (1) (b) provides the other instances in which DPOs should be appointed. Nevertheless, this section has not specifically mentioned the instances, and it can be defined very broadly. I recommend amending this section and specifically mentioning that the instances in DPOs should be appointed.

III. Recommendations for the implementation mechanism of the PDPA

- Ensuring that individuals have access to legal remedies against data misuse under the PDPA is essential. Without a clear enforcement framework, guaranteeing compliance would be challenging and would make the legislation merely symbolic. Therefore, it is essential to ensure a clear enforcement mechanism under this new law. The government must act right away to enforce the PDPA.
- Accordingly, I recommend establishing a code of conduct for organisations that process personal data for the effective implementation of the PDPA, specifically

concerning the specific needs of MSMEs. Sri Lanka can learn special lessons from the GDPR in creating this code of conduct.

- Also, I recommend establishing a special certification mechanism for organisations that process personal data for compliance with the PDPA. However, certification fees should be based on the size of the businesses, and a system should be set up to review annually the adequacy of the measures taken by the organisation to protect the personal data. According to Section 34 of the PDPA, the DPA can issue licenses to regulate identity management and related services.[317] However, this section does not mention the certification mechanism for all organisations that process personal data.
- It is important to ensure that individuals in Sri Lanka are notified of data breaches and potential violations of their rights, and that they have access to legal protections against these infringements. I recommend issuing guidelines regarding PDPA to make it easy to understand the PDPA for any organisation that processes personal data, including understanding the data protection basics, rights of the data subjects, compliance with the PDPA, and how to secure personal data, penalties of data breaches, etc. It can include videos, flowcharts, and interactive materials to make it easy to understand the PDPA.
- DPA should identify the challenges in the implementation process of the GDPR, such as technical, legal, organisational, and regulatory challenges, etc. Specifically, they should identify challenges faced by the SMEs in implementing the PDPA, including insufficient human resources and budget limitations, lack of awareness, etc. Accordingly, they should take measures to minimise these problems. This can be included,

[317] The Personal Data Protection Act, No. 9 of 2022, s.34.

1. Considering the size of the business when issuing charges for the certification mechanism.

Businesses operating in the UK are obligated to remit a data protection fee to the ICO. The fee is calculated according to the scale of the business. For charities and SMEs, it is approximately Great Britain Pounds (GBP) 52 to 78. However, large organisations should pay GBP 3763 per year.[318] According to the PDPA, large businesses in Sri Lanka also do not need to pay a data protection fee, and there is no certification mechanism. As a result, the Sri Lankan treasury must cover costs related to the function of the DPA. I propose establishing a certification mechanism, exempting micro enterprises from this requirement and the data protection fee. SMEs should pay an annual fee of less than 12000 Rupees, while large enterprises should pay 120,000 Rupees annually.

2. Conducting awareness programmes about the PDPA,

The DPA should take proactive steps to support SMEs in understanding and complying with the PDPA. This can be achieved through the organisation of targeted awareness programmes focused on key areas such as PDPA obligations, lawful data processing practices, appropriate security measures, and practical procedures for compliance.

These programs should be specifically designed to tackle the distinct challenges that SMEs encounter, particularly those with limited resources or technical expertise. Moreover, the DPA should establish feedback mechanisms to gather insights from participants, evaluate the success of the training sessions, and recognise areas that need further development. Regular audits and assessments

[318] 'Guide to the Data Protection Fee/ICO', Information Commissioner's Office, <https://ico.org.uk/for-organisations/data-protection-fee/data-protection-fee/> Accessed 10 August 2025.

should also be conducted to ensure that data protection measures are properly implemented and to identify any existing compliance gaps. This multi-faceted approach will enhance the overall effectiveness of the PDPA and ensure broader compliance across different business sectors.

In addition, the DPA should encourage organisations to prioritise internal staff education by promoting ongoing training and fostering a culture of data protection across all levels. These training initiatives should address essential topics such as data processing practices, security measures, breach reporting protocols, etc. A variety of training delivery methods, such as e-learning platforms, in-person workshops, and interactive exercises, should be used to maximise engagement. Furthermore, training resources must be accessible to all employees, accommodating different learning styles, language proficiencies, and levels of digital literacy. By institutionalising continuous training, organisations can ensure that data protection becomes an integral part of their operations and compliance strategies.

3. Providing technical knowledge for data processing activities

Providing technical knowledge is essential to ensure the secure, lawful, and efficient handling of personal data. This involves a comprehensive understanding of data protection principles and the adoption of suitable technical and organizational safeguards, such as maintaining accurate records of processing activities, adopting risk-based approaches, conducting DPIAs, etc.

4. The DPA can introduce standard contractual clauses (SCCs)

SCCs can be particularly beneficial for SMEs, which often lack the capacity to negotiate bespoke data transfer agreements with each commercial partner. To support such organisations, the UK has introduced its own version of SCCs, known as the

'International Data Transfer Agreement' (IDTA).[319] Key benefits of using SCCs are providing a ready-made legal framework that reduces the need for drafting individual agreements, minimising legal expenses and administrative effort, especially critical for resource-constrained SMEs, and ensuring personal data is consistently protected during international transfers. Also, demonstrating a commitment to data protection can improve an organisation's reputation and strengthen trust among customers and stakeholders.

- Also, Government officials should be aware of the data protection laws. According to Section 20(1) of the PDPA, 'if the processing is carried out by a government ministry, department, or public corporation, the controller or processor shall appoint DPOs. Furthermore, they should be aware of doing the DPIA.[320] There are some limitations on the public authorities regarding cross-border transfers, and government officials should be aware of these special circumstances. [321] Accordingly, I recommend organising awareness programmes for government officials about the PDPA.
- Furthermore, if law enforcement officials are not familiar with the relevant regulations, personal rights cannot be enforced efficiently. Therefore, it is crucial to organized judges' training programmes, awareness programmes for lawyers, and other law enforcement personnel regarding data protection laws.
- Also, it is crucial to conduct awareness programmes for professionals that involve journalistic activities and explain what types of journalistic activities come under

[319] 'International Data Transfer Agreement' (IDTA), issued by the Information Commissioner's Office. <https://ico.org.uk/media2/migrated/4019538/international-data-transfer-agreement.pdf> Accessed 01 August 2025.

[320] The Personal Data Protection Act, No. 9 of 2022, s.24.

[321] ibid, s.26.

the exemption. Moreover, it is essential to emphasise the importance of protecting personal data and the penalties of data breaches under the PDPA.

5.3.2 General Recommendations

- There should be a balance between the needs of the data subjects, data users, and society. This can be achieved by treating all parties' interests with equal importance, while ensuring that the rights of data subjects remain paramount.
- It could be argued that Sri Lanka will be hesitant to enact a comprehensive law governing data protection and privacy due to several factors, such as a lack of resources, an insufficient IT infrastructure, funding issues, political issues, etc. However, according to the above-mentioned findings, there are lots of problems that can be identified at present. Hence, it is crucial for Sri Lanka to promptly enforce the PDPA to safeguard individuals' privacy and ensure data security.

BIBLIOGRAPHY

Primary Sources

Legislation

Sri Lankan Legislation

Computer Crime Act, No. 24 of 2007

Electronic Transactions Act, No. 19 of 2006

Information and Communication Technology Act, No. 27 of 2003

International Covenant on Civil and Political Rights (ICCPR) Act No. 56 of 2007

Payment Devices Fraud Act, No 30 of 2006

Personal Data Protection Act, No.9 of 2022

Personal Data Protection Amendment Bill, Sri Lanka

Post Office Ordinance No. 11 of 1908

Right to Information Act, No. 12 of 2016

Sri Lanka Telecommunications Act, No. 25 of 1991

The Constitution of the Democratic Socialist Republic of Sri Lanka, 1978

The United Kingdom Legislation

Data Protection Act, 2018

Data Protection Act, 1998

Data Protection Act, 1984

Freedom of Information Act, 2000

General Data Protection Regulations (GDPR)

Human Rights Act 1998 (UK)

The Procurement Act 2023

The European Union Legislation

Council of Europe, European Convention on Human Rights and Fundamental Freedoms, 3 September 1953 (ECHR)

Council of Europe, Convention for the Protection of Individuals with regard to the Automatic Processing of Individual Data, 28 January 1981, ETS 108

European Union, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, OJ 1995 L 281/31. (Data Protection Directive)

European Union, Charter of Fundamental Rights of the European Union, 18 December 2000 (2000/C 364/01) (EU Bill of Rights).

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of natural Persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1 (came into force on 25th May 2018) (EU GDPR).

Other Legislation

Constitution of Thailand, 1997

United States Constitution, 1789

International Instruments

Convention for the Protection of Individuals about Automatic Processing of Personal Data (Treaty 108)

International Covenant on Civil and Political Rights 1966 (ICCPR)

Universal Declaration of Human Rights 1948 (UDHR)

Case Laws

Sri Lankan Cases

Nadarajah v Obeysekera [1971] 52 NLR 76

Sinha Rathnathunge v The State [2001] 2 SLR 172

Sirimane vs. New Indian Assurance Company Limited 35 NLR 413.

European Union & UK Cases

Commission v Germany, [2010] ECR I-01885.

Frantisek Rynes v. Urad pro ochranu osobnich udaju, C-212/13, EU: C: 2014: 2428

Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González C-131/12 [2012] OJ C165/11

Nowak v. Data Protection Commissioner, 1/1 C- 434/16, ECLI:EU:C:2017:994

NTI v. Google LLC (2018) EWHC 799 (QB) (2018) 3 WLR 1165 (99)

Patrick Breyer v. Bundesrepublik Deutchland ECLI:EU:C: 2016:779

Satakunnan Markkinaporssi and Satamedia [2008] ECLI: EU: C: 2008:727

Sergejs Buivids v. Datu Valsts Inspekcija[2019] ECLI: EU: C: 2019:122 2

Sugar V. British Broadcasting Corporation [2012] UKSC 4, [2012] 1 WLR 43

United States Cases

Katz v. United States, [1967] 389 U.S.347.

Indian Cases

Justice K.S. Puttaswamy (Retd.) and Anr. v. Union of India and Ors. [(2017) 10 SCC 1]

SECONDARY LEGAL SOURCES

Books

Abeyratne S D B, *Introduction to Information and Communication Technology Law* (Author Publication 2008)

Ausloos J, *The Right to Erasure in EU Data Protection* (7th edn, OUP Oxford 2020)

Carey P, Data Protection: *A Practical Guide to UK and EU Law* (5th edn, OUP 2018)

Greenleaf G, *Asian Data Privacy Laws: Trade & Human Rights Perspectives* (1st edn, Oxford University Press 2014)

Gunawardena N, *Digital Transformation in Sri Lanka; Opportunities and Challenges in Pursuit of Liberal Policies*, (Friedrich Naumann Foundation (FNF) Sri Lanka, 2017) 1-101, 22.

Crotty M, *The Foundations of Social Research: Meaning and Perspectives in the Research Process* (3rd edn, Sage Publications 2003) 1-233, 10.

Lloyd I J, *Information Technology Law* (9th edn, OUP 2020)

United Nations Human Rights Office of the High Commissioner (OCHR), *Reproductive Rights are Human Rights – A Handbook for National Human Rights Institutions* (United Nations 2014)

Welfare D and Carey P, '*Territorial Scope and Terminology' in Peter Carey (ed), Data Protection: A Practical Guide to UK and EU Law* (5th edn, OUP 2018) 1-31, 2.

Westin A F, *Privacy and Freedom* (1st edn, Athenum, New York 1967)

Journal Articles

Abeysekara TB and. Ranasighe AE, 'Holistic Approach in Introducing Proper Legal Framework to regulate data protection and privacy in Sri Lanka', Vidyodaya Journal of

Management, 2022 vol 8(1) 169-200, < https://scholar.google.com> Accessed 04 November 2024

Abeyratne S D B, 'Contact tracing raises privacy concerns; Data Protection Bill in limbo' Daily Mirror Online (Sri Lanka, 12 November 2020) < http://www.dailymirror.lk/news-features/Contact-tracing-raises-privacy-concerns/131-199697>accessed 03 December 2024.

Berners-Lee T**,** 'The World Wide Web: A very short personal history' (1998), <https://www.w3.org/People/Berners-Lee/ShortHistory.html> accessed 21 October 2024

Freitas MDC and Silva MMD, 'GDPR Compliance in SMEs: There is much to be done', Journal of Information Systems Engineering and Management, Vol. 3 No.4, 30. https:// doi .org/ 10.20897/ jisem/ 3941 < chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.jisem-journal.com/download/gdpr-compliance-in-smes-there-is-much-to-be-done-3941.pdf > Accessed 30th January 2025.

Cochrane L, Zaniewicz LJ and Wills DB, "Data Protection Authorities and their Awareness- raising Duties under the GDPR: The Case for Engaging Umbrella Organizations to Disseminate Guidance for Small and Medium-Size Enterprises", European Data Protection Law review, Volume 6 (2020) issue 3, page 352-364, DOI: https://doi.org/10.21552/edpl/2020/3/6, < https://edpl.lexxion.eu/article/edpl/2020/3/6 > Accessed 5th December 2024.

Erodes D, 'Special, Personal and Broad Expression: Exploring Freedom of Expression Norms under the General Data Protection Regulation' Yearbook of European Law, Vol.40, No 1 (2021), pp. 398-430, doi:10.1093/yel/ yeab004, < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3565385> Accessed 03 December 2024.

European Commission, 'Commission report: EU data protection rules empower citizens and are fit for the digital age'(*ec.europa.eu*,24 June 2020)

<https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1163> Accessed 22 May 2025

Fernando J and Wickramasinhe S, 'Sri Lanka Data Protection Legislation- An Overview' (3 August 2022), <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4246818> Accessed 05 November 2024

Gabel D, Hickman T, "Unlocking the EU General Data Protection Regulation: A practical handbook on the EU's new data protection law" 28 May 2025 < https://www.whitecase.com/insight-our-thinking/chapter-1-introduction-unlocking-eu-general-data-protection-regulation > Accessed 10 June 2025.

Galina Kulakova, '7 principles of the GDPR and what they mean' (amara-marketing.com.co, 2019) <https://www.amara-marketig.com/travel-blog/7-principles-of-the-gdpr-and-what-they-mean>Accessed 13 May 2025.

Kemp S, 'Digital; 2025 Sri Lanka' (03 March 2025), <https://datareportal.com/reports/digital-2025-sri-lanka.> Accessed 10 April 2025

Kokott J & Sobotta C, 'The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECHR' (2013) vol 3\4 International Data Privacy Law 222–228. < https://doi.org/10.1093/idpl/ipt017> Accessed on 01 December 2024

Kulakova G, '7 principles of the GDPR and what they mean' (*amara-marketing.co*, 2019) < https://www.amara-marketing.com/travel-blog/7-principles-of-the-gdpr-and-what-they-mean> Accessed 13 May 2025

Longstaff G, 'The importance of data privacy law in the digital age', 11 October 2024, Accessed 12 December 2024.

Madushani TP, "Legislative Brief, Personal Data Protection Bill 2021", <https:// www.tisrilanka.org uploads 2021/07> Accessed 05 December 2024.

Mahanamahewa P, ‘Data Protection Law an E-Business and E-Government Perception’ (2003) Ph.D. Research Scholar in IT Law < http://www.mediareform.lk/wp-content/uploads/2020/02/67-Prathiba-Mahanamahewa-2003-Data-Protection-Law-An-E-Business-and-E-Government-Perception.pdf>. Accessed 22 October 2024

Marsoof A, ‘Privacy Related Computer Crimes: A Critical Review of the Computer Crimes Act of Sri Lanka’ (2007) 5 Sri Lanka Law College Law Review

Marsoof A, ‘The Right to Privacy in the Information Era: A South Asian Perspective’ (2008) 5(3) Script-ed 553

O’Donoghue C and O'Brien J, ‘Data Protection Act 2018 Comes into Force’ (*technology law dispatch.com*, 15 June 2018), <https://www.technologylawdisptch.com/2018/06/privacy-data-proection/data-protection-act-2018-comes-into-force/> Accessed 22 May 2025.

‘Non-Agricultural Economic Activities in Sri Lanka, Economic Census 2013/2014’, Listing Phase, Department of Census and Statistics, Ministry of Policy and Planning Economic Affairs, Child Youth and Cultural Affairs, < http://www.statistics.gov.lk> Accessed 10 April 2025.

Petters J, ‘Data Privacy Guide: Definitions Explanations and Legislation’ (28 September 2020) < https://www.varonis.com/blog/data-privacy/> accessed 10 February 2025

Samarajeewa R, ‘Personal Data Protection Act Passed; what will it mean’, (22 March 2023) <https://srilankabrief.org/personal-data-protection-act-passed-what-will-it-mean-prof-rohan-samarajiva/> accessed 05 November 2024

Smirnova Y, and Travieso-Morals V, “Understanding Challenges of GDPR Implementation in Business Enterprises: A Systemic Literature Review”, January 2024, International Journal of Law and Management 66 (3): 326-344, doi:10.1108/IJLMA-08-2023-0170,

<https://www.researchgate.net/publication/377572957_Understanding_challenges_of_GDPR_implementation_in_business_enterprises_a_systematic_literature_review> Accessed 03rd December 2024.

Swire PP, Ahmad K and McQuay T, *Foundations of Information Privacy and Data Protection: A Survey of Global Concepts, Laws and Practices* (N.H. International Association of Privacy Professional, UK 2012).

The Economist, 'The world's most valuable resource is no longer oil but data' (*economist.com*, 6th May 2017) <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data> Accessed 12 December 2024.

United Nations Conference on Trade and Development, 'Data protection regulations and international data flows: Implications for trade and development' (New York and Geneva, 2016) < https://unctad.org/system/files/official-document/dtlstict2016d1_en.pdf> accessed 25 October 2024

Warren SD & Brandeis LD, 'The Right to Privacy' (1890) IV (5) Harvard Law Review 193<https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html> accessed 20 October 2024

Warren A & Dearnley J, "Data Protection Legislation in the United Kingdom, from development to statute 1969-84, 12 April 2011, page 238-263, https://doi.org/10.1080/13691180500146383 <https://www.tandfonline.com/doi/full/10.1080/13691180500146383?scroll=top&needAccess=true> Accessed 13 June 2025.

Wong B, "The Journalism Exemption in UK Data Protection Law", Journal of Media Law, 2020, vol 12. No 2, 216-236, https://doi.org/10.1080/17577632.2020.1843326.

Theses

Sapukotana U, 'Protecting eHealth Information Privacy: Towards a Legal Framework for Sri Lanka' (PhD Thesis, General Sir John Kotelawala Defence University 2019)

Websites

"Application of the Personal Data Protection Act No. 09 of 2022 in the Public Sector and Introduction to the Data Protection Authority", Circular No. 01/2024 issued by the Data Protection Authority. < https://www.dpa.gov.lk> Accessed 20th April 2025.

"Cabinet Endorses PDPA Amendments to strengthen Stakeholder Alignment and Regulatory Capacity Prior to Enforcement" Media Release, 24 February 2025, Ministry of Digital Economy < https://www.dpa.gov.lk > Accessed 20th April 2025.

Centre for Policy Alternative CPA in Sri Lanka, Right to Privacy in Sri Lanka, (September 2020) < https://www.cpalanka.org/right-to-privacy-in-sri-lanka/> accessed 21 November 2024

Cookiebot, 'New UK-GDPR law after Brexitl Compliance with Cookiebot CMP' (Cookiebot, 01 July 2021) < https://www.cookiebot.com/en/uk-gdpr/>. Accessed 28 May 2025.

Commission Recommendation concerning the definition of micro, small, and medium-sized enterprises on 06 May 2003 (C(2003)1422), 2003/361/EC, Official Journal of the European Union L 124/16 dated 20.05.2003. < https://eur-lex.europa.eu/eli/reco/2003/361/oj/eng > Accessed 10 July 2025

Communication from the Commission to the European Parliament and the Council, Second Report on the application of the General Data Protection Regulation, European Commission, Brussels COM (2024) 357 final. < https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52024DC0357> Accessed 15 May 2025.

Council of Europe, 'Modernisation of the Data Protection "Convention 108" ' (May 2018) <https://www.coe.int/en/web/portal/28-january-data-protection-day-factsheet> Accessed on 11 May 2025.

Council of the European Union, 'The general data protection regulation', < https://www.consilium.europa.eu/en/policies/data-protection-regulation/> Accessed 18 December 2024.

'Data Privacy Act; A brief history of Modern Data Privacy Laws', (10th April 2018) <https://blog.eperi.com/en/data-privacy-act-a-brief-history-of-modern-data-privacy-laws> Accessed 20th October 2024.

Data Protection Manager, 'What are the 7 principles of GDPR (01/10/2020), < https://dataprivacymanager.net/what-are-the-7-gdpr-principles/> accessed 13 May 2025

'Data Privacy Act; A brief history of Modern Data Privacy Laws', (10th April 2018) <https://blog.eperi.com/en/data-privacy-act-a-brief-history-of-modern-data-privacy-laws> Accessed 20 October 2024.

'Data Protection and Journalism Code of Practice', issued by the Information Commissioner's Office in 2023. < https://ico.org.uk/media2/migrated/4025760/data-protection-and-journalism-code-202307.pdf> Accessed 30 July 2025.

Department of Census and Statistics, "Key indicators of Industry Trade and Services Sector, Economic Census 2013/14", Press Release on 14.07.2015, <http:// www.statistics.gov.lk, chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.statistics.gov.lk/Economic/Non_agri/PRESS%20RELEASEEcoCen_en.pdf > Accessed 10 February 2025.

EDPB Launches Data Protection Guide for Small Businesses, 27 April 2023, < https://www.edpb.europa.eu/news/news/2023/edpb-launches-data-protection-guide-small-business > Accessed 15 May 2025.

European Commission, ‘Commission report: EU data protection rules empower citizens and are fit for the digital age’(*ec.europa.eu*,24June 2020) <https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1163> Accessed 12 May 2025.

“GDPR for Small Businesses, why is it important and how to comply” < dataguard.com/blog/gdpr-for-small-businesses > Accessed 15 June 2025.

‘Guide to the Data Protection Fee/ICO’, Information Commissioner’s Office, <https://ico.org.uk/for-organisations/data-protection-fee/data-protection-fee/> Accessed 10 August 2025.

Hansards of 03 June 2025 < https://www.parliament.lk/en/business-of-parliament/hansards?start=20> accessed 10 August 2025.

‘Impact of Economic Crisis on MSMEs, Insights and Analysis’, 2022, Ministry of Finance, Economic Stabilisation and National Policies in Sri Lanka, <https://www.statistics.gov.lk/Resource/en/Industry/Other_Tables_Reports/MSMEs_Report.pdf> Accessed 11 March 2025.

‘Impact of the economic crisis on MSMEs in Sri Lanka, Media release on 13th February 2024, Department of Census and Statistics, Ministry of Finance, Economic Stabilization and National Policies <https://www.statistics.gov.lk > Accessed 10 April 2025

Information Commissioner's Office, “An Overview of the Data Protection Act 2018”, < chromeextension://efaidnbmnnnibpcajpcglclefindmkaj/https://ico.org.uk/media/2614158/ico-introduction-to-the-data-protection-bill.pdf > accessed 28 January 2025.

‘International Data Transfer Agreement’ (IDTA), issued by the Information Commissioner’s Office. <https://ico.org.uk/media2/migrated/4019538/international-data-transfer-agreement.pdf> Accessed 01 August 2025.

IT Governance, ‘An Overview of UK Data Protection Law, the UK GDPR, DPA 2018 and EU GDPR, and the ePR and PECR’<https://www.itgovernance.co.uk/data-protection> accessed 13 October 2024

‘OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.’ <https://www.oecd.org/en/publications/2002/02/oecd-guidelines-on-the-protection-of-privacy-and-transborder-flows-of-personal-data_g1gh255f.html> Accessed 02 January 2025

O’Donoghue C and O'Brien J, ‘Data Protection Act 2018 Comes into Force’ (*technology law dispatch.com*, 15 June 2018),<https://www.technologylawdisptch.com/2018/06/privacy-data-proection/data-protection-act-2018-comes-into-force/> Accessed 22 May 2025.

‘National Policy Framework for Small and Medium Enterprises (SME) Development’, 2016, chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/http://www.sed.gov.lk/sedweb/en/wpcontent/uploads/2017/03/SME-fram-work_eng.pdf> Accessed 10 February 2025.

‘The Internal Market: General Principles’ Fact Sheets on the European Union < https://www.europarl.europa.eu/factsheets/en/sheet/33/the-internal-market-general-principles> accessed 10 April 2025

‘What is the freedom of information and data protection?’, < https://www.ucl.ac.uk/constitution-unit/research-areas/research-archive/freedom-information-and-data-protection-archive/what-freedom> Accessed 13 June 2025