UNIVERSITY of LUSAKA

Passion for Quality Education: Our Driving Force

SCHOOL OF LAW

A COMPARATIVE ANALYSIS OF THE DATA PROTECTION AND PRIVACY LAW LEGAL FRAMEWORK IN ZAMBIA AND THE UK

BY

NAKAUNDI NAKAZWE

LLB19116061

AN OBLIGATORY ESSAY SUBMITTED TO THE UNIVERSITY OF LUSAKA IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE AWARD OF THE BACHELOR OF LAWS (LLB) DEGREE.

2025

Table of Contents

DECLARATION I
RECOMMENDATION II
ACKNOWLEDGEMENT III
DEDICATION IV
CHAPTER ONE 1
1.0 Introduction 1
2.0 Background Of The Study 2
3.0 Statement Of The Problem 3
4.0 Research Objectives 4
4.1 Research Questions 4
5.0 Significance Of The Study 4
6.0 Scope Of The Study 5
7.0 Literature Review 5
8.0 Methodology 7
8.1 Research Approach 7
8.2 Research Type 7
8.3 Research Design 8
8.4 Data Collection Techniques 8
8.5 Study Population 8
8.6 Data Analysis 8
8.7 Sampling Size 8
8.8 Sampling Techniques 8
8.9 Ethical Considerations 9
CHAPTER TWO 10
THE CONCEPT OF DATA PROTECTION AND ITS IMPORTANCE 10
2.1 Introduction 10
2.2 Conceptual Foundations and Definitions 10
2.3 Historical Evolution and International Frameworks 13

2.4 Core Principles and Lawful Bases 14
2.5 Data subject rights 16
2.6 Controllers, Processors, Accountability and Security 17
2.7 Why Data Protection Matters 19
2.7.1 Human Dignity, Autonomy, and Equality 19
2.8 Conclusion 19
CHAPTER THREE 20
DATA PRIVACY LEGAL FRAMEWORKS IN ZAMBIA AND THE UNITED KINGDOM 20
3.0 Introduction 20
3.1 Data Protection Legal Framework in Zambia 20
3.1.1 Data Protection Act 20
3.1.2 Electronic Communications and Transactions Act 2021 23
3.1.3 Cyber Security Act No. 3 of 2025 24
3.1.4 The Cyber Crimes Act No. 4 of 2025 27
3.1.5 The Information and Communications and Technologies Act 28
3.2 Data Protection Legislation in the United Kingdom 29
3.2.1 The Data Protection Act of 2018 29
3.2.2 The Computer Misuse Act 1990 30
3.2.3 Telecommunications (Security) Act 2021 (TSA) 31
3.3 Conclusion 31
CHAPTER FOUR 32
COMPARATIVE ANALYSIS OF DATA PROTECTION LEGAL REGIMES IN ZAMBIA AND THE UNITED KINGDOM 32
4.0 Introduction 32
4.1 Conceptual and Philosophical Foundations of Data Protection 33
4.2 Critical Comparative Analysis of Specific Provisions 35
4.2.1 Institutional and Enforcement Mechanism 35
4.2.2 Scope and Definition of Personal Data 37
4.2.3 Autonomy of the Data Protection Commission 38
4.2.4 Rights of Data Subjects 42

4.2.5 Cross-Border Data Transfers 42
4.3 Cybersecurity and Ancillary Legislation 44
4.4 Public Awareness and Trust 45
4.5 Conclusion 45
CHAPTER FIVE 47
CONCLUSIONS AND RECOMMENDATIONS 47
5.0 Introduction 47
5.1 General Conclusion 47
5.2 Summary Of Chapters 48
5.2.1 Chapter One 48
5.2.2 Chapter Two 49
5.2.3 Chapter Three 49
5.2.4 Chapter Four 49
5.3 Recommendations 50
5.3.1 Legislative Harmonization 50
5.3.2 Strengthening The Office Of The Data Protection Commissioner 50
5.3.3 Respect Of Data Subject'S Consent 50
5.3.4 Public Awareness And Education 50
5.3.5 Capacity Building For Data Controllers And Processors 51
5.4 Final Remarks 51
Bibliography 52

DECLARATION

I declare that this dissertation entitled, **A COMPARATIVE ANALYSIS OF THE DATA PROTECTION AND PRIVACY LAW LEGAL FRAMEWORK IN ZAMBIA AND THE UK**

which is hereby submitted in partial fulfilment of the requirement for the award of a Bachelor's Degree at the University of Lusaka is my own original work and it has not been previously submitted for the award of a degree at this university or any other tertiary institution.

I understand what plagiarism entails and I'm aware of the University's policy in this regard. Thus, where other people's work is cited, I have duly acknowledged. The errors or omissions in this work are solely mine.

NAKAUNDI NAKAZWE

.....

2025

RECOMMENDATION

I **THOMAS MALAMA** do recommend that this dissertation titled **A COMPARATIVE ANALYSIS OF THE DATA PROTECTION AND PRIVACY LAW LEGAL FRAMEWORK IN ZAMBIA AND THE UK**, authored by **NAKAUNDI NAKAZWE** with Student Number LLB19116061 was done under my supervision, be admitted by the University. I have checked it carefully and I am satisfied that it meets the requirements related to the format laid down by the University regulations.

.....

MR THOMAS MALAMA

(Supervisor)

12th November 2025

(Date)

ACKNOWLEDGEMENT

First and foremost, I want to give my thanks to God, the Almighty, for all of his gifts, wisdom, and opportunities that have allowed me to complete the dissertation and get this far.

My profound appreciation is extended to Mr. Thomas Malama, my supervisor, who helped me finish the dissertation. His skill, perseverance, and talent for legal writing cannot be overlooked, Sir. I am so grateful.

Additionally, I want to thank Dr. Beatrice Chirwa for her encouragement and faith in me.

Finally, I would want to express my gratitude to everyone whose names are not listed but who nevertheless made me realize that with perseverance and God's grace, I can do anything.

DEDICATION

This dissertation is dedicated to my daughter Wane Namwinga.

CHAPTER ONE

1.0 Introduction

In a time when there has been a boom in technology breakthroughs and the world has become more interconnected than ever before the protection of personal data has become very critical both in personal lives and the corporate world .

Now than ever before there is a huge amount of data caused by the digital age's ever-expanding frontiers, emphasizing the importance of safeguarding this important resource. The intricacy stems from the mosaic of data protection and privacy regulations that have arisen across varied jurisdictions, each seeking to solve the intricate balance of utilising data for innovation and maintaining the sacrosanct rights of individuals. This evolving legal framework, with its different constructions, principles and enforcement mechanisms, has led to significant differences in how personal data is handled and protected. The fact that countries have different data protection and privacy laws creates a complicated and nuanced conundrum that necessitates careful consideration.

It is these circumstance that necessitate an investigation into the major differences between the Zambian and UK data protection and privacy legal framework. Despite the two countries having a shared grasp of the global imperatives related with data privacy, their distinct legislative frameworks and approaches have resulted in intriguing variances and complexity. The essence of these differences, in light of their shared global responsibilities, raises concerns about the effectiveness of their respective legal systems in securing personal data, protecting individuals' rights, and facilitating the free flow of data across borders for the advancement of economic and social interests.

This chapter establishes the groundwork for the extensive exploration that follows. It opens by outlining the research's general goals and objectives, emphasising the importance of the study in the worldwide context of data protection and privacy.

2.0 Background of Study

This paper gives background and explanation for the research, explaining the problem it seeks to answer and why it is relevant and worth investigating. It explains the aims of the research and reviews the current literature on the issue while noting the gaps or limitations associated with such work.

The problem this research seeks to resolve is the existence of inadequacies in the Data Protection Act No. 3 of 2021 in Zambia which are amplified when considered from the perspective of its counterpart in the United Kingdom.

Among the most important human rights are data security and privacy ,these are important because they safeguard a human's dignity freedom and self determination .Furthermore these rights are at the heart of the development of a digital economy and society based on trust, creativity, and inclusion. However laws around data protection and privacy are different from country to country and region to region this is because they are dependent on the unique historical, cultural, political, and legal traditions. Individuals and organisations who deal in cross-border data processing activities such as ecommerce, cloud computing, social media, and online education have challenges due to these differences, which results in shortcomings. Zambia and the United Kingdom are two countries that have enacted data protection and privacy legislation in response to the changing technology landscape and global standards. ***Zambia's Data Protection Act*** [1] (referred to as the DPA) is the principal governing statute for data privacy and protection in the country. It provides a framework for how personal data can be used and protected, regulates how personal data should be collected, used, transmitted, stored and processed, stipulates the rights that individuals have in relation to their personal data, and creates the office of the Data Protection Commissioner. The ***United Kingdom's Data Protection Act***[2] is the main piece of legislation that implements the European Union's General Data Protection Regulation (the GDPR') into domestic law. It sets out the rules for processing personal data by controllers and processors, establishes the rights of data subjects, and confers powers and duties on the Information Commissioner's Office.

Despite sharing some common objectives and principles, such as fairness, lawfulness, transparency, accuracy, security, accountability, and data minimization[1], there are notable differences between the data protection and privacy laws in Zambia and the United Kingdom. The differences are but not limited to the scope of application, conditions for consent, exemptions and derogation's, the obligations of controllers and processors, enforcement mechanisms and the cross-border data transfer rules.[2] These have significant consequences for the protection of personal data, the exercise of individual rights and the facilitation of cross-border data flows between Zambia and the United Kingdom. Therefore, it is critical to conduct a comprehensive comparative analysis in order to appreciate the nature and extent of these differences and to explore potential areas for convergence or harmonization.

3.0 Statement of The Problem

In 2021 the government of Zambia enacted the Data Protection Act[3] whose main objective is to protect provide an effective system for the collection, use, transmission, storage and otherwise processing of personal data. Despite the coming into effect of the Act, the effectiveness of its provision is one that suggests it may neither be living up to expectations nor achieving its purpose. The DPA and its provisions though binding, are not as effective as should be. This is because the Act has lacunas on the one hand, while also exhibiting and shortcomings on the other. An example of the above relates to the application of the Act outlined in Section 3 which projects the scope of what is encompassed in a regulatory manner by the piece of legislation. The provision as it currently is, raises potential right to privacy – related issues. In addition, the act states that this does not relate to the handling of personal data by an individual for personal use. However, it does not define what personal use is. This critical omission opens up the possibility of individuals processing personal data in the guise of “personal use” while putting it to other uses that undermine the data subject’s individuals’ privacy. Section 37(1) requires a licensee to apply for a license renewal in the prescribed method and form,

[1] Zambia Data Protection Act No.3 of 2021
[2] ibid
[3] Act No.3 of 2021

along with payment of a prescribed fee, at least three months before the license's expiration date. While it may be argued that any application made in defiance of the preceding article shall, by deduction, be null and void, that should, to avoid unnecessary conflicts, have been specifically given. This is essential as it may clarify whether or not the Data Protection has discretion to entertain late applications or is compelled to reject them. Section 42 of the DPA indicates that processing of personal data for research purposes shall be exempted from section 12(1)(a)(b) and (f) which require the processing to be among others - lawful, and legitimate. This suggests personal data may be processed for illegal and illegitimate research. This paper will try to address these inefficiencies and also seek to recommend solutions to them.

4.0 Research Objectives

(a) Consider the concept of data protection and its importance
(b) Identify the legal framework governing data protection in Zambia
(c) Compare the Zambian data protection legislative regime with that of the United Kingdom and draw lessons from the latter and best practice.

4.1 Research Questions

(a) What is the concept of data protection and why is it important?
(b) What legal framework governs data protection in Zambia?
(c) How does the data protection legal regime in Zambia compare with that of the United Kingdom and what lessons can Zambia draw from the latter and best practice?

5.0 Significance of The Study

This study is of significance and relevance in today's rapidly evolving technological landscape, where the safeguarding of personal data has become a paramount concern

for individuals and organizations worldwide. With the global landscape becoming more interconnected, states must strike a delicate balance between leveraging data-driven innovation and protecting individual privacy rights. Despite shared global imperatives, the disparity between Zambian and UK data protection and privacy laws raises serious concerns about the effectiveness of their respective legal frameworks in securing personal data, ensuring individual rights, and facilitating cross-border data flows, ultimately affecting economic and social progress. This study aims to shed light on these challenges and explore potential areas for convergence or harmonisation, contributing to the ongoing discussion about data protection and privacy in a digital world where personal data is becoming increasingly important.

6.0 Scope of The Study

The study's scope includes a comprehensive examination of data protection and privacy laws and practices in two specific countries, Zambia and the United Kingdom, as well as their global context. The study will look at the principles, rights, and responsibilities of data controllers and processors in each jurisdiction, as well as the practical implications of these legal frameworks for individuals, organisations, and government agencies in terms of data processing, sharing, and protection. Furthermore, the study will examine the enforcement methods and penalties in place in each nations to ensure compliance and accountability for data privacy violations.

7.0 Literature Review

In the age of rapid technological advancements and global interconnectivity, the significance of data protection and privacy has become increasingly apparent, impacting individuals, organizations, and nations.

Numerous scholars have underlined the pivotal role of data protection and privacy in the digital era such as **Mittelstadt et al.** [4] The authors**,** in their work, underscore the call for legal frameworks that strike a delicate balance between the advantages of data-driven

[4] Available at : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3662302

innovation and the safeguarding of individual privacy rights, particularly emphasizing the complications arising when disparities exist in data protection and privacy laws across various jurisdictions. Borrowing from the above, this dissertation will acknowledges the importance of legal frameworks that strike a balance between individual rights and the fostering of data driven technology in this digital age. The scope of this dissertation will, however, be limited to a comparison of data protection frameworks of Zambia and the United Kingdom.

Van der Sloot et al. and **Greenleaf**[5] undertook an important study that introduces and analyzes the European Union General Data Protection Regulation (GDPR), which is a comprehensive and influential legal framework for regulating personal data in the digital age. They explain the origins, objectives, provisions, and implications of the GDPR, as well as its differences from other privacy regimes, such as the U.S. approach.

Comparative analyses have emerged as invaluable instruments for comprehending the effectiveness of data protection and privacy laws in diverse nations. Numerous comparative studies have delved into the examination of legal frameworks across various jurisdictions. This one being conducted in this dissertation like many others, will acknowledge the strides and positives scored by the GDPR while highlighting drawbacks if any and comparing the said GDPR to the DPA in Zambia,

Another study conducted by **Christopher Kuner**[5] focused on the European Union and how it deals with data protection and privacy. It is an example of the many research papers that have consistently unveiled notable discrepancies in the principles, rights, obligations, and enforcement mechanisms concerning data controllers, processors, and subjects. Such differences emphasize the imperative need for conducting comprehensive analyses of the specific laws and practices within each country. This dissertation, in keeping with the above, seeks to highlight such shortcomings in the Zambian data privacy framework

[5] Available at : https://pure.uva.nl/ws/files/34085945/European_Union_General_Data_Protection_Regulation.pdf [5] Available at : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2162781

and differences between such framework and United Kingdom's data protection legislation. The paper will draw lessons from best practice of each.

The studies above have spent a great deal focusing on the broader issues of data protection and privacy on the global scale and the importance of having legal frameworks that balance data driven innovation with individual's rights to privacy. The studies have had a bias on major legislative instruments, such as the European Union's General Data Protection Regulation (GDPR), and narrowed down on the differences in principles, rights, obligations, and enforcement methods between jurisdictions. They shed light on the need for extensive studies of certain countries' legislation.

In contrast, this study is more streamlined and geographically focused, comparing data protection and privacy regulations in Zambia with the United Kingdom. It underlines developing difficulties in these two countries, despite similar global imperatives, and calls into question the efficiency of their legal regimes. The emphasis is on analysing the ramifications of the disparities between these two jurisdictions and investigating the possibility of convergence or harmonisation. This study focusses on a specific comparison between the two states, whereas other studies have taken a larger international approach.

8.0 Methodology

8.1 Research Approach

This research shall follow the qualitative method, allowing the researcher to acquire information through various sources such as articles, books and statutory provisions. This research methodology will be evaluative. As such, it will assess the **Data Protection Act** critically, comparing it to its counterpart in the United Kingdom.

8.2 Research Type

The research will be conducted using the analytical research type by which relevant provisions of legislation will be critically analyzed and compared.

8.3 Research Design

The research design adopted for this dissertation is descriptive and evaluative.

8.4 Data Collection Techniques

This study will focus on collecting primary data through qualitative interviews, of which will be physical or telephone. With the Secondary data, data will be collected through legislation, textbooks, journal articles, research papers, published legal reports, various electronic sources and academic papers.

8.5 Study Population

The study population of this research will be person's knowledge, expertise and experience in the subject matter.

8.6 Data Analysis

All the data which has been collected from primary and secondary, will be analysed qualitatively involving interviews and assembling the data into themes and patterns using content analysis and thematic methods of analysis.

8.7 Sampling Size

This study will include 10 people selected from the population of which will include key stakeholders in the Zambian ICT sector, ICT industry professional and legal experts with the law governing data privacy and the ICT sector in Zambia.

8.8 Sampling Techniques

This study subject will be sampled using purposive sampling technique, so as to make the study even more practical while still targeting people and workplaces that will help in delivering reliable results with regards to the study.

8.9 Ethical Considerations

Ethical considerations are held in very high esteem and considered paramount in this study. To maintain the highest ethical standards, the researcher will consistently and accurately attribute all sources of information incorporated into this study, adhering to well established citation conventions. Additionally, any individual involved in the research will be approached for their informed consent. The researcher will be dedicated to maintaining impartiality, transparency, and precision at all stages of the research, ensuring the trustworthiness and dependability of the findings. The researcher will also abide by rules applicable to research as laid out by the University of Lusaka.

These proactive measures will preserve the integrity of the research process and reduce the possibility of ethical dilemmas arising.

CHAPTER TWO

THE CONCEPT OF DATA PROTECTION AND ITS IMPORTANCE

2.1 Introduction

The current studies have had a bias towards data protection and privacy on a global scale they have shown how important it is to have a balance between data driven innovation and the need to safe guard the privacy rights of individuals .

They focus more on examining significant legislative instruments, such as the European Union's General Data Protection Regulation (GDPR), and highlight disparities in concepts, rights, obligations, and enforcement techniques among jurisdictions.They highlighted the importance of conducting in-depth research on certain countries' regulations. This chapter strives to help the reader understand what data protection is ,how it has evolved and the key concepts and rights, it further explains why it matters to individuals, institutions and governments. The Chapter will make use of a number of international instruments such as the GDPR, Convention 108/108+, OECD Guidelines, regional norms such as the AU and SADC, and chosen comparative legislation to ground definitions and standards in authoritative sources.

2.2 Conceptual Foundations and Definitions

The concept of **data protection** can best be understood as a comprehensive system of legal norms, institutional structures, and technical-organizational safeguards designed to regulate the processing of personal data across its entire lifecycle.[6] This lifecycle spans the moment data are first collected, through their use, storage, and potential disclosure, to their eventual erasure or destruction.[7] While data protection is often discussed

[6] L A Bygrave, 'Data Protection Law: Approaching Its Rationale, Logic, and Limits' (Kluwer Law International 2002).
[7] L A Bygrave, 'Data Protection Law: Approaching Its Rationale, Logic, and Limits' (Kluwer Law International 2002).

alongside **cybersecurity**, the two are conceptually distinct yet mutually reinforcing. **Cybersecurity** focuses on defending systems and information from compromise, whereas **data protection** governs whether, how, and why personal data may be processed at all, embedding in that process both enforceable rights and accountability obligations.[8]

In Zambia , to fully understand the scope of the data protection it is key to focus on the core terminologies as defined in Section 2 of the **Data Protection Act[9]**:

Personal data this is data that looks at an individual who is directly or indirectly identified from that data. This date would include the name, identification number, location, an online identifier. It can also include factors that are specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.[10]

This definition is deliberately broad, capturing the full range of information that, alone or combined, can single out an individual.

Processing encompasses virtually any operation performed on personal data. This includes activities such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, alignment or combination, restriction, erasure, and destruction.[11]

Under section 2 of **Data Protection Act[12]**, **"sensitive personal data"** is defined as personal data which, owing to its nature, may be used to suppress the data subject's fundamental rights and freedoms. The Act explicitly includes the following categories:

(a) the race, marital status, ethnic origin, or sex of a data subject.

(b) genetic data and biometric data;

(c) child abuse data;

---

[8] European Union Agency for Cybersecurity (ENISA), Privacy and Data Protection by Design – from Policy to Engineering (ENISA 2015) 9–10.

[9] Act No. 3 of 2021

[10] ibid

[11] ibid

[12] Act No. 3 of 2021

(d) data subject's political opinions;
(e) a data subject's religious beliefs or other beliefs of a similar nature;
(f) trade union membership; and
(g) a data subject's physical or mental health, or physical or mental condition.
This statutory definition aligns with international standards such as Article 9 of the GDPR and Article 6 of Convention 108+, reinforcing the principle that sensitive data must be subject to stricter processing conditions, enhanced safeguards, and explicit legal bases to ensure the protection of vulnerable individuals and groups. Processing of such data is typically prohibited unless strict conditions are met.

Controller and **processor** describe the principal actors in data governance. The controller is the natural or legal person, public authority, agency, or other body which determines the purposes for which and means by which personal data are processed.[13] The processor, by contrast, processes data solely on behalf of the controller, acting within the framework of a contractual or statutory mandate. These roles are central to allocating responsibility and ensuring that compliance duties are met.

Viewed in this light, data protection operates as the practical mechanism through which constitutional and international privacy guarantee such as those enshrined in Article 12 of the **Universal Declaration of Human Rights** and Article 17 of the **International Covenant on Civil and Political Rights** are translated from abstract commitments into concrete, enforceable standards, procedures, and remedies. In other words, it is the bridge between the normative promise of privacy and its day-to-day realization in law, policy, and institutional practice.

[13] O Belleflamme, 'Roles and Responsibilities of Data Controllers and Data Processors ' (Academy of European Law, 20 June 2023) Available at : https://yela.era.int/wp-content/uploads/sites/52/2023/07/Roles-and-responsibilities-of-data-controllers-and-data-processors-O.-Belleflamme-ERA-20.06.23.pdf.

2.3 Historical Evolution and International Frameworks

The data protection legal framework began to emerge somewhere around the 1970s,when societies were faced with the rapid proliferation of computerised systems and the emergence of state-held databases. In Germany, early initiatives such as the Hesse and Bavarian data laws culminated in the Federal Data Protection Act of 1977, which was one of the first comprehensive national regulations of its kind.[14] These activities were motivated by concerns about monitoring, profiling, and the uncontrolled collection of personal information by both governmental and private institutions.

At the international level, three foundational instruments established the framework for modern data protection regimes. The **OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,** adopted in 1980 and revised in 2013, introduced the Fair Information Practice Principles (FIPPs) collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability.[15] These principles remain central to global privacy frameworks and were designed to reconcile the protection of privacy with the facilitation of international trade and digital services. In parallel, the Council of Europe adopted **Convention 108 in 1981[16]**, the first binding international treaty on data protection, which required member states to establish supervisory authorities and laid down core principles for lawful processing. Its modernized version, **Convention 108+**, adopted in 2018, updated the treaty to address new risks such as algorithmic profiling and cross-border surveillance, strengthened enforcement mechanisms, and embedded accountability as well as privacy by design and by default.[17] The European Union came up with Directive

---

[14] S Carr, 'The Origins of Data Protection Law: The German Experience '(2017) 33(1) *Computer Law & Security Review* 1, 3–5.

[15] Organisation for Economic Co-operation and Development, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (OECD Publishing 2013) <https://doi.org/10.1787/9789264196391-en>

[16] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (opened for signature 28 January 1981, entered into force 1 October 1985) ETS No 108

[17] Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (adopted 18 May 2018, opened for signature 25 June 2018) CETS No 223.

95/46/EC, which had the objective of having a uniform set of regulations among member states, this also laid the groundwork for a unified internal market in personal data. This was later on replaced by the General Data Protection Regulation (GDPR) of 2018, which established a directly applicable, risk-based, and extraterritorial framework. The GDPR was very progressive because it came up with a formalised comprehensive set of data subject rights, it also imposed stringent requirements on controllers and processors, and introduced substantial penalties for any one who was found in breach.The scope and enforcement have facilitated global convergence on DPR-style legislation.[18]

In Africa regional instruments have played a very siginficant role in influencing national reforms .

The **African Union Convention on Cyber Security and Personal Data Protection**, was adopted in Malabo in 2014,it provides a continental framework that encourages member states to have a similar set of standards in terms of protecting personal data, building digital trust and enhancing cross-border cooperation.The **SADC Model Law on Data Protection of 2013** offers a legislative template for states in Southern African it addresses data subject rights, lawful processing, supervisory authorities, and international transfers. It has directly inspired national enactments in Kenya through the Data Protection Act of 2019, in South Africa with the Protection of Personal Information Act of 2013 and in Zambia through the Data Protection Act of 2021.

2.4 Core Principles and Lawful Bases

Modern data protection statutes increasingly converge on a core set of principles that constrain and guide the lawful processing of personal data. The **General Data Protection Regulation (GDPR)** offers the most influential articulation of these principles and its framework has been widely adopted or echoed across African jurisdictions, including

[18] 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) [2016] OJ L119/1.

Zambia's **Data Protection Act**.[19] These principles begin with lawfulness, fairness and transparency requiring that processing rest on a valid legal basis, be contextually fair and be clearly communicated to data subjects through accessible notices.[20]Purpose limitation mandates that data be collected only for specified, explicit, and legitimate purposes, with any secondary use strictly limited to compatible objectives.[21] Data minimization ensures that only data which is adequate, relevant, and necessary for the stated purpose is processed, while the principle of accuracy obliges controllers to keep data up to date and rectify inaccuracies promptly.[13] Storage limitation restricts retention to the duration necessary for the original purpose, often requiring defined retention schedules.[22]Integrity and confidentiality demand robust technical and organizational safeguards against unauthorized access, accidental loss, or damage. Accountability places the burden of demonstrable compliance on controllers, who must maintain policies, records, conduct data protection impact assessments (DPIAs), and undergo audits.[23]

Lawful bases for processing typically include consent, performance of a contract, compliance with legal obligations, protection of vital interests, tasks carried out in the public interest or under official authority and legitimate interests provided these do not override the rights of data subjects.[24]

Processing sensitive data is subject to tougher criteria, which frequently require express consent, significant public interest, preservation of essential interests in cases where consent is not possible, public health imperatives, or research done with sufficient protections. These concepts are operationalised through methods such as privacy by design and default, mandated Data Protection Impact Assessment for high-risk

---

[19] Act No.3 of 2021
[20] 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 (General Data Protection Regulation) [2016] OJ L119/1, art 5(1)(a)–(f), art 5(2), arts 6, 24–25, 30, 35.
[21] ibid
[22]ibid
[23] ibid
[24] Articles 6 and 9 of the GDPR,

processing, and security-by-design approaches, which incorporate compliance into data system architecture.[25]

2.5 Data subject rights

Rights translate ideas into individual power, allowing people to see, rectify, limit, contest, and remove data about themselves, as well as seek remedies. These rights are codified in Chapter III of the General Data Protection Regulation (GDPR), notably Articles 12–21. They form the backbone of individual empowerment under EU data protection law and are paralleled in many national systems, including Zambia's **Data Protection Act**[26] and these are:

Right to be informed : includes clear, accessible notices identifying the controller, purposes, legal bases, recipients, retention, rights, and transfer procedures.

Right of access: Confirmation of data processing and access to the data and critical information.

Right to Rectification: Correction of inaccurate or incomplete data.

Right to Erasure: Deletion where data are no longer necessary, consent is withdrawn, processing is unlawful, or legal obligations require it subject to exceptions.

Right to Restriction of Processing: Temporary freeze pending verification, objection determination, or where processing is unlawful and erasure is not sought.

---

[25] 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 (General Data Protection Regulation) [2016] OJ L119/1, arts 9(2)(a)–(j), 25, 32, 35.

[26] Act No.3 of 2021

Right to Data Portability: Receive personal data in a structured, commonly used, machine-readable format and transmit to another controller where processing is based on consent/contract and by automated means.

Right to Object: Object to processing based on public interest/legitimate interests and to direct marketing at any time.

Rights in relation to automated decision-making: Safeguards against decisions producing legal or similarly significant effects based solely on automated processing, including profiling with narrow exceptions.

Effective rights require enforceable timelines, minimal fees, identity verification proportionate to risk, and accessible complaint and judicial avenues.

2.6 Controllers, Processors, Accountability and Security

To ensure lawful and accountable data processing, controllers must incorporate data protection into their organisational governance structures and procurement policies, while processors must implement adequate measures and closely adhere to the controller's recorded instructions. **Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016,** on the protection of natural persons with regard to the processing of personal data and the free movement of such data **(General Data Protection Regulation)**[27] . Effective governance entails keeping detailed records of processing activities, appointing a Data Protection Officer (DPO) where required, implementing internal policies and staff training programs, supervising third-party vendors, and conducting **Data Protection Impact Assessments (DPIAs)** for high-risk operations.[28] Contracts between controllers and processors must explicitly state the subject matter, duration, nature, and purpose of processing, types of personal data concerned, data subject categories, applicable security measures, subprocessing criteria

[27] [2016] OJ L119/1 (GDPR), articles 5, 24-32.
[28] GDPR, art 30 (record-keeping); art 37 (Data Protection Officer); arts 35–36 (DPIAs).

and audit rights.[29] Security in processing must be appropriate to the risk, encompassing techniques such as pseudonymization, encryption, system resilience, regular backups, and testing methods, sometimes governed by sectoral standards like **ISO/IEC 27001**.[30]

In the event of a personal data breach, controllers are obligated to notify the supervisory authority without undue delay and to inform affected data subjects where the breach poses a high risk to their rights and freedoms, unless effective mitigations such as strong encryption are in place.[31] Cross-border data transfers are permitted only where adequate protection is ensured, typically through mechanisms such as adequacy decisions.
In the event of a personal data breach, controllers are required to notify the supervisory authority without undue delay, and in many jurisdictions, within a specified statutory timeframe. Where the breach presents a high risk to data subjects 'rights and freedoms, affected individuals must also be informed, unless effective mitigations such as strong encryption render the risk negligible. Cross-border data transfers are permissible only where the receiving jurisdiction ensures an adequate level of protection. This principle of adequacy was rigorously examined in two landmark decisions by the Court of Justice of the European Unions namely, ***Schrems I*** invalidated the Safe Harbor framework on the grounds that US surveillance practices lacked sufficient safeguards and redress mechanisms for EU citizens, while ***Schrems II*** struck down the Privacy Shield and clarified that adequacy must be both **substantive** offering protections equivalent to those under EU law and **enforceable**, meaning that data subjects must have access to effective legal remedies in the recipient country.[32] These rulings underscore that adequacy cannot be merely formal or aspirational; it must be real and judicially defensible.

---

[29] GDPR, art 28(3) (controller–processor contracts).
[30] GDPR, art 32 (security of processing); see also International Organization for Standardization, ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection – Information Security Management Systems – Requirements (ISO, 2022).
[31] GDPR, arts 33–34 (breach notification).
[32] Case C-362/14 Schrems v Data Protection Commissioner [2015] ECLI:EU:C:2015:650 (Schrems I); Case C-311/18 Data Protection Commissioner v Facebook Ireland Ltd and Schrems [2020] ECLI:EU:C:2020:559 (Schrems II).

2.7 Why Data Protection Matters

2.7.1 Human Dignity, Autonomy, and Equality

Privacy is universally recognized as a fundamental human right, enshrined in key international instruments such as Article 12 of the ***Universal Declaration of Human Rights*** and Article 17 of the ***International Covenant on Civil and Political Rights*****.** Data protection serves as the operational mechanism through which this right is realized in practice, extending its reach into related freedoms including expression, association, religion, and protection against discrimination. In contemporary contexts such as algorithmic profiling, biometric identification systems, and data-driven welfare or credit scoring, robust safeguards are essential to prevent arbitrary or disproportionate interference with individual rights and to mitigate the risk of structural bias.

2.8 Conclusion

This chapter has shown that data protection is a cornerstone of modern governance, human rights, and digital trust. From its roots in the 1970s to global instruments such as the OECD Guidelines, Convention 108/108+, and the GDPR, data protection has evolved into a proactive framework balancing innovation with accountability. Its core principles and rights empower undivided **Data Protection Act**[33] is expected to reflect this global trajectory, embedding rights, principles, and enforcement mechanisms into national law.

[33] Act No. 3 of 2021

CHAPTER THREE

DATA PRIVACY LEGAL FRAMEWORKS IN ZAMBIA AND THE UNITED KINGDOM

3.0 Introduction

Data protection is a fundamental human right that is increasingly challenged by the rapid development of emerging Information Communication Technologies. Different countries have adopted different legal frameworks to regulate the collection, use, transmission, storage, and otherwise processing of personal data, as well as protect the rights and interests of data subjects, data controllers, and data processors. This essay will examine and compare the data protection and privacy laws in Zambia and the United Kingdom, two countries with different historical, political, and economic backgrounds, but also with some commonalities and influences. This chapter will outline legal frameworks on Data Protection in the two countries. This will create a foundation upon which a comparative analysis of the data protection legal frameworks in the two countries may be conducted. This comparative analysis will be conducted in the chapter following this one.

3.1 Data Protection Legal Framework in Zambia

3.1.1 Data Protection Act

The main piece of legislation governing data protection and privacy in Zambia is the **Data Protection Act**[34]. This Act seeks to provide a system for the use and protection of

[34] Act No.3 of 2021

personal data and regulate the collection, use, transmission, storage and otherwise processing of the said data. It establishes the Office of the Data Protection Commissioner and provides for its functions, registration of data controllers, licensing of data auditors as well as duties of data controllers and data processors. The Act also provides for the rights of data subjects as well as for matters connected with, or incidental to, all of the foregoing.[35]

The primary goals of this Act revolve around safeguarding the privacy of individuals as they relate to their personal data, aiming to simultaneously establish a robust framework that ensures the free and secure flow of such information. Another key objective is to enforce compliance with international standards and best practices on data protection and privacy. Additionally, the Act seeks to cultivate public trust and confidence in the utilization of personal data, emphasizing the importance of responsible and ethical handling of such sensitive information.

The fundamental provisions laid out in this Act include definition of key terms crucial for understanding the scope and perspective in which they are used. Part I of the Act contains preliminary provisions, and this is where definitions and the scope of application of the Act fall. **Personal data** is defined as any data which relates to an individual who can be directly or indirectly identified from that data which includes a name, an identification number, location data, an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.[36] **Sensitive personal data** goes further to encompass personal data which by its nature may be used to suppress the data subject's fundamental rights and freedoms. Such data includes race, marital status, ethnic origin or sex, genetic data, biometric data, child abuse data, political opinions, religious or other such beliefs, membership of a trade union, physical health, physical condition, mental health and mental condition.[37] A **data subject** is defined as a natural person to whom personal data relates while **data**

[35] Preamble of The Data Protection Act
[36] Section 2 of The Data Protection Act
[37] ibid

controller is a person who, either independently or in collaboration with others, determines the purposes and means of processing personal data.

Meanwhile, a data processor is a person or entity engaged in processing personal data on behalf of a data controller. Additionally, the Act introduces a data auditor and outlines the role of such auditor. A **data auditor** is a licensed person responsible for conducting audits on the processing of personal data by both data controllers and data processors. The term **processing** is defined broadly to encompass various operations performed on personal data, whether automated or not, including collection, recording, organization, storage, retrieval, consultation, use, disclosure, alignment, combination, restriction, erasure, or destruction.[38]

The Act applies to different types of personal data, data subjects, data controllers and data processors as follows**:**

The Act applies to the processing of personal data by automated means as well as by means that are not automated.[39] It, however, does not apply to the processing of personal data by a natural person for their personal use.

Part II establishes the office of the Data Protection Commissioner and lays out its functions, while **Part III** provides for the inspectorate and its powers. **Part IV** outlines principles and rules relating to processing personal data and **Part V** deals with regulation of data controllers and data auditors. **Part VI** has provisions relating to data auditors while provisions under **Part VII** relate to exemptions from principles earlier outlined in **Part IV.** Duties of data controller and data processor are contained in **Part VIII**, rights of the data subject in **Part IX**, transfer of personal data outside the republic in **Part X** and general provisions in **Part XI.**

[38] ibid
[39] Section 3 of The Data Protection Act

3.1.2 Electronic Communications and Transactions Act 2021

The **Electronic Communications and Transactions Act[40] 2021** is a piece of legislation that was enacted to provide a safe and effective environment for electronic transactions.

The Act aims to achieve multiple objectives, including the promotion of secure electronic signatures and the facilitation of electronic document filing by public authorities. It further addresses the use, security, facilitation, and regulation of electronic communications and transactions, fostering legal certainty, confidence, as well as encouraging investment and innovation in this domain. The Act also contains provisions regulating the National Public Key Infrastructure. The Act signifies a substantial legislative update by repealing and replacing the Electronic Communications and Transactions Act of 2009, reflecting the ever rapidly evolving landscape of electronic transactions and communications.[41]

The Act addresses a spectrum of data types, encompassing:

Data messages: data generated, sent, received or stored by electronic, optical or similar means including emails, texts, images, videos, and similar forms of electronic communication.

Digital signatures: an electronic signature consisting of a transformation of an electronic record using an asymmetric cryptosystem and a hash function such that a person having the initial untransformed electronic record and the signer's public key can accurately determine whether the -

(a) transformation was created using the private key that corresponds to the signer's public key; and

(b) initial electronic record has been altered since the transformation was made.

Timestamps: a data unit created using a system of technical and organizational means which certifies the existence of electronic data at a given time.

[40] Act no.4 of 2021
[41] Preamble of The Electronic Communications and Transactions Act

The **ECT Act** also has provisions relating to rules pertaining to the expression in electronic format of requirements in law as they relate to electronic data. The National Public Key Infrastructure is provided for in **Part IV** of the Act. This is a government - deployed virtual infrastructure whose root certification authority is established as the highest-level certification authority of Zambia and is managed by ZICTA. The National Public Key Infrastructure forms the basis upon which a safe and effective environment for electronic transactions, secure electronic signatures and legal certainty - at least in the public sector – may be achieved.

Part VIII of the Act provides for online consumer protection – outlining measures aimed at ensuring protection to such consumers including among others, compelling online service providers to use a safe and secure payment system, according to online consumers the right to return goods or cancel a contract for services for no reason without incurring liability. **Section 82** falling under **Part X** empowers a recipient of a service or any person whose rights have been affected to order a service provider to take-down content or activity infringing the rights of the recipient or of a third party or which is otherwise unlawful. The service provider in receipt of a take-down notification is obligated to take down the complaint about content as soon as practicable.

Part XI of the Act providing encryption among others prohibits the unauthorized decryption or release of a decryption key. **Part XII,** on the other hand, provides for general provisions including appeals, offences by corporate or un-incorporate bodies corporate and admissibility of illegally obtained evidence in criminal proceedings.

3.1.3 Cyber Security Act No. 3 of 2025

The Cyber Security Act was enacted to, provide for cyber security in the Republic; establish the Zambia Cyber Security Agency and provide for its functions; provide for the regulation of cyber security service providers; provide for the constitution of the Zambia Cyber Incident Response Team and provide for its functions; provide for the constitution of sectoral cyber incident response teams; continue the existence of the Central Monitoring and Co-ordination Centre; provide for the designation, protection and

registration of critical information and critical information infrastructure; repeal and replace the Cyber Security and Cyber Crimes Act, 2021; and provide for matters connected with, or incidental to, the foregoing.

The Act, in section 2 - its Interpretation Clause attaches different interpretations to various terms and phrases including the following:

“Critical Information” means computer data that relates to public safety, public health, economic stability, national security, international stability and the sustainability and restoration of critical cyberspace including -

(a) personal data that is managed, stored or transmitted through critical information infrastructure or processed by a controller;

(b) information relating to any research and development in relation to critical information infrastructure;

(c) information needed to operate critical information infrastructure; or

(d) information relating to risk management and business continuity in relation to critical information infrastructure;

“Critical Information Infrastructure” means a computer system, device, network, computer program or computer data that -

(a) is vital to a country such that the incapacity or destruction of, or interference with, the computer system, device, network, computer program or computer data would have a debilitating impact on national security, economy, public health or safety; or

(b) supports the processing of critical information or an essential service;

The Act, in section 3, establishes the Zambia Cyber Security Agency (“the ZCSA” or “the Agency”) in the Office of the President which is responsible for the administration of this Act under the general direction of the President. The Agency is the body tasked with spearheading the fostering of cyber security in Zambia.

The functions of the Agency, outlined in section 4 of the CSA, are to -

(a) subject to the Zambia Security Intelligence Service Act, 1998, coordinate activities relating to cyber security and cyber resilience;

(b) take measures in response to cyber security incidents which may threaten critical information, critical information infrastructure or any information or infrastructure in the Republic likely to be affected by a cyber security incident;

(c) disseminate information on cyber threats and vulnerabilities;

(d) identify and ensure the protection of critical information and critical information infrastructure;

(e) establish codes of practice and standards for cyber security and monitor compliance with the codes of practice and standards by controllers;

(f) issue licenses for the provision of cyber security services;

(g) regulate the conduct of cyber security service providers;

(h) promote and undertake research and development relating to cyber security;

(i) promote and undertake capacity building, education and awareness activities on matters relating to cyber security;

(j) undertake information security audits on critical information and critical information infrastructure;

(k) adopt standards for cyber security products and services and certify cyber security products and services;

(l) develop and implement a national cyber security response plan;

(m) undertake digital forensics;

(n) provide technical assistance and collaborate with other relevant national and international institutions in matters relating to this Act; and

(o) advise the President on matters relating to cyber security.

The CSA provides for the constitution of another body that plays a critical role in cyber security - the Cyber Incident Response Team. Section 6(1) compels the Agency to constitute the Zambia Cyber Incident Response Team which shall -

(a) be the first point of contact with reference to the handling of cyber incidents and communication between local, regional and international cyber security incident response teams;

(b) provide incident response and management services in a coordinated manner through established industry standard policies and procedures to manage threats associated with cyber incidents;

(c) provide alerts and warnings on the latest cyber threats and vulnerabilities which may impact the public and the private sector;

(d) undertake national cyber security risk assessments;

(e) assess and coordinate the work of sectoral cyber incident response teams within the public and private sector.

3.1.4 The Cyber Crimes Act No. 4 of 2025

The Cyber Crimes Act No. 4 of 2025 (the CCA) was enacted to provide for offences relating to computers and computer systems; provide for the protection of persons against cyber crimes; provide for child online protection; and provide for matters connected with, or incidental to, the foregoing.

The Act outlines and provides or a whole list of offences including unauthorized access to computer system and data in section 3, unauthorized interference with computer system and data in section 4, prohibition of unauthorized disclosure of data relating to Critical Information or Critical Information Infrastructure in section 5 and unauthorized possession of data relating to Critical Information or Critical Information Infrastructure in section 6.

Section 7 prohibits the illegal acquisition of data while section 8 prohibits the introduction of malicious software into a computer system and section, illegal system interference.

Prohibition of recording of private conversation without prior notice is provided for in section 10, while section 12 prohibits computer related misrepresentation and computer fraud.

3.1.5 The Information and Communications and Technologies Act

The Information and Communications Technologies Act 2009 is a law enacted by the Parliament of Zambia to regulate the information and communication technology (ICT) industry in the country.

The Act sets forth its primary objectives with a comprehensive vision, transforming the existing Communications Authority, the ICT Sector regulator into the Zambia Information and Communications Technology Authority (ZICTA). It delineates what is aimed to be a robust regulatory framework for the Information Communication Technology sector, covering crucial aspects such as licensing, fees, access, numbering, and type approval. A key focus is placed on facilitating widespread access to information and communication technologies, particularly in rural, unserved and underserved areas, aligning with broader inclusivity goals. The legislation prioritizes safeguarding the rights and interests of both service providers and consumers, emphasizing aspects like privacy, service quality, and fair competition. Furthermore, the Act strategically repeals the outdated Telecommunications Act, 1994, and the Radiocommunications Act, 1994, recognizing their inconsistency with the present ICT landscape, thus paving the way for a more contemporary and adaptive regulatory framework.[42]

The Act handles a wide range of ICT-related issues, including service provider licensing, radio frequency allocation, and spectrum management, all of which are critical parts of telecommunications. It also expands its scope to include the provision and use of electronic communication services and networks, emphasising the importance of competent regulation in this dynamic environment. Furthermore, the Act investigates data related to the registration and identification of SIM cards and devices, underlining the necessity of safe and responsible mobile communication activities. It also addresses

[42] Preamble of The Information and Communications and Technologies Act

data relating to the monitoring and enforcement of ICT standards and rules, ensuring adherence to set benchmarks. Finally, for our purposes, the Act addresses data related to the collection and administration of ICT levies and taxes, demonstrating its comprehensive approach to governance and fiscal issues in the Information and Communication Technology sector.

3.2 Data Protection Legislation in the United Kingdom

The United Kingdom (UK) is a sovereign state located in Western Europe, consisting of four countries: England, Scotland, Wales and Northern Ireland. The UK was a member of the European Union (EU), but decided to leave the bloc following a referendum in 2016.[43] The UK is a member of the Commonwealth of Nations, the United Nations, NATO, the G7 and the G20.

3.2.1 The Data Protection Act of 2018

The Data Protection Act (DPA) is the UK's main legislation that regulates the processing of personal data, which is any information relating to an identified or identifiable individual.[44] The DPA implements the EU General Data Protection Regulation (GDPR), which is a comprehensive and harmonized data protection framework for the EU. The DPA also covers areas that are not fully covered by the scope of the GDPR, such as law enforcement, national security, immigration and intelligence services.

The DPA aims to protect the rights and freedoms of individuals in relation to their personal data, while also enabling the lawful and effective use of data for various purposes. The DPA sets out principles that data controllers and processors must follow when handling personal data, such as lawfulness fairness and transparency; purpose limitation; data

[43] Frere, Sheppard Sunderland, et al. "United Kingdom." Encyclopedia Britannica, 14 Jan. 2024, https://www.britannica.com/place/United-Kingdom. Accessed 15 January 2024

[44] Section 3 Data Protection Act 2018 - Legislation.gov.uk. https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted.

minimization; accuracy; storage limitation integrity and confidentiality (security); as well as accountability.

The DPA also grants individuals a number of rights over their personal data, such as the right to access, rectification, erasure, restriction, porting data as well as the right to object to the processing of their data.[45] The DPA, in the same part, imposes obligations on data controllers and processors to ensure the compliance with the data protection rules. These include conducting data protection impact assessments, appointing data protection officers, reporting data breaches and cooperating with the supervisory authorities.

The DPA is enforced by the Information Commissioner's Office (ICO), which is the UK's independent data protection authority. The ICO has the power to issue guidance, codes of practice, certification schemes, fines, orders and sanctions for data protection violations. The ICO also handles complaints from individuals and co - operates with other data protection authorities in the EU and beyond.[46]

The DPA is a complex and evolving piece of legislation that reflects the challenges and opportunities of the digital age. The DPA aims to balance the protection of personal data with the promotion of innovation, economic growth, public safety and social welfare.

3.2.2 The Computer Misuse Act 1990

The Computer Misuse Act 1990 (CMA) in the United Kingdom, regulates the access and use of electronic data, computers and computer networks. Cardinal to note is the fact that this pieces of legislation by implication, seeks to safeguard information – some of which is personal information from illegal access, modification, deletion, transfer and exposure. The CMA criminalizes among others by interfering with a computer or data thereon, hacking - which is illegal access, as well as access to computer data with intent of committing a further crime. Introducing malware into a computer is also prohibited.

---

[45] Chapter 3, Section 3 Data Protection Act 2018 - Legislation.gov.uk. https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

[46] Schedule 12 Data Protection Act 2018 - Legislation.gov.uk. https://www.legislation.gov.uk/ukpga/2018/12/contents/data.pdf.

3.2.3 Telecommunications (Security) Act 2021 (TSA)

This piece of legislation amended the Communications Act 2003. It, amends section 105 of the Communications Act 2003 by among others, providing for an obligation to service providers to take security measures mitigating to mitigate risk of security compromises[47] defined as anything that compromises the availability, performance, functionality or confidentiality of the network, allows unauthorized access or interference, or causes signals or data to be lost or altered without the provider's permission.[48] The Act compels service providers to take appropriate measures to identify and reduce risks of security compromises as well as put measures in place to counter future security compromises.[49]

The Act places upon service providers the burden of taking reasonable and appropriate steps to notify users of risks of security compromises. It is a requirement that service provides bring to the attention of users, measures taken to mitigate or remedy the above. Service providers are mandated to report security compromises with significant effect on the operations of the network to Ofcom, the regulator.[50]

3.3 Conclusion

This chapter introduced and considered the specific data protection legislation in Zambia and the UK, together with those forming the greater legal framework supporting the said specific data protection legislation.

The following chapter will undertake a comprehensive comparative analysis of the legal frameworks in Zambia and the United Kingdom as they relate to data protection and privacy.

---

[47] 105 Communications Act 2003 as amended by the TSA
[48] Ibid
[49] Ibid
[50] Ibid

CHAPTER FOUR

COMPARATIVE ANALYSIS OF DATA PROTECTION LEGAL REGIMES IN ZAMBIA AND THE UNITED KINGDOM

4.0 Introduction

This chapter aims at providing a comparative analysis of the Zambian and United Kingdom data protection legal frameworks. It builds upon the descriptive overview in the previous chapter and highlights the similarities, differences and practical implications in the regulation of personal data and privacy. The analysis also draws on best practices in the United Kingdom, a jurisdiction with a more mature data protection regime, and considers what lessons Zambia can learn to strengthen its framework for effective data subject protection while encouraging innovation and trust in the digital economy.

Data protection law regimes reflect philosophical commitments to privacy, autonomy, and accountability. A comparative research is crucial because Zambia's legislative framework in this area is very young, having been adopted in 2021, but the United Kingdom has decades of institutional experience under consecutive data protection legislation dating back to the **1984 Data Protection Act**. The comparison allows for the identification of strengths and faults in Zambia's evolving framework.

4.1 Conceptual and Philosophical Foundations of Data Protection

The United Kingdom's data protection policy is strongly based on the idea that personal data protection is a basic right. This fundamental viewpoint is consistent with Article 8 of the European Convention on Human Rights (ECHR), which ensures the right to respect for private and family life, home, and communication. UK courts have consistently interpreted data protection statutes, specifically the Data Protection Act 2018 and its precursor legislation, through a rights-based lens, thus supporting the constitutional character of informational privacy within the domestic legal order.[51]

This interpretive approach has been shaped not only by domestic jurisprudence but also by influential decisions from the **Court of Justice of the European Union (CJEU)** prior to Brexit. A very important case in this regard is **Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González** [52] decided in May 2014.

In this case, the CJEU was asked to determine whether an individual could compel a search engine operator to remove links to web pages containing outdated or prejudicial personal information, even if the original publication was lawful and accurate.

The facts involved **Mario Costeja González**, a Spanish citizen who objected to Google indexing links to a 1998 newspaper notice about a property auction related to his past social security debts. He argued that the continued availability of this information via Google's search results infringed his data protection rights under **Directive 95/46/EC**, the precursor to the **General Data Protection Regulation (GDPR)**. The Spanish Data Protection Authority (AEPD) conceded and the matter was referred to the CJEU for a preliminary ruling.

The Court held that search engine operators are **data controllers** when they process personal data by indexing and displaying search results. All in all, the CJEU recognized that individuals have the right under certain conditions to request the **de-indexing of links**

---

[51] European Convention on Human Rights (adopted 4 November 1950, entered into force 3 September 1953) ETS No 5, art 8; Data Protection Act 2018 (UK); *R (Bridges) v Chief Constable of South Wales Police* [2020] EWCA Civ 1058, [2020] 1 WLR 5027.

[52] Case C-131/12

to personal data that is **inadequate, irrelevant, no longer relevant, or excessive** in relation to the purposes for which it was originally processed. This decision established the so-called "right to be forgotten," which is now enshrined in the General Data Protection Regulation (GDPR), and represented a substantial expansion of data subject rights in the digital age.

Although the UK formally exited the European Union in 2020, the Google Spain case remains persuasive. The UK's post-Brexit data protection policy, while now governed by the UK GDPR, retains many of the key ideas of EU data protection law, such as balancing privacy rights with freedom of expression and the public interest. UK courts continue to look to CJEU jurisprudence for interpretive assistance, particularly in issues involving digital erasure, search engine liability, and the proportionality of data retention.[53]

Zambia's **Data Protection Act**[54] while a commendable step toward modernizing the country's digital governance architecture, remains primarily framed within a **regulatory and compliance-oriented paradigm**. The Act establishes mechanisms for lawful data processing, consent, data subject rights, and oversight through the Office of the Data Protection Commissioner.[55] However, its normative foundation is largely administrative, lacking the deeper constitutional protection that characterizes rights-based data protection regimes.

Although **Article 17 of the Zambian Constitution** guarantees the right to privacy, this provision has not yet been judicially interpreted to encompass a **substantive right to data protection**. The absence of jurisprudential development in this area means that informational privacy is treated more as a statutory entitlement than a constitutional guarantee. Consequently, the Zambian data protection legal framework remains susceptible to **executive discretion and administrative override** in areas involving

---

[53] Information Commissioner's Office, 'Guide to the UK GDPR '(ICO, 2021) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-uk-gdpr accessed 26 August 2025

[54] Act No. 3 of 2021

[55] ibid (Preamble)

national security, surveillance, or public interest exemptions - areas where judicial scrutiny is most needed.

In contrast, the **United Kingdom's data protection framework** even post-Brexit continues to reflect a **rights-based orientation**, deeply influenced by **Article 8 of the European Convention on Human Rights (ECHR)** and landmark decisions such as ***Google Spain SL v Agencia Española de Protección de Datos*** *(2014)* these affirm that data protection is not merely a matter of compliance but a **fundamental right** deserving of robust judicial protection.

A key lesson Zambia can draw from the UK experience is the **strategic importance of embedding data protection within a constitutional or quasi-constitutional framework** doing this would elevate the normative status of privacy, ensuring that individuals are protected not only by statutory mechanisms but by **constitutional safeguards** that demand proportionality, necessity and legality in any interference. This would empower courts to scrutinize executive actions more rigorously, provide clearer interpretive guidance, and foster a culture of rights-respecting data governance. This would facilitate **harmonization with international best practices**, specifically those under the **African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention)** and the **General Data Protection Regulation (GDPR)**, both of which emphasize the centrality of human rights in digital regulation. For Zambia, this shift would enhance legal certainty, judicial oversight and reinforce the legitimacy of Zambia's data protection legal framework in the eyes of citizens, investors and international partners.

4.2 Critical Comparative Analysis of Specific Provisions

4.2.1 Institutional and Enforcement Mechanism

The efficacy of any data protection legal framework is inextricably linked to the strength, independence and operational capacity of the institutions tasked with its enforcement.

Robust institutional architecture is very fundamental because it not only ensures compliance but also fosters public trust, deters misconduct and affirms the normative value of privacy in the digital age.

In the **United Kingdom**, the **Information Commissioner's Office (ICO)** serves as the independent supervisory authority responsible for overseeing the implementation of the **UK General Data Protection Regulation (UK GDPR)** and the **Data Protection Act 2018**. The ICO is endowed with extensive investigatory and enforcement powers, including the authority to conduct audits, issue compliance notices, and impose administrative fines. [56]

Under the UK GDPR, the ICO may levy penalties of up to **£17.5 million or 4% of a company's global annual turnover**, whichever is higher, which is a sanctioning power that reflects the seriousness with which data breaches are treated.[57]

Notable enforcement actions underscore the ICO's institutional credibility and deterrent capacity. In **2020**, the ICO fined **British Airways £20 million** following a cyberattack that compromised the personal data of over **400,000 customers**, citing failures in security measures and breach notification protocols. Similarly, **Marriott International** was fined **£18.4 million** for inadequate protection of customer records, affecting millions of individuals across jurisdictions.[58] These cases demonstrate not only the ICO's willingness to hold powerful entities accountable but also its role in shaping corporate data governance practices through precedent and public scrutiny.

By contrast, Zambia's **Data Protection Act** [59] establishes the **Office of the Data Protection Commissioner** as the statutory regulator responsible for overseeing compliance with the Act. While the Commissioner is vested with functions such as

---

[56] Information Commissioner's Office, *Guide to the UK GDPR* (ICO, 2021) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-uk-gdpr/ accessed 26 August 2025

[57] ibid

[58] Information Commissioner's Office, *Monetary Penalty Notice: British Airways plc* (16 October 2020) <https://www.gdprregister.eu/news/british-airways-fine/ accessed 26 August 2025 : Information Commissioner's Office, *Monetary Penalty Notice: Marriott International Inc.* (30 October 2020) <https://natlawreview.com/article/ico-fines-marriott-international-184-million-security-breach accessed 26 August 2025

[59] Act No. 3 of 2021

monitoring data processing activities, investigating complaints, and promoting public awareness, the institutional framework remains **nascent and underdeveloped**. The major challenges that Zambia faces include limited **operational autonomy**, **insufficient budgetary allocation** and a **lack of technical capacity** to conduct extensive forensic investigations.[60]

4.2.2 Scope and Definition of Personal Data

The idea of "personal data" is fundamental to any data protection regime because it dictates the area of regulatory coverage and the extent of individual rights. Both **Zambia's Data Protection Act**[61] and the **United Kingdom's GDPR framewor**k use definitions, showing a common commitment to protecting data that allows individuals to be identified in an increasingly digital society.

In all countries, personal data is defined as basic identifiers like names and identification numbers, as well as online identifiers like IP addresses, cookies, and device IDs. These definitions are consistent with worldwide regulations such as the European Union's General Data Protection Regulation (GDPR) and the African Union's Malabo Convention, which emphasise the importance of protecting both direct and indirect identifiers.

Zambia's Act[62] goes further by enumerating a **detailed list of "sensitive personal data"**, which includes:

- Biometric and genetic data
- Political opinions
- Religious or philosophical beliefs
- Health status
- Sexual orientation

---

[60] Data Protection Act No. 3 of 2021 (Zambia), ss 4–6, 19, 29, 74 Office of the Data Protection Commissioner, *Data Protection Act 2021 Quick Guide* (August 2024) <https://www.dataprotection.gov.zm/wp-content/uploads/2025/03/DATA-PROTECTION-QUICK-GUIDE_2.pdf accessed 26 August 2025

[61] Act No. 3 of 2021

[62] Section 2 of The Data Protection Act No. 2 of 2021

- Ethnic or racial origin

This classification mirrors the GDPR's provisions and signals Zambia's intent to align with **international best practices** in recognizing that certain categories of data warrant **heightened protection** due to their potential to expose individuals to discrimination, profiling, or social harm.

Both the Zambian Data Protection Act as well as the **UK GDPR framework** not only identify categories of personal and sensitive data but also embed **operational principles** that govern how such data must be processed. These include:

- **Data minimisation** – only collecting data that is strictly necessary
- **Purpose limitation** – using data solely for the specified, lawful purpose
- **Proportionality** – ensuring that the scope and intensity of data collection are justified in relation to the intended outcome

These principles are not merely aspirational they are **operationalized** through binding obligations such as:

- Data Protection Impact Assessments (DPIAs) for high-risk processing activities
- **Record-keeping requirements** under the UK GDPR and Section 45 of the Data Protection Act in Zambia.
- Documentation of lawful bases for processing under GDPR and Section 45 of the Data Protection Act in Zambia.

4.2.3 Autonomy of the Data Protection Commission

Section 4 (1) of the Data Protection Act in Zambia provides as follows:

"There is established in the Ministry responsible for communications the Office of the Data Protection Commissioner which is responsible for the regulation of data protection and privacy in the Republic."

The Commission in Zambia is not a separate entity with legal personality, but rather a mere office in a Ministry. The Commissioner, thus, in practice, reports to the Permanent Secretary, who, in turn, reports to the Minister who is the head of the Ministry.
This is a misnomer and definitely negatively affects the discharge, by the Commission, of its functions. The Commission falls short of international best practice in various ways including the lack of autonomy.

The United Nations Development Programme and the International Telecommunication Union in a publication entitled “Guidelines on Regulation,”[63] in reporting shortcomings observed in various jurisdictions’ ICT regulators, indicate that regulators were within the Ministry or, if separate, lacked a firm legal mandate and the necessary political independence due to inadequate legislation or decree, the power of special interests, staff limitations or uncertain funding.

The ITU and World Bank Digital Regulation Platform, in a publication entitled Policy and Regulatory Governance: Regulatory Governance and Independence authored in December 2020 had, in echoing the above, the following to say:[64]

According to data, in over 80 per cent of countries, the regulatory authority for telecommunications and ICTs is independent from the sectoral ministry in terms of its financing, structure, and decision-making, as of the end of 2018. The regulator’s sources of funding can strongly influence its level of autonomy. Generally, a financially independent regulator obtains direct funding through legislative and budgetary allocations, allowing the regulator to identify its budget requirements in a transparent manner. In addition to direct budget allocations, regulators may be funded by licensing and other fees. Particularly if fees from licensees is the regulator’s sole source of funding, they face the challenge of setting the appropriate fee for cost recovery that

63 https://www.itu.int/ITU-D/treg/Documentation/Guideline_Regulation95.pdf Page 35 Accessed 25th October 2025

64 https://digitalregulation.org/regulatory-governance-and-independence/ Accessed 25th October 2025

balances adequate funding while not imposing unnecessarily high fees on licensees. A third mechanism is to allocate government appropriations to the ministry that oversees the regulator and, in turn, the ministry distributes funding to the regulator. However, this mechanism risks decreasing the regulator's independence by introducing the possibility of greater political influence in the regulator's decision-making processes.

Clear from the above two publications is the fact that best practice requires the regulator to be autonomous in the following manner:

(a) Structural Autonomy

The regulator should, as much as is practicable, be a separate and autonomous body – in practice statutorily created.

An example of a regulatory body that is structurally independent would be the Zambia Information and Communication Technology Authority of which section 4 of the ICT Act declares a body corporate with a common seal, capable of suing and of being sued and, subject to the provisions of the Act, capable of performing all such acts and things as a body corporate may, by law, do or perform.

(b) Financial Autonomy

This relates to the ability to retain monies generated during the course of the discharge of its obligation or otherwise have adequate resources to discharge its mandate.

(c) **Operational Autonomy**

The regulator's decisions should not be unduly influenced and should only be overturned on appeal as provided for in the law following due process.

What is clear is the fact that the Data Protection Commission seems not capable of satisfying any aspect of the above criteria. This is considering that it, being part of the Ministry and reporting to the Permanent Secretary, does not possess structural

autonomy. Reporting directly to the Permanent Secretary or Ministry potentially robs the Data Protection Commission of operational autonomy as well.

The Commission is not funded separately from the Ministry and completely depends on the monies appropriated to the Ministry by Parliament – a portion of which trickles down to the Commission. This clear robs it of financial autonomy whose absence the Government can use to control the Commission.

The Information Commissioner's Office in the United Kingdom is, in comparison, an independent body with its own Board to govern and oversee it.[65] It is, thus, separate from the central government ensuring structural autonomy in line with best practice.

The Commissioner's Office is primarily funded by organisations paying the data protection fee, which covers over 85% of the ICO's annual expenditure. This is supplemented by grant-in-aid from the government to fund the ICO's regulation of various other laws. The ICO is seemingly well funded with the institution, for instance, having collected roughly £66 million through the data protection fee from 1st April 2022 to 31st March 2023. The ICO collected £62 million in fee income in the 2021/2 financial year. The ICO also received £10,298,000 total grant-in-aid from April 2022 to March 2023, compared to £7,578,000 in the 2021/22 financial year.[66]

The above paints a picture of a regulator that is financially autonomous and with nothing indicating any interference by the government in the decisions of the ICO, it may well be said that it is operationally autonomous as well.

65 Information Commissioner's Office, https://ico.org.uk/about-the-ico/who-we-are/how-we-are-funded/ Accessed 25th October 2025

66 https://ico.org.uk/about-the-ico/who-we-are/how-we-are-funded/

4.2.4 Rights of Data Subjects

The rights of individuals form the cornerstone of data protection law. In the United Kingdom, data subjects enjoy a wide range of rights, including the right of access, rectification, erasure (the "right to be forgotten"), restriction of processing, data portability, and the right to object.[67] These rights are enforceable and supported by accessible mechanisms, with the ICO empowered to hear complaints and issue enforcement orders.

Zambia's **Data Protection Act,**[68] like its counterpart**,** grants data subjects' rights of access, correction, and objection, eraser and portability among others. Procedural mechanisms for exercising these rights, however, remain underdeveloped and untested in Zambia. This may have an effect in the practical protection of personal data in Zambia.

4.2.5 Cross-Border Data Transfers

The regulation of international data transfers is a critical issue in today's interconnected world. The United Kingdom, even after Brexit, has retained the adequacy standard from the EU, ensuring that personal data can only be transferred to jurisdictions that offer equivalent protection. This provides legal certainty for businesses and individuals while safeguarding privacy.

General Data Protection Regulation provides as follows**:**

Without prejudice to the GDPR the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor in accordance with the procedure provided in Article 60.

General Data Protection Regulation, on the other hand, provides:

---

[67] UK General Data Protection Regulation, arts 12–23 Information Commissioner's Office, *Your Data Protection Rights*(ICO, 2025) <https://ico.org.uk/global/privacy-notice/your-data-protection-rights/ accessed 26 August 202

[68]Act No. 2 of 2021

The lead supervisory authority shall cooperate with the other supervisory authorities concerned in accordance with this Article in an endeavour to reach consensus. 2The lead supervisory authority and the supervisory authorities concerned shall exchange all relevant information with each other.

The above provisions acknowledging that various supervisory authorities may have oversight authority over a Data Controller, attempts to facilitate coordination and harmonization by indicating which authority will have primary oversight.

The Zambian legal and regulatory framework neither acknowledges that a data controller may be subject to various supervisory authorities and as a result, nor does it attempt to resolve the potential challenges that may arise in the scenario.

Sections 71 of the Data Protection Act, in regulating cross border transfer of data provides:

(1) Personal data other than personal data categorised in accordance with section 70(2) may be transferred outside the Republic where -

(a) the data subject has consented **and**

(i) the transfer is made subject to standard contracts or intragroup schemes that have been approved by the Data Protection Commissioner; or

(ii) the Minister, has prescribed that transfers outside the Republic is permissible; or

(b) the Data Protection Commissioner approves a particular transfer or set of transfers as permissible due to a situation of necessity.

Section 70(1) and (2) with the latter having been referred to above provide as follows:

“70 (1) A Data Controller shall process and store personal data on a server or data centre located in the Republic.

(2) Despite subsection (1), the Minister may prescribe categories of personal data that may be stored outside the Republic.

The net effect of the above provisions is that personal data may not be transferred outside the republic on the basis of consent alone, but the consent should, rather, be accompanied by either the Data Protection Commissioner's consent or Minister's authorization in regulations. The implication of the above is that a Data Subject's consent for his or her data to be transferred outside the republic is not enough for such a request or demand to be carried out. It, rather, requires approval or consent from either the Data Protection Commissioner or the Minister.[69]

The above seems to militate and contradict Data Protection theory and concept which accords consent prominence only overridden in exceptional circumstances.[70]

4.3 Cybersecurity and Ancillary Legislation

Data protection regimes are often reinforced by cyber security and electronic communication – related legislation. In Zambia, cyber security and cyber-crime are governed by the **Cyber Security Act No. 3 of 2025 and the Cyber Crimes Act No. 4 of 2025** respectively. [71] Legislation including the **Electronic Communications and Transactions Act [72]** provide complementary support by regulating cryptography, electronic signatures and online consumer protection.

69 Thomas Katuma Malama (ICT Law Lecturer University of Zambia) University of Lusaka ICT Law Lecture Address March 2025

70 Ibid

[71] Act No. 2 of 2021

[72] Act No. 4 of 2021

In the United Kingdom, the **Computer Misuse Act 1990** and the **Telecommunications (Security) Act 2021 s**erve similar purposes but are supported by decades of institutional experience and integration with international networks.

The difference lies in implementation and capacity. While Zambia's legal framework is place, aspects of it have not been fully operationalized. The Data Protection Act was enacted in 2021 but had the Data Protection Commissioner only appointed in 2023. Regulations and guidelines supporting the Act are yet to be finalized and implemented. Registration of Data Controllers only commenced about a year ago when the Act commenced to be enforced in earnest.

The Cyber Security Act was first enacted as the Cyber Security and Cyber – Crimes Act in 2021 but was only detached from the Cyber - crimes Act this year 2025. The Cyber Security Act provides for the Cyber Security Agency whose Director General was only recently appointed. The agency is still in the process of putting in place foundational requisites such as organogram and strategic plan and with its impact only being appreciated later.

The United Kingdom benefits from stronger institutional capacity and already existing and operational international partnerships, including through the Council of Europe Convention on Cybercrime (the Budapest Convention).

4.4 Public Awareness and Trust

Public trust is very important when it comes to the efficacy of the data protection systems. In the United Kingdom, ongoing public education initiatives and rigorous enforcement have developed a culture in which people are aware of their rights and more willing to use them. Civil society organisations are also very instrumental in lobbying and monitoring.[73]In Zambia, on the other hand most people are illiterate when it comes to

[73] Centre for Data Ethics and Innovation, *Addressing Trust in Public Sector Data Use* (GOV.UK, 20 July 2020) <https://www.gov.uk/government/publications/cdei-publishes-its-first-report-on-public-sector-data-sharing/addressing-trust-in-public-sector-data-use accessed 26 August 2025

understanding data privacy regulations. This restricts the effectiveness of the legislation because unknown rights cannot be utilised. Zambia should invest in public education initiatives, collaborate with civil society, and incorporate data protection measures into digital literacy programmes.

4.5 Conclusion

This chapter conducted a comparative analysis between the data protection legal and regulatory framework in Zambia with that in the United Kingdom. The above analysis demonstrated that both Zambia and the United Kingdom recognize the importance of data protection and had in place legislation to that effect. Noted was the fact that Zambia's legal framework, like that of the United Kingdom, had very progressive and appropriate provisions. It was, however, noted that Zambia's legal framework lagged behind best practice in certain aspects including cross border transfer data regulation and autonomy of the Data Protection Commission.

CHAPTER FIVE

CONCLUSIONS AND RECOMMENDATIONS

5.0 Introduction

This chapter summarizes the contents presented in the preceding chapters of this study. It, at the same time, provides recommendations that aim to address the problems in the Zambian data protection legal and regulatory framework as identified in this study.

The recommendations are aimed at improving the legal, institutional, and practical frameworks governing personal data protection, drawing lessons from the United Kingdom’s developed data protection regime.

5.1 General Conclusion

The protection of personal data is a fundamental human right that is critical to preserving individuals' dignity, autonomy, and privacy in the digital age. The study found that, while Zambia has made substantial progress towards developing an adequate legal framework for data protection, the existing regime is still in its early stages requiring review with protection of personal data facing a number of challenges. Challenges include both in the legal and regulatory framework itself as well as institutional and implementation – related ones. This has led to the data protection regime in Zambia not being as effective as can be.

Zambia's Data Protection Act No. 3 of 2021, along with complementary legislation such as the Electronic Communications and Transactions Act of 2021, Cyber Security Act No. 3 of 2025, and Cyber Crimes Act No. 4 of 2025, form a foundation for data governance. However, fragmentation among these laws, overlapping mandates, and insufficient enforcement mechanisms have led to gaps in implementation.

The United Kingdom's Data Protection Act 2018, which integrates the General Data Protection Regulation (GDPR) principles, provides a comprehensive and well-enforced system. The UK approach demonstrates how a strong institutional framework, adequate and appropriate data protection legislation coupled with effective implementation and regulatory supervision can effectively protect data privacy.

5.2 Summary of Chapters

This research paper consists of five chapters, each contributing to the understanding and analysis of data protection and privacy laws in Zambia and the United Kingdom.

5.2.1 Chapter One

The first chapter introduced the research topic, setting out the background to the study, the statement of the problem, the research objectives, and the significance of the study. It established that data protection and privacy are increasingly under threat in Zambia due to rapid technological developments and inadequacies in the legal framework coupled with insufficient enforcement of existing laws. The chapter laid the foundation by highlighting the need for a comparative study with the United Kingdom, whose data protection framework serves as a model of best practice.

5.2.2 Chapter Two

Chapter Two looked at the notion of data protection and its significance.It dealt with the theoretical basis of the right to privacy, essential terms such as "personal data," "data subject," "data controller," and "data processor." It also examined the justification for data protection, emphasising its importance in fostering trust, guaranteeing accountability, and protecting individuals from the exploitation of their personal information.

5.2.3 Chapter Three

Chapter Three focused on the data privacy legal frameworks in Zambia and the United Kingdom. It analyzed Zambia's **Data Protection Act**[74] and other related statutes such as the **Electronic Communications and Transactions Act**[75], the **Cyber Security Act**[76], the **Cyber Crimes Act**[77] and the **Information and Communications Technologies Act**[78]. It also examined the **UK's Data Protection Act 2018, Computer Misuse Act 1990, and Telecommunications (Security) Act 2021.**

5.2.4 Chapter Four

Chapter Four provided a comparative analysis of the data protection frameworks in the two jurisdictions. It revealed significant similarities and differences in legal structure, institutional monitoring, enforcement, and protection of data subjects' rights. The analysis indicated that, while Zambia's framework is still maturing, it has the potential to be more effective if guided by lessons from the UK model.

---

[74] Act No. 3 of 2021
[75] Act No.4 of 2021
[76] Act No. 3 of 2025
[77] Act No.4 of 2025
[78] Act No.15 of 2009

5.3 Recommendations

Having identified the challenges and shortcomings in Zambia's data protection framework, this study makes the following recommendations to improve the protection and enforcement of data privacy rights in Zambia:

5.3.1 Legislative Harmonization

Zambia should harmonize its various laws relating to data protection, cyber security, and ICT regulation. The existence of multiple overlapping statutes may lead to confusion and inconsistency in enforcement.

5.3.2 Strengthening the Office of The Data Protection Commissioner

The Office of the Data Protection Commissioner must be adequately resourced and granted greater institutional independence. This will enhance its ability to monitor compliance, issue directives, and enforce penalties against non-compliance, similar to the role played by the Information Commissioner's Office (ICO) in the United Kingdom**.**

5.3.3 Respect for Data Subject's Consent

Data Protection should be amended in sections 70 and 71 to provide for a scenario in which a Data Subject should be sent from a Data Subject to have his or her personal data transferred outside the republic should, as a rule, be respected and honored.

5.3.4 Public Awareness and Education

Public knowledge of data protection rights remains low in Zambia. The government, civil society, and private sector should collaborate to create continuous awareness campaigns

and educational programs to inform individuals and organizations about their data rights and obligations.

The Data Protection Act should be amended to provide for express and meaningful sanction for failure on the part of the Data Protection Commission to conduct regular country wide awareness campaigns.

5.3.5 Capacity Building for Data Controllers and Processors

There is a need to provide in the Data Protection Act, express implementable obligations on the part of Data Controllers and Data Processors to ensure their Data Protection Officers undergo regular training and attain data protection – related qualifications recognized by the Data Protection Commission within a given period of time. This can be extended to Data Protection auditors with failure to do so attracting sanctions.

This will promote compliance with the Data Protection Act and ensure that entities processing personal data do so in line with global best practices.

5.4 Final Remarks

Zambia has made significant progress in achieving a comprehensive data protection legal framework but it is still developing .Unfortunately the country is struggling to ensure effective implementation of the existing pieces of legislation and harmonising the laws around data protection,involving the public at large and ensuring that all citizens' are able to fully realise their data protection rights .Zambia can therefore create a resilient, transparent, and trustworthy data protection environment that meets international standards and safeguards its citizens' privacy rights by learning from the United Kingdom's existing framework.

BIBLIOGRAPHY

STATUTES

The Computer Misuse Act 1990 (UK)

The Data Protection Act 1984 (UK)

The Data Protection Act 2018 (UK)

The General Data Protection Regulation (EU) 2016/679

The UK General Data Protection Regulation, SI 2019/419

The Data Protection Act No 3 of 2021 (Zambia)

The Cyber Security and Cyber Crimes Act No 2 of 2021 (Zambia)

The Electronic Communications and Transactions Act No 4 of 2021 (Zambia

INTERNATIONAL INSTRUMENTS

The Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) (ECHR) art 8

The African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention, adopted 27 June 2014, not yet in force)

CASES

R (Bridges) v Chief Constable of South Wales Police* \ [2020] EWCA Civ 1058, \ [2020] 1 WLR 5027

Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González (Case C-131/12, CJEU, 13 May 2014)

REGULATORY AND POLICY DOCUMENTS

Information Commissioner's Office (ICO), **'Guide to the UK GDPR'** (ICO 2021) [https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-uk-gdpr/](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-uk-gdpr/ Aaccessed 26 August 2025

Information Commissioner's Office (ICO), 'Your Data Protection Rights' (ICO 2025) [https://ico.org.uk/global/privacy-notice/your-data-protection-rights/ (https://ico.org.uk/global/privacy-notice/your-data-protection-rights/ accessed 26 August 2025

Information Commissioner's Office (ICO), **'Monetary Penalty Notice: British Airways plc'** (16 October 2020) [https://www.gdprregister.eu/news/british-airways-fine/](https://www.gdprregister.eu/news/british-airways-fine/ Aaccessed 26 August 2025

Iinformation Commissioner's Office (ICO), **'Monetary Penalty Notice: Marriott International Inc'** (30 October 2020) [https://natlawreview.com/article/ico-fines-marriott-international-184-million-security-breach (https://natlawreview.com/article/ico-fines-marriott-international-184-million-security-breach Accessed 26 August 2025

Office of the Data Protection Commissioner (Zambia), Data Protection Act 2021 Quick Guide (August 2024) [https://www.dataprotection.gov.zm/wp-content/uploads/2025/03/DATA-PROTECTION-QUICK-

GUIDE_2.pdf](https://www.dataprotection.gov.zm/wp-content/uploads/2025/03/DATA-PROTECTION-QUICK-GUIDE_2.pdf Accessed 26 August 2025

Centre for Data Ethics and Innovation (CDEI), 'Addressing Trust in Public Sector Data Use' (GOV.UK, 20 July 2020) [https://www.gov.uk/government/publications/cdei-publishes-its-first-report-on-public-sector-data-sharing/addressing-trust-in-public-sector-data-use (https://www.gov.uk/government/publications/cdei-publishes-its-first-report-on-public-sector-data-sharing/addressing-trust-in-public-sector-data-use Accessed 26 August 2025

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2162781
https://pure.uva.nl/ws/files/34085945/European_Union_General_Data_Protection_Regulation.pdf https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3662302

UNIVERSITY of LUSAKA
Passion for Quality Education: Our Driving Force

SCHOOL OF LAW

L400B / Dissertation II – DIRECTED RESEARCH (OBLIGATORY ESSAY)

RESEARCH CLEARANCE FORM

NAME: NAKAUNDI NAKAZWE STUDENT NUMBER: LLB19116061

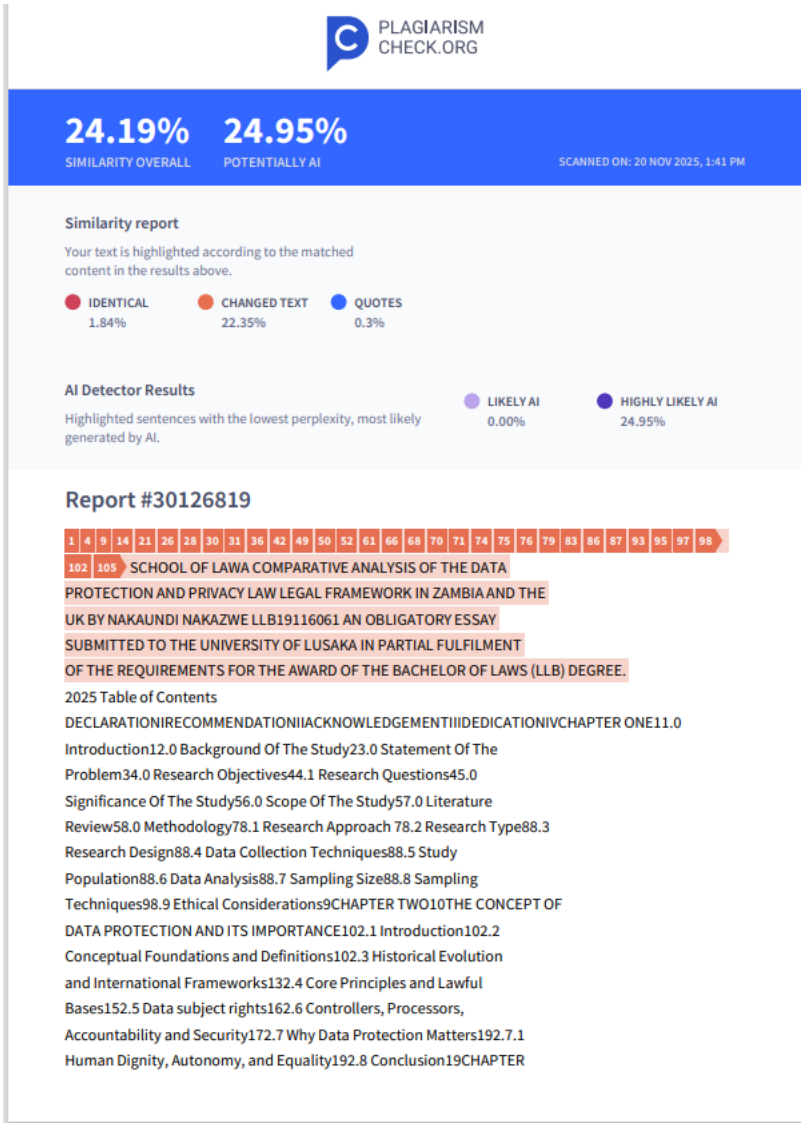
SUPERVISOR: Mr. THOMAS MALAMA TOPIC: A COMPARATIVE ANALYSIS OF THE DATA PROTECTION AND PRIVACY LAW LEGAL FRAMEWORK IN ZAMBIA AND THE UK

Stage	Supervisor's Comments	Supervisor's Signature & Date	Student's Signature & Date
Research Proposal	Corrections Reviewed and approved.	27/09/2025	27/09/2025
Chapter 1 – Introduction	Corrections Reviewed and approved.	06/10/2025	06/10/2025
Chapter 2 –	Reviewed and approved [a] Titles of the Chapter, Sections and Works should have first words capitalized except the words "a" " the" " for" "and" etc [b] Rights in the GDPR fall under Articles 12 - 23 and not 12-21 as indicated.	12/10/2025	12/10/2025

	[c] Renumbering of sections - some seem to have been erroneously numbered. [d] Under Conclusion AT THIS STAGE you cannot make a determination that the the Data Protection Act reflects the global trajectory embedding rights, principles etc You haven't yet conducted a critical analysis of the Act		
Chapter 3 –	Reviewed and Approved [a] A couple of words in Chapter Title had first words wrongly capitalized [b] Indicate dates when internet sources were accessed [c] Note Cyber Security Act separated from Cyber Crimes Act in Zambia. [c] 3.1 heading included [d] See Renumbering from 3.1.3 [e] See clarification of content relating to TSA	14/10/2025	14/10/2025
Chapter 4 –	Reviewed and approved SECTION 46 IN THE DATA PROTECTION ACT PROVIDES FOR IMPACT ASSESSMENT THE SAME WAY GDPR DOES IN ARTICLES 35, 84, 90, AND 91	25/10/2025	25/10/2025

	SECT 45 Data Protection Act provides for data processing documentation requirements Section 65 provides for Data Portability Section 60 provides for Right to Erasure / be Forgotten Cyber Security and Cyber Crimes Act WAS REPEALED AND REPLACED WITH TWO SEPARATE ACTS: Cyber Security Act No. 3 of 2025 Cyber Crimes Act No. 4 of 2025		
Chapter 5 – Conclusions & Recommendations	Reviewed and approved. Ensure reference is to UK GDPR in places we discussed.	31/10/2025	31/10/2025
Abstract, Table of Contents and Bibliography	Reviewed and Approved	02/11/2025	02/11/2025
First Draft	Reviewed and Approved		
Second Draft	Reviewed and Approved		
Final Draft	Reviewed and Approved	12/11/2025	12/11/2025

Please attach this form to the back of your dissertation at the end of the research, before submission via the Moodle e-learning platform


PLAGIARISM CHECK.ORG
24.19%
SIMILARITY OVERALL
24.95%
POTENTIALLY AI
SCANNED ON: 20 NOV 2025, 1:41 PM
Similarity report
Your text is highlighted according to the matched content in the results above.
IDENTICAL 1.84%
CHANGED TEXT 22.35%
QUOTES 0.3%
AI Detector Results
Highlighted sentences with the lowest perplexity, most likely generated by AI.
LIKELY AI 0.00%
HIGHLY LIKELY AI 24.95%
Report #30126819
1 4 9 14 21 26 28 30 31 36 42 49 50 52 61 66 68 70 71 74 75 76 79 83 86 87 93 95 97 98 102 105 SCHOOL OF LAWA COMPARATIVE ANALYSIS OF THE DATA PROTECTION AND PRIVACY LAW LEGAL FRAMEWORK IN ZAMBIA AND THE UK BY NAKAUNDI NAKAZWE LLB19116061 AN OBLIGATORY ESSAY SUBMITTED TO THE UNIVERSITY OF LUSAKA IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE AWARD OF THE BACHELOR OF LAWS (LLB) DEGREE.
2025 Table of Contents
DECLARATIONIRECOMMENDATIONIIACKNOWLEDGEMENTIIIDEDICATIONIVCHAPTER ONE11.0 Introduction12.0 Background Of The Study23.0 Statement Of The Problem34.0 Research Objectives44.1 Research Questions45.0 Significance Of The Study56.0 Scope Of The Study57.0 Literature Review58.0 Methodology78.1 Research Approach 78.2 Research Type88.3 Research Design88.4 Data Collection Techniques88.5 Study Population88.6 Data Analysis88.7 Sampling Size88.8 Sampling Techniques98.9 Ethical Considerations9CHAPTER TWO10THE CONCEPT OF DATA PROTECTION AND ITS IMPORTANCE102.1 Introduction102.2 Conceptual Foundations and Definitions102.3 Historical Evolution and International Frameworks132.4 Core Principles and Lawful Bases152.5 Data subject rights162.6 Controllers, Processors, Accountability and Security172.7 Why Data Protection Matters192.7.1 Human Dignity, Autonomy, and Equality192.8 Conclusion19CHAPTER

THREE20DATA PRIVACY LEGAL FRAMEWORKS IN ZAMBIA AND THE UNITED KINGDOM203.0 Introduction203.1 Data Protection Legal Framework in Zambia203.1.1 Data Protection Act203. 1.2 Electronic Communications and Transactions Act 2021223.1. 3 Cyber Security Act No. 3 of 2025243.1. 4 The Cyber Crimes Act No. 4 of 2025273.1.5 The Information and Communications and Technologies Act283.2 Data Protection Legislation in the United Kingdom293.2.1 The Data Protection Act of 2018293.2.2 The Computer Misuse Act 1990303.2.3 Telecommunications (Security) Act 2021 (TSA)313.3 Conclusion31CHAPTER FOUR32COMPARATIVE ANALYSIS OF DATA PROTECTION LEGAL REGIMES IN ZAMBIA AND THE UNITED KINGDOM324.0 Introduction324.1 Conceptual and Philosophical Foundations of Data Protection334.2 Critical Comparative Analysis of Specific Provisions364.2.1 Institutional and Enforcement Mechanism364.2.2 Scope and Definition of Personal Data374.2.3 Autonomy of the Data Protection Commission394.2.4 Rights of Data Subjects424.2.5 Cross-Border Data Transfers424.3 Cybersecurity and Ancillary Legislation444.4 Public Awareness and Trust454.5 Conclusion46CHAPTER FIVE47CONCLUSIONS AND RECOMMENDATIONS475.0 Introduction475.1 General Conclusion475.2 Summary Of Chapters485.2.1 Chapter One485.2.2 Chapter Two495.2.3 Chapter Three495.2.4 Chapter Four495.3 Recommendations505.3.1 Legislative Harmonization505.3.2 Strengthening The Office Of The Data Protection Commissioner505.3.3 Respect Of Data Subject'S Consent505.3.4 Public Awareness And Education515.3.5 Capacity Building For Data Controllers And Processors515.4 Final Remarks51Bibliography..... ..... 1 4 5 9 12 14 16 17 20 26 28 33 35 40 41 42 44 49 50 52 54 55 56 58 59 61 66 70 71 74 75 76 79 80 83 85 86 87 93 94 95 97 101 105 107 52 DECLARATION I declare that this dissertation entitled, A COMPARATIVE ANALYSIS OF THE DATA PROTECTION AND PRIVACY LAW LEGAL FRAMEWORK IN ZAMBIA AND THE