UNIVERSITY of LUSAKA

Passion for Quality Education: Our Driving Force

SCHOOL OF LAW

A CRITICAL ANALYSIS OF THE LEGAL FRAMEWORK GOVERNING DATA PROTECTION AND CYBER SECURITY IN ZAMBIA: LESSONS FROM INTERNATIONAL STANDARDS.

BY

NAMASIKU ANAKOKA

LLB22113403

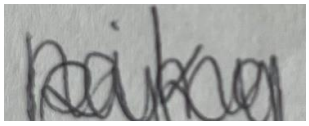
AN OBLIGATORY ESSAY SUBMITTED TO THE UNIVERSITY OF LUSAKA IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE AWARD OF THE BACHELOR OF LAWS (LLB) DEGREE.

2025

DECLARATION

I, NAMASIKU ANAKOKA**,** declare that this dissertation entitled, **A CRITICAL ANALYSIS OF THE LEGAL FRAMEWORK GOVERNING DATA PROTECTION AND CYBER SECURITY IN ZAMBIA: LESSONS FROM INTERNATIONAL STANDARDS,** 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.

NAMASIKU ANAKOKA



……..

2025

RECOMMENDATION

I, KASWALALE MWAULUKA recommend that this dissertation prepared under my supervision by NAMASIKU ANAKOKA, entitled A CRITICAL ANALYSIS OF THE LEGAL FRAMEWORK GOVERNING DATA PROTECTION AND CYBER SECURITY IN ZAMBIA: LESSONS FROM INTERNATIONAL STANDARDS be accepted for examination. I have checked it carefully and I'm satisfied that it fulfils the requirement pertaining to the format laid down in the regulations governing directed research.

……

K. MWAULUKA

ACKNOWLEDGEMENTS

To begin with, I would like to give my lord and saviour all the glory for carrying me with grace throughout this tedious journey that is law school. A journey that has been filled with tears, laughs, failures, achievements and above everything, lessons and through it all, my God has been with me reminding me that he did not create me with a spirit of fear, but of power and love and of a sound mind.

Secondly, I would like to extend my heartfelt gratitude to my supervisor, Mrs. Kaswalale Mwauluka for guiding me through this research and being very patient and thorough with my work and ensuring that I make the necessary adjustments to ensure that this work serves its purpose and is as comprehensive as possible.

Thirdly, I would like to wholeheartedly thank my father Hon. Mubita Boris Anakoka and my late mother Mrs. Virginia Hapeza Anakoka. To my father, I owe you the world and more and I'm beyond grateful for all the sacrifices you've made in order to ensure I have a life beyond my imagination. To my mother, even in your absence I've felt your love and support through all the memories of the lessons you taught me. The both of you crawled so I could walk and for that I will always be grateful.

I would also like to thank my parental figures, my aunts, Ms. Mwangala Jane Mufungulwa, Mrs. Vivian Hapeza Mweetwa and Mrs. Joan Chama Mufungulwa. Thank you for being strong mother figures and raising me to be an upstanding lady, instilled with morals and a hardworking spirit. I'm beyond grateful for all the love and support you've given me.

To my siblings, Lungowe, Eva and Mufungulwa, thank you for always believing in me and being constant cheerleaders throughout this journey. I'm extremely grateful for all of you. I'd like to specifically thank my first friend, my sister by chance and best friend by choice, Tehilla. To my biggest cheerleader I want to say thank you, thank you for always being my rock, for being my voice when mine was shaken, for assuring me that the reward is worth the hard work and for constantly holding my hand throughout all four years of this journey.

Lastly, I'd like to thank my friends, Bupe Emmanuel Mukamba, Kasongo Shisholeka, Tianna Chimwemwe Kumwenda, my friend turned sister, Mwenya Nchimunya Mwansa, Choolwe Kalaluka, Grace Chansa, Hope Kamangu and Wana Martha Kapambwe, my forever friend, all of whom made this journey bearable and worth

remembering by offering all the emotional support I needed and creating some of the best memories that will last a lifetime. To you all, I'm forever grateful. I would like to give a special thanks to my friend turned sister, Doreen Soko, who has been with me from the first day of law school and watched me grow. I'm so glad I get to experience not only law school with you but life generally and I cannot wait to see what more God has in store for us.

DEDICATION

This dissertation is dedicated to my beloved parents, Hon. Mubita Anakoka and my late mother Mrs. Virginia Hapeza Anakoka. This dissertation would not have been possible without your help both physically and in spirit. Through their unwavering support, constant cheerleading and unlimited love, I have been given all the strength to successfully complete this program of study. I am eternally grateful to them both for constantly reminding me that the sky isn't the limit, it's only the view.

Table of Contents

ABSTRACT

This thesis was a critical analysis on the legal framework governing data protection and cyber security in Zambia, drawing lessons from international standards. The purpose of this study was to assess the adequacy, coherence and alignment of the Data Protection Act no.3 of 2021 and Cybersecurity Act no.3 of 2025 with international standards such as the General Data Protection Regulation (GDPR), Budapest Convention and the Malabo Convention. The objectives of this study include examining the legal framework on cybersecurity and data protection in Zambia, the extent to which these pieces of legislation align with international standards and lastly the need for alignment of the local legislation with said international standards.

The methodology of this research was as follows; the research was a qualitative mode of research as data was obtained from statutes, reports, internet sources as well as articles.

The major findings of this research were that that is some partial convergence with international benchmarks but persistent divergence in institutional autonomy, procedural safeguards and operational clarity. The misalignment undermined individual rights, national security and economic development while full harmonization would enhance resilience, investor confidence, cross border cooperation and digital innovation. It further identified shortcomings with the current legislation like the absence of emerging cybercrimes and an ambiguity in the scope, consent overrides and inadequate enforcement mechanisms

CHAPTER ONE

GENERAL INTRODUCTION

INTRODUCTION

This chapter discusses the legal framework that governs data protection and cyber security in Zambia, evaluating its strengths, weaknesses, adequacy, coherence and enforcement mechanisms. This study draws comparative studies from the General Data Protection Regulation (GDPR) which is an international convention of the European Union, the Budapest Convention, which is a global cybersecurity framework and the Malabo Convention which is a convention by the African Union on cyber security and personal data protection. The study will be examining how well Zambia's legal framework complies with international standards that have been set and how best it addresses the challenges of protecting personal data and cyber security in a manner that balances national security, individual rights and economic development. The chapter will highlight the background, objective and the significance of the study as it adds to the already existing pool of knowledge while subsequently serving as a point of reference for further studies in similar research areas or interests.

1.1 BACKGROUND OF THE STUDY

Cybersecurity includes the tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practice, assurances and technologies that can be used to protect the cyber environment, organisation and user assets.[1] Cybersecurity is the practice of protecting computer systems, networks, programs and data from digital attacks, unauthorized access, theft, damage and disruption. It encompasses a wide range of technologies, processes and practices designed to safeguard the confidentiality, integrity and availability of information on the cyber space. Data protection refers to strategies, processes and technologies aimed at safeguarding sensitive information from corruption, compromise and loss while ensuring its availability for authorized use. It encompasses measures to prevent data breaches, data loss incidents and compliance violations as well as mechanisms for restoring lost or damaged data.

[1] Act no.3 of 2025

Over the years there has been a vast change in the way people, companies, businesses, countries, among other things, relate to each other. As there has been a rapid advancement of information and communication technologies (ICTs), there has also been a revolution in the way society's function, enabling access to data, enhancing connectivity and transforming service delivery across both public and private sectors. Regardless of this spectacle, there has been an introduction of complex challenges relating to data protection and cyber security. In an era that is marked by increasing cyber threats, data breaches, identity theft, constant online scamming, hacking of major corporations, the establishment of robust legal frameworks to protect digital rights and a secure cyber space has become a critical necessity calling for desperate attention.

In Zambia, as a result of the rapid use of internet services, mobile technologies and digital financial services such as mobile money and mobile banking, there has been a rise in vulnerability to cybercrime and data privacy violations. The Zambian government, having recognized these threats, decided to introduce key pieces of legislation to tackle these issues being the **Cybersecurity Act no.3 of 2025** and the **Data Protection Act no. 3 of 2021.** These laws represent important steps towards regulating the digital space, protecting personal information and deterring cybercrime. However, regardless of this, there is still some concern that is raised in relation to these Acts and their effectiveness, scope and compatibility with international standards. There have been questions asked by various stakeholders as to whether the current legislation adequately balances state interests with individual rights and whether the current legislation provides sufficient clarity, safeguards and enforcement mechanisms.

Furthermore, Zambia's capacity to implement and enforce these laws remains a significant challenge due to institutional weaknesses, limited technical expertise and lack of public awareness hindering their practical application. The regulator and authority in charge of ensuring such things primarily is the Zambia Information and Communication Technology Authority herein referred to as ZICTA and their adequate implementation is lacking due to lack of adequate expertise and means to deal with cybercrimes and data breaches.

1.2 STATEMENT OF THE PROBLEM

Zambia has taken progressive steps to address data protection and cyber security through the enactment of the Cybersecurity Act no.3 of 2025 and the Data Protection Act no.3 of 2021 however regardless of this, several issues persist. For the Cybersecurity Act, examples of the inadequacies include the fact that there are missing crimes. This basically alludes to the fact that the current Act does not account for certain cyber-attacks such as sonic attacks and swatting. Sonic attacks involve the use of Sonic and ultra-sonic weapons (USW) that use sound to injure or incapacitate an opponent. In 2020 there had been a report of mysterious head injuries suffered by US diplomatic staff in China and Cuba that had been described as sonic attacks and they were as a result of directed microwave energy according to a report that was given.[2] Such a crime can be committed in Zambia and because the Act does not provide for it, it would be difficult to try someone. Swatting is a term that is used to describe the action of making deceptive phone calls to report serious crimes to emergency services.[3] It is a cyber-crime that involves people pranking emergency services into sending the Special Weapons and Tactics (SWAT) team to respond to the supposed emergency. Regardless of the fact that Zambia does not have such a team, it does have emergency services like fire services and they could equally be called in such a manner and because the current Act does not provide for this crime, it would be difficult to try or charge the perpetrators.

Section 3 of the Cyber Security Act[4] provides for the establishment of the Zambia Cyber Security Agency in the Office of the President which is responsible for the administration of the entire Act under the general direction of the President. It can be seen that, considering the fact that there is a specific agency that is to deal with matters is cyber security, it can be seen that there is autonomy in how the agency functions and operates however question can be raised as to whether the agency is fully autonomous in terms of finances as an agency like that needs to be financially autonomous to properly function.

[2] Sonic attacks suffered by US diplomats likely caused by microwave energy accessed at www.cnn.com on 16/04/2025
[3] Swatting accessed at https://www.fortinet.com on 16/04/2025
[4] Act no.3 of 3025

There is a lack of adequate safeguards when the law provides for derogation. In terms of interception of communication, the safeguards are not adequate in that ***section 21 of the Cyber Security Act***[5] provides for the establishment of the Central Monitoring and Co-ordination Centre which is managed, controlled and operated by the department responsible for government communications however in practice no one is aware of where this centre is or which department exactly is being talked about as there is an ambiguity.

In relation to the Data protection Act, the institutional framework is wrong as the Data Protection Commissioner which is established by ***section 4 of the Data Protection Act***[6] belongs to the Ministry of Technology and Science when it should be a stand-alone institution. It would be difficult for the commissioner to adequately perform is duties as he reports to the Minister and the Permanent Secretary and if they breach data protection laws, the commissioner would not be able to site them. Another problem is that there is lack of autonomy for the commission financially, structurally and operationally. Another inadequacy is the overriding of consent in that the commissioner has the power to override consent given by the data subject in a situation where their data is being used and consent is required. Another inadequacy is that the scope of application is confusing. ***Section 3 of the Data Protection Act***[7] states that the Act applies to the processing of personal data performed wholly or partly by automated means and shall not apply to the processing of personal data by an individual for personal use. The term personal use is subjective and the whole section does not give a clear definition of what the actual scope is as there are too many ambiguities.

1.3 GENERAL OBJECTIVE

This study is aimed at critically analysing the legal framework governing data protection and cyber security in Zambia with the aim of assessing its adequacy, effectiveness and alignment with international standards and best practices established in the General Data Protection Regulation (GDPR), The Malabo Convention and the Budapest Convention. Furthermore, this study seeks to explore the extent to which current Zambian laws respond to the dynamic challenges posed in

[5] Act no.3 of 2025
[6] Act no.3 of 2021
[7] Act no.3 of 2021

the digital era and how this affects her economy as well as how the adherence to international standards or lack of affects her economy.

SPECIFIC OBJECTIVES

i. To examine the legal framework governing the cyber security and data protection in Zambia

ii. To assess the extent to which Zambia's legal framework aligns with international set standards such as the GDPR, Budapest Convention and the Malabo Convention in governing cyber security and data protection.

iii. To examine the need for Zambia's legal framework to align with international set standards such as the GDPR, Budapest Convention and the Malabo Convention in governing cyber security and data protection.

1.4 RESEARCH QUESTIONS

i. What is the legal framework governing cyber security and data protection in Zambia?

ii. What is the extent to which Zambia's legal framework align with international set standards such as the GDPR, Budapest Convention and the Malabo Convention in governing cyber security and data protection?

iii. Why is there a need for Zambia's legal framework to align with international set standards such as the GDPR, Budapest Convention and the Malabo Convention in governing cyber security and data protection?

1.5 SIGNIFICANCE OF THE STUDY

This study is important as it contributes to the already existing body of law on cyber security and data protection particularly in the African context, specifically in Zambia where such research remains limited. It identifies practical challenges and inconsistencies in the legal framework, offering recommendations to strengthen legal and institutional responses to cyber threats and data protection concerns. This study is significant as it highlights how a well-developed legal framework can act as an enabler of economic development by enhancing investor confidence, supporting digital innovation and facilitating international cooperation in cybercrime prevention. It will show how aligning with international standards can also enhance Zambia's global standing and readiness to participate in international digital commerce.

1.6 SCOPE OF THE STUDY

This study will focus on the legal framework governing data protection and cyber security in Zambia as it critically analyses the content, implementation and practical impact of these laws in addressing the challenges posed by this digital era. It will be limited to Zambia though there will be comparisons with international legal instruments such as the GDPR of the European Union, the Budapest Convention on Cybercrime and the Malabo Convention on Cyber Security and Data Protection formulated by the African Union. It will show how adherence to the international standards or lack thereof would affect the Zambian economy.

1.7 LITERATURE REVIEW

Local and foreign authors have written on the cybersecurity and data protection. They've written on the legal framework governing cybersecurity and data protection and their implementation of international standards. This study aims to add to the already existing body of knowledge created by the following authors.

Christine Simfukwe and Alice P Shemi have written that digital technologies have become increasingly integral to critical infrastructure and emerging economies like Zambia are facing heightened cybersecurity threats. The two authors have stated that current security measures are often inadequate, leaving essential services vulnerable to cyber-attacks.[8] These authors brought out the fact that there is a high rise of the use of technology in relation to emerging economies such as Zambia however they did not highlight how having an autonomous cyber security body in charge of handling cyber threats would aid in the heightened threats that have emerged.

Howard Shrobe, David L Shrier and Alex Pentland wrote that resolving the tension between data sharing and privacy, to unlock the potential value of that data is a challenge, particularly for governments and regulated industries. Although centralized databases for processing may be conceptually simpler, distributed networks with privacy preserved algorithms can maximise security for data processing in compliance with legal and ethical requirements.[9] These authors brought out the fact that a centralized system for data protection may be effective however may not be the best solution in terms of legal and ethical compliance and they spoke of this in relation to

[8] S Christine and S P Alice, Advancing cybersecurity measures to safeguard critical infrastructure and data: is Zambia ready? Available at https://ictjournal.icict.org.zm accessed on 14/04/2025

[9] S Howard and P Alex, New Solutions for Cybersecurity (The MIT Press,2017)

the cyber space. They did not, however, highlight how having a well built-up institutional framework for data protection would be adequate as there would be efficiency in terms of practice and administration of data protection in the country.

Rohit Manglick wrote in his book that for the United States, there is no single agency or departments that is responsible for nationwide cybersecurity as it does for other departments. Due to the unique nature of cybersecurity, responsibilities are scattered throughout the federal government.[10] This author focuses on the fact that cybersecurity is too intricate to have only one agency handling it however the author does not highlight the importance of having only one autonomous body to handle cyber security considering its very intricate nature.

Chaminda Hewage and Lasith Yasakethu wrote in their book that ensuring the privacy of data has become a complex challenge, necessitating robust frameworks to balance the transformative potential of AI with the fundamental rights of individuals.[11] These authors are of the view that data protection requires a robust framework to balance rights of individuals and technology however the two authors do not comment on the importance of having legislation that governs data protection as it would establish a proper institutional framework that would impose sanctions on those that do not abide by said laws.

Samuel Fikiri Cinini wrote in an article that the cost of cybersecurity is steadily increasing, both in terms of the overall loss to the organisation and in terms of the number of cyberattacks. Every day, new cyber threat types and features appear in the worldwide environment. African countries have recently suffered from an increase in cyber threats and the continent is experiencing an increase in cyber-attacks which can be ascribed to weak cybersecurity measures and vulnerable systems.[12] This author emphasized the need for a strong cybersecurity system and measures however they did not highlight how this can be achieved through alignment of local legislation to international standards that have proven to aid in the alleviation of cyber security and data protection breaches.

[10] R Manglik, Cybersecurity and Law (EduGorilla Prep Experts, 2024) 269
[11] C Hewage and L Yakasethu, Data Protection: the wake of AI and machine learning 2024
[12] S F Cinini, The trends of cybersecurity and its emerging challenges in Africa available at www.link.springer.com accessed on 14/04/2025

1.8 METHODOLOGY

1.8.1 RESEARCH APPROACH

This study adopts a qualitative approach focusing on legislation, regulations and legal principles related to cyber security and data protection so as to better explore the topic and generate new insights on the subject where possible.

1.8.2 RESEARCH DESIGN

This study will adopt the evaluative design as it will focus on the collecting and analysing of data to assess the impact or effectiveness of a piece of legislation. This will allow for further understanding of both the Cybersecurity Act and the Data Protection Act and their adherence to international set standards and best practices.

1.8.3 RESEARCH TYPE

This research is undertaken in a way that examines the legal framework governing cybersecurity and data protection in Zambia, with lessons drawn from international conventions such as the GDPR, Malabo Convention and Budapest Convention.

1.8.4 STUDY POPULATION

Given the fact that this study is of qualitative nature, the study population consists of legal instruments, institutional frameworks and key stakeholders involved in the regulation, implementation and oversight of data protection and cyber security in Zambia.

1.8.5 SAMPLING TECHNIQUE

For the purposes of this study, purposive sampling shall be used as it allows selective analysis of legal instruments and international conventions that are relevant to this study.

1.8.6 DATA COLLECTION

The information that will be used in this study will be secondary data that is gathered from pieces of legislation, books, journal articles, international conventions and regulations.

1.8.7 ETHICAL CONSIDERATION

In meeting the ethical standards set, the author of this dissertation shall seek permission from the University of Lusaka before commencement of the research. This

includes the use of OSCOLA referencing of scholarly writings to avoid plagiarism as per university and ethical expectations of the legal profession.

1.9 CHAPTER OVERVIEW

CHAPTER ONE stands as an introduction to the dissertation, providing a background of the study as well as problem statement in relation to the study.

CHAPTER TWO examines the legal framework governing cyber security and data protection in Zambia.

CHAPTER THREE assesses the extent to which Zambia's legal framework aligns with international set standards on cyber security, identifying the harmonization and lack thereof.

CHAPTER FOUR highlights the need for Zambia's legal framework to align with international standards, comparing the benefits of alignment with said standards from other jurisdictions and the pitfalls of none alignment by Zambia.

CHAPTER FIVE summarizes the contents provided in the aforementioned chapters of this dissertation

CHAPTER TWO

THE LEGAL FRAMEWORK GOVERNING CYBER SECURITY AND DATA PROTECTION IN ZAMBIA

2.0 INTRODUCTION

This chapter provides a thorough examination of the legal framework in Zambia that governs cyber security and data protection, being the Cybersecurity Act no.3 of 2025 and the Data Protection Act no.3 of 2021. It critically reviews the institutional frameworks under the Cyber security and Data Protection Acts, the key provisions in both Acts, the enforcement mechanisms that are currently in place, how these laws regulate and control the cyber space, protect personal information as well as tackle and reprimand cybercrime in Zambia. It will also be identifying the strengths and weaknesses of both Acts in relation to implementation of the aforementioned laws.

2.1 THE CYBERSECURITY ACT NO.3 OF 2025

The Zambian government realized the high number of growing threats in Zambia that appear in the cyber space and issues of data breaches due to the increased use of digital platforms and for this reason decided to establish a law that would aid in combatting the same. The Cybersecurity Act, as stated in its short title, is a piece of legislation in Zambia that was enacted for the purposes of establishing the Zambia Cyber Security Agency and providing for its functions, the regulation of cyber security service providers in Zambia, provide for the constitution of the Zambia Cyber Incident Response Team and its functions, continue the existence of the Central Monitoring and Co-ordination Centre as well as provide for its designation, protection and registration of critical information and critical information infrastructure inter alia.[13] This Act is a representation of Zambia's attempt to mitigate cyber-crime as well as address cyber threats and establish a secure virtual environment in the country. The Act seeks to criminalize various forms of cyberattacks, establish institutional frameworks for cyber security as well as put mechanisms in place for the identification, investigation and prosecution of cybercrimes.

[13] Act 3 of 2025

2.2 ZAMBIA CYBER SECURITY AGENCY

An institutional framework refers to a structured set of formal and informal rules and practices that guide interactions and actions within a system.[14] It encompasses the legal and organizational arrangements that define how institutions function, interact and make decisions as well as ensure accountability and efficiency within an organization in the implementation of laws and policies. The Cybersecurity Act establishes various institutional such as the Zambia Cyber Security Agency and the Central Monitoring and Coordination Centre.

Section 3 of the Cybersecurity Act[15] establishes the Zambia Cybersecurity Agency in the office of the President which is responsible for the administration of the Act under the general direction of the President. This agency is responsible for the coordination of cyber security in the Zambia with its functions being stipulated under ***Section 4 of the Cybersecurity Act[16].*** The section stipulates that the agency has the role of coordinating activities relating to cyber security and cyber resilience, subject to the Zambia Security Surveillance Act 1998. Cyber resilience is defined under ***section 2 of the Cybersecurity Act***[17] as the ability to prepare for, respond to and recover from cyber-attacks, ensuring that essential functions continue despite adverse conditions. This means that the agency has the duty to continuously identify and mitigate potential cyber risks across virtual environments within its realm and jurisdiction. Another function of the agency is to take measures in response to cyber security incidents which may threaten critical information, critical information infrastructure and any information in Zambia that is likely to be affected by a cyber security incident. This means that the agency has the duty and function to have predefined response plans and a team that is adequately prepared to minimize damage and restore operations in the event that an attack does occur, invest in monitoring, detection, protection and recovery technology that would aid in treating a potential cyber threat or the after math of a cyber-attack and conduct a thorough analysis to understand the root cause of the cyber-attack among other things, these being the most prominent ones. The third function of the agency under the Act is to disseminate information on cyber threats and vulnerabilities. This illustrates the fact that the Zambia Cyber Security Agency

[14] Institutional framework-an overview accessed on https://www.sciencedirect.com on 13/08/2025
[15] Act 3 of 2025
[16] Act 3 of 2025
[17] Act 3 of 2025

has the duty to share adequate information, with enough clarity and in an organized manner, on potential cyber threats and the ways in which the targeted audience would be able to prepare and respond to the said cyber-attack. It is clearly notable, with the emerging of artificial intelligence and other technologies like ransomware, the potential of cyber threats and cyber-attacks have increased and so it is important for people to have adequate information on ways in which they can detect, prevent and respond to attacks more effectively. It also allows various stakeholders to make informed decisions and adapt defenses that would allow a minimization of damage.

The fourth function of the Zambia Cybersecurity Agency stipulated in the Act is to identify and ensure the protection of critical information and critical information infrastructure. Subsequent to delving into what this means, it is imperative to illustrate what is meant by these terms as defined by ***section 2 of the Cybersecurity Act***[18]***.*** 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-personal data that is managed or transmitted through critical information infrastructure or processed by a controller , information relating to any research and development in relation to critical information infrastructure, information needed to operate critical information infrastructure or 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- is vital to a country such that the incapacity or destruction of or interference with the computer system, device or computer data would have a debilitating impact on national security, economy, public health or safety or supports the processing of critical information or an essential service. This means that the agency has the duty to safeguard assets used for public safety and health, networks, systems, processes and information essential to national security, economic stability, public health and safety of the country at large. This may involve identification of critical infrastructure and conduction of a vulnerability assessment to allow for targeted defenses that would mitigate risks efficiently. Another function of the agency is to regulate the conduct of cyber security service providers which involves constructing legal and administrative frameworks that would ensure that the service providers meet cybersecurity standards that are set out

[18] Act 3 of 2025

in the Cybersecurity Act and deliver services that would not cause harm to the virtual environment in the country. The last function that will be spoken about in this piece of writing is the function of the Zambia Cybersecurity Agency to adopt standards for cybersecurity products and services and certify cyber security products and services. This involves adopting established standards and implementing them into established frameworks and guidelines in order to ensure efficiency in the delivery of cyber security goods and services.

2.3 CENTRAL MONITORING COORDINATION CENTRE

The other institutional framework established by the Cybersecurity Act is the Central Monitoring Coordination Centre which is established by ***section 21 of the Cybersecurity Act***[19]. According to subsection 2 of the same section, the center shall be the sole facility in the country through which lawful interceptions shall be effected and intercepted communication and call related information of an interception target shall be forwarded. This means that the center is the only body in the country that is in charge of state authorized surveillance of communications. It is the only hub that has been given authority by law to make call or message interceptions and all service providers are required by law to take their interception requests through the center's infrastructure. This is established under ***section 39(1) of the Cybersecurity Act*** [20] which states that an electronic communication service provider is obliged to provide one or more interfaces from which an intercepted communication shall be transmitted to the Center and if they do not comply, are liable on conviction to a fine not exceeding ten million penalty units.

The Central Monitoring Coordination Center is a necessary institutional framework as it allows for the mass surveillance of interceptions made within the cyber space without robust safeguards that would potentially lead to the violation of the right to privacy under ***Article 17 of The Constitution***[21]***.***

2.4 KEY PROVISONS UNDER THE CYBERSECURITY ACT NO.3 OF 2025

In terms of key provisions under the Act, these clauses hold more importance compared to other clauses in the Act. They are considered essential for defining the core parts of the Act itself. Some of the key provisions of the Act include section 3

[19] Act 3 of 2025
[20] Act 3 of 2025
[21] Act 2 of 2016

which establishes the Zambia Cyber Security Agency aforementioned as an institutional framework. Another key provision includes ***section 6***[22] of the act which establishes the Zambia Cyber Incident Response Team under the Zambia Cyber Security Agency. This team's purpose, among other things, is to serve as a first point of contact with reference to the handling of cyber incidents and communications between local, regional and international cyber security incident response teams as well as undertake national cyber security risk assessments, participate in regional and international computer emergency response team groups and establish a cyber security incident monitoring and response system. Another key provision includes ***section 42 of the Cybersecurity Act***[23] which prohibits the providing of cyber security services without a license and the same section penalizes such acts with a liability of a fine not exceeding five hundred thousand penalty units or imprisonment for a term not exceeding five years or to both. This is to ensure that there is a systematic order of services being provided and that the standard of the service is up to par with the Agency that authorizes the provision of cyber security services. Other key provisions include the penalties that are attached to the violation or non-adherence of the requirements under the Act. This is to ensure that parties who do not strictly adhere to the provisions under the act and their necessary requirements face consequences as non-adherence could lead to serious damage to the cyber space as well as the nation at large, seeing as the country is developing and adapting to the digital era of life.

2.5 ENFORCEMENT MECHANISMS UNDER THE CYBERSECURITY ACT

Enforcement mechanisms involve a set of rules and regulations as well as measures that are put in place in order to ensure compliance of the provisions of a particular set of laws. In the Cybersecurity Act no.3 of 2025, some of the enforcement mechanisms that are put in place include the power of the Central Monitoring Coordination Centre to intercept communication without a warrant if they see a potential threat to the virtual environment. This gives the Center discretion to conduct surveillance without safeguards. Another example of the enforcement mechanisms that are contained in the Cybersecurity Act include the power of the institutional frameworks under the Act to investigate cyber incidents. Another enforcement mechanism that exists is the

[22] Act 3 of 2025
[23] Act 3 of 2025

emergency cyber measures which allow for the immediate response to cyber threats and incidents.

2.6 THE DATA PROTECTION ACT NO.3 OF 2021

The Data Protection Act no.3 of 2021 was enacted for the sole purpose of protecting personal information and regulating the digital space in Zambia. This Act seeks to regulate the processing of personal data, protect privacy rights of data subjects as well as provide a written demonstration of the ways in which data needs to be protected. According to its short title, the Act is supposed to provide an effective system for the use and protection of personal data, regulate the collection, use, transmission, storage and otherwise processing of personal data, establishing the office of the Data Protection Commissioner and provide for its functions , the registration of data controllers and licensing of data auditors, provide for the duties of data controllers and data processors, provide for the duties of data controllers and data processors, provide for the rights of data subjects and provide for matters connected with or incidental to the foregoing.

2.7 INSTITUTIONAL FRAMEWORKS UNDER THE DATA PROTECTION ACT

The institutional frameworks established under the Data Protection Act no.3 of 2021 include the Office of the Data Protection Commissioner which is brought out under ***section 4 of the Data Protection Act***[24] which stipulates that under the Ministry responsible for communications the Office of the Data Protection Commissioner is established and is responsible for the regulation of data protection and privacy in Zambia. Subsection 2 of the same section in the Act brings out the functions of the Data Protection Commission, the first being to register controllers and data processors. A data processor is defined under ***section 2 of the Data Protection Act***[25] as a person, or a private or public body that processes personal data for and on behalf of and under the instruction of a data controller. The second function of the Commission is to license data auditors. Data auditing is the process of monitoring data creation, collection, usage, storage and destruction.[26] This means that the commission has the duty to give licenses to the people who monitor data collection, creation, usage, storage and destruction. The third function is to disseminate information and

[24] Act 3 of 2021

[25] Act 3 of 2021

[26] Data auditing and analytics accessed at https://www.secoda.com on 13/08/2025

promote the participation of stakeholders in the process of data protection in Zambia. This means that the Commission must undertake public awareness campaigns, publish guides such as registration guidelines for data controllers and processors and materials that help various stakeholders understand the legal requirements for data protection. In terms of promoting participation of stakeholders, the Commission can carry out surveys to incorporate stakeholder views and collaboratively develop data protection strategies. Other functions of the Commission include advising the government on matters relating to data protection, keeping and maintaining a register of data controllers, data processors and data auditors, represent the government internationally on matters relating to data protection, conduct research and development relating to data protection and ensure proper and effective coordination and collaboration with similar regional and international authorities.

2.8 KEY PROVISIONS UNDER THE DATA PROTECTION ACT

In terms of key provisions, some of the key provisions that exist under the Data Protection Act no.3 of 2021 include section 4 which establishes the Office of the Data Protection Commissioner which is a key institution under the concept of data protection in the country. Other key provisions are stipulated under ***Part IX of the Data Protection Act***[27]***.*** These provisions are stipulated as rights of the data subject. A data subject is defined under ***section 2 of the Data Protection Act***[28] as an individual from or in respect of whom, personal information is processed. Some of these rights include the right of access and notification stipulated under ***section 58 of the Data Protection Act***[29] which states that a data subject has the right to obtain, from the data controller, confirmation as to whether or not personal data concerning that data subject is being processed. This means that an individual has the right to be notified whenever their personal information and data is being processed. Another right under Part IX is stipulated under ***section 59 of the Data Protection Act***[30] which stipulates that a data subject has the right to, rectification of inaccurate personal data concerning the data subject as soon as practicable. Rectification is the correction of a document if it does not correctly express the common intention of the parties to it.[31] This right stipulates

[27] Act 3 of 2021
[28] Act 3 of 2021
[29] Act 3 of 2021
[30] Act 3 of 2021
[31] Elizabeth A Martin, Oxford Dictionary of Law (7th edition)

that the data subject has the right to change information pertaining to them if that information is not an accurate representation of what they wish for it to represent. The third right is the right to erasure which is stipulated under ***section 60 of the Data Protection Act***[32] which states that the data subject has the right to erasure of personal data of that data subject as soon as practicable and the data controller shall have the obligation to erase personal data without undue delay where the personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed, where the data subject or person holding parental responsibility, where the data subject is a child, withdraws consent and there is no other legal ground for the processing of that data, where the data subject objects to the processing and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing unless the data controller is otherwise permitted by the provisions of this Act, among other things.

2.9 ENFORCEMENTS MECHANISMS UNDER THE DATA PROTECTION ACT

When it comes to enforcement mechanisms, the Data Protection Act of Zambia has set some out in order to ensure that the provisions of the Act are complied with. According to ***section 4 of the Data Protection Act***[33], the Commission has the power to oversee and regulate as well as ensure compliance with the Act as it handles the registration, investigations, complaints as well as promotes stakeholder participation. Another enforcement mechanism is seen under ***section 7 of the Data Protection Act***[34] which states that the Civil Service Commission may appoint a suitably qualified person to be an inspector for the purposes of ensuring compliance with this Act. This is a clear representation of how the Data Protection Act employs enforcement mechanisms. Another enforcement mechanism that exists under the Act is stipulated under ***section 18 of the Data Protection Act***[35] which states that a body corporate that contravenes the provisions of this Part commits and offence and is liable on conviction to a fine not exceeding one hundred million penalty units or two percent of annual turnover of the preceding financial year, whichever is higher. Subsection 2 further goes to state that if the offence is committed by a natural person, that person

[32] Act 3 of 2021
[33] Act 3 of 2021
[34] Act 3 of 2021
[35] Act 3 of 2021

shall be liable on conviction to a fine not exceeding one million penalty units or to imprisonment for a term not exceeding five years or both.

3.0 THE PROTECTION OF PERSONAL INFORMATION BY THE DATA PROTECTION ACT

When it comes to the aspect of protecting personal information, the Data Protection Act no.3 of 2021 protects personal information through a comprehensive set of measures that are designed to regulate the collection, use, transmission, storage and processing of personal information. The Data Protection Act as a legal framework has its core in principles stemming from The Constitution of Zambia being Act no.2 of 2016. ***Article 17 of the Constitution***[36] upholds and respects the right to privacy which includes protection against unlawful searches and seizures as well as communication interception. The Act requires that data must be processed lawfully, fairly and transparently and the collection of said data must be for explicit and genuine purposes, only limited to what is necessary. This is due to the fact that personal data is a very delicate aspect and in order to uphold the right to privacy, the collection and use of personal data must only be done when necessary. The Data Protection Act allows the subjects of the data being used to give consent to their data being used in order to allow the data subjects to have an overall say on how their personal information is being used. The Act also give data subjects various rights over their data like correct inaccuracies, erasure of their data as well as data portability. The Act gives data controllers a duty to notify the Data Protection Commissioner any security breach affecting personal data and notify affected data subjects as soon as practicable. The Data Protection Commissioner, with authority from the Act, has the power to issue a code of conduct that is binding on controllers, processors as well as data auditors in order to ensure strict compliance with the provisions under the Act, thereby ensuring protection of personal information. Another way in which the Act provides for protection of personal information ensure transparency and accountability, in the sense that it places a requirement on data controllers to provide clear information about the processing activities that will be undertaken to the data subjects and by doing so, allowing individuals to exercise their rights. According to ***section 70 of the Data Protection Act***[37], a data controller shall process and store personal data on a server

[36] Act 2 of 2016
[37] Act 3 of 2021

or data center within Zambia, however the Minister may prescribe categories of personal data that may be stored outside Zambia. This is subject to the fact that the data subject would need to give consent to the above and as such, promoting protection of personal information.

3.1 CONCLUSION

Zambia's legal framework for cyber security and data protection, while being very progressive, faces some significant pitfalls and drawbacks in terms of structure and operation. In terms of Cybersecurity, the Act establishes important institutions as well as their various roles however it fails to explain in depth to what extent the structure and operations run. In terms of Data Protection, the legal framework that is put in place in Zambia creates rights for data subjects while at the same time, undermining those rights by giving more power to the Data Commissioner and creating various exceptions. These gaps hinder effective protection of personal information and the cyber space at large. The next chapter will be assessing the extent to which the current legal framework meets international standards.

CHAPTER THREE

THE EXTENT TO WHICH ZAMBIA'S LEGAL FRAMEWORK ALIGNS WITH INTERNATIONAL SET STANDARDS SUCH AS THE GDPR, BUDAPEST CONVENTION AND THE MALABO CONVENTION IN GOVERNING CYBER SECURITY AND DATA PROTECTION

3.2 INTRODUCTION

This chapter provides an elaborate assessment of the extent to which Zambia's legal framework aligns with international set standards and best practices like the GDPR of the European Union, the Budapest Convention and the Malabo Convention in governing cyber security and data protection. It critically assesses Zambia's legislation and institutional frameworks against each of the various conventions, clearly indicating and highlighting areas of convergence and divergence.

3.3 GENERAL DATA PROTECTION REGULATION

The General Data Protection Regulation, herein referred to as the GDPR, is a piece of legislation that was enacted by the European Union with the purpose of protecting individuals' fundamental rights to privacy and allow the people more control over their personal information and data while ensuring organizations handle the data responsibly and transparently. The regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.[38] It is considered to be the global set standard for data protection frameworks across the world as it establishes stringent requirements for data processing. Among other things, it encompasses lawful basis requirements, rights awarded to data subjects, security measures and cross border data transfer restrictions. The GDPR applies to organizations, regardless of their location, that processes personal data of members or residents of the European Union.

3.3.1 PERSONAL DATA UNDER THE GENERAL DATA PROTECTION REGULATION

Personal data is defined as any information relating to an identified or identifiable natural person (data subject).[39] The GDPR places a requirement that personal data

[38] Article 1 of the General Data Protection Regulation

[39] Article 4 of the General Data Protection Regulation

shall be processed lawfully, fairly and in a transparent manner in relation to the data subject which is stipulated under ***Article 5(a)***.[40] This means that even though organizations or institutions have the power or freedom to process personal data belonging to individuals, this processing must be done lawfully and in a transparent manner, allowing the owner of the information to have a fair say in what happens to their personal information and data. The GDPR also requires, under ***Article 5(b)***[41] that if personal data is collected, it must be collected for specified, explicit and legitimate purposes and not further processed that is incompatible with those purposes. This means that personal data must be collected for the right reasons and the way in which that data is processed must not stray away from those purposes. According to ***Article 5(c)***[42], personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. This means that the data that is collected must be sufficient to properly fulfil the purpose for which it is being processed. It also means that the data must have a direct and clear connection to the purpose. An example of this can be seen through music streaming services as all that's required from people that sue their services is their music preferences and nothing else like their date of birth or nationality. This sub article practically speaks on the matter of data minimisation which is an important aspect of data protection as it reduces the risk of data breaches and misuse of data. ***Article 5(2)***[43] speaks on the fact that the data controller has responsibility over, and is able to demonstrate compliance with the first sub article. A controller has been defined under ***Article 4***[44] as the natural or legal person, public authority, agency or other body which alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by the Union or Member State law, the controller or the specific criteria for its nomination may be provided for by the Union or Member State law. According to ***Article 6***[45] the GDPR states that processing shall be lawful only if and to the extent that at least one of the following applies; the data subject has given consent to the processing of his or her personal data for one or more specific purposes, processing is necessary for the

[40] General Data Protection Regulation
[41] General Data Protection Regulation
[42] General Data Protection Regulation
[43] General Data Protection Regulation
[44] General Data Protection Regulation
[45] General Data Protection Regulation

performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract, processing is necessary for the compliance with a legal obligation to which the controller is subject, processing is necessary in order to protect the vital interests of the data subject or of another natural person, processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller and where processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden y the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

3.3.2 DATA SUBJECT RIGHTS UNDER THE GENERAL DATA PROTECTION REGULATION

The GDPR grants a data subject various personal rights in relation to their personal data and this is in order to ensure that they have a say in the way that their personal information is handled, stored and processed, among other things. The first right includes the right to access. ***Article 15***[46] stipulates that a data subject shall have the right of obtaining from the data controller confirmation as to whether or not personal data concerning him or her are being processed and if that is the case, the data subject is allowed access to the personal information and information such as the purpose for which said information is being processed, the categories of personal data concerned, the recipients or categories of recipients who will be receiving the personal data, if it is possible, the envisaged period for which the personal data will be stored and where the personal data are not collected from the data subject, any available information as to their source. This article clearly stipulates that the data subject has the right to a copy of their data and information as well as how it is being processed as well as knowledge on how long their personal data is to be stored and processed. Another right that is afforded to the data subject is the right to rectification. Rectification is the correction of a document if it does not correctly express the common intention of the parties to it.[47] ***Article 16***[48] states that the data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data

[46] General Data Protection Regulation
[47] E Martin, Oxford Dictionary of law (7th edition, Oxford University Press, 2009) 457
[48] General Data Protection Regulation

concerning him or her. This implies that the data subject has the right to change of the information that is being processed in a situation where that information is inaccurate. Sub article 2 further states that when taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed including by means of providing a supplementary statement. This means that the data subject has the right to ask an organization that is processing their data to add any missing information and the organization has no option to comply without delay. Another right that is given to data subjects is the right to erasure which is stipulated under ***Article 17***[49], which stipulates that the data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies; the personal data is no longer necessary in relation to the purposes for which they were collected or otherwise processed, the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1) and where there is no legal ground for processing, the data subject objects to the processing and there are no legitimate grounds for the processing, where the data has been unlawfully processed. This in itself is a representation of how the data subject is given freedom over their personal information and how much consent is very important for organizations and countries that are privy to the GDPR. Another right that is given to the data subject by the GDPR is the right to data portability which is stipulated under ***Article 20***.[50] It states that the data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to the controller , in a structured, commonly used and machine readable format and have the right to transmit those data to another controller to which the personal data have been provided where; the processing is based on consent pursuant to point (a) of Article 6(1) among other things. This basically means that the data subject has the right to have their data provided in a format that is able to be read by other controllers in a situation where the data subject wishes for their data to be taken to another data controller. Lastly but not the least, another right that is granted to data subjects is the right to object which is stipulated under ***Article 21***.[51] This article states that the data subject shall have the right to object on grounds relating to his or

[49] General Data Protection Regulation
[50] General Data Protection Regulation
[51] General Data Protection Regulation

her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which overrides the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims. This basically illustrates that the data subject has the right to stop their data from being processed and if that data is to be further processed, the data controller would need to provide extremely compelling reasons and those grounds would need to be legitimate as well as the further processing of that information would be infringing on the interests and freedoms of the data subject. Sub article 2 further goes on to say that where personal data is processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing. This means that when personal data is used for marketing purposes the data subject has the right to object to the processing of his data at any time and this includes not only direct marketing activities but also profiling that is done in relation to said marketing. upon the data subject objecting to their information being used, the organization that is processing the data must immediately stop using their data and this is with no exceptions. An example can be seen in where an individual receives promotional emails from a company advertising its products. The individual exercises their right to object and sends a request to stop receiving those emails and immediately, the company has an obligation to cease sending those marketing emails. Another example of this is where a person's online behaviour is tracked and analysed to create a profile used for targeted ads. If the person objects to this profiling as part of direct marketing, the company must stop using their data for this purpose and no longer target them with ads based on such profiling.

These provisions collectively ensure that there are strong protections for individuals' personal data and impose rigorous obligations on organizations processing such data.

3.4 BUDAPEST CONVENTION ON CYBERCRIME- TREATY 185

The Budapest Convention on Cybercrime is the first international treaty that was aimed at addressing matters of cybersecurity and cybercrime as well as improving investigative techniques and increase international cooperation among countries to

effectively combat crimes committed via the internet and on the virtual space. It is a framework that permits hundreds of practitioners from party states to share experience and create relationships that facilitate cooperation in specific cases, including in emergency situations, beyond the specific provisions foreseen in the convention.[52] Some of the key objectives of the Budapest Convention are the criminalization of specific cyber related offenses such as illegal access to data, data interference and computer related fraud, providing procedural law tools to facilitate investigation and securing electronic evidence and enhancing international police and judicial cooperation on cybercrime and electronic evidence.

3.4.1 KEY PROVISIONS UNDER THE BUDAPEST CONVENTION- TREATY 185

In terms of key provisions, ***Article 2***[53] speaks on the criminalization of illegal access.it states that each party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system. This Article shows how there is need to obtain consent before accessing one's computer system and the lack of consent would indicate a criminal offence. Another key provision in the Budapest Convention is one that speaks on illegal interception. ***Article 3***[54] states that each party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means of non-public transmissions of computer data to from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to computer system that is connected to another computer system. This article prohibits the unauthorized interception of non-public data transmissions allowing the owner of the data some form of protection from illegal interception of data. The next key provision is ***Article 5***[55] which speaks on system interference. It states that each party shall adopt such

[52] About the Convention-Cybercrime available at https://www.coe.int accessed on 16/09/2025
[53] Budapest Convention-Treaty 185
[54] Budapest Convention- Treaty 185
[55] Budapest Convention- Treaty 185

legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

These provisions, amongst others, provide a comprehensive framework for criminalizing cyber offences, enabling cross border investigations and balancing security with rights. Regardless of the fact that Zambia is neither a signatory nor a party to this treaty, adopting the principles under this treaty would enhance Zambia's cyber security laws.

3.5 THE MALABO CONVENTION

The African Union Convention on Cybersecurity and Personal Data Protection, also known as the Malabo Convention is a treaty that was created and adopted by the African Union. It establishes a comprehensive legal framework for cybersecurity, electronic transactions and personal data protection across Africa as a continent. The treaty aims to criminalise certain cyber acts like hacking, identity theft and cyber fraud while promoting international cooperation for investigation and prosecution of cybercrime. It also mandates member states to create legal frameworks and data protection authorities to ensure the secure processing and storage of personal data. According to the preamble[56]it states that the Convention on the Establishment of a Legal Framework for Cyber security and Personal Data Protection embodies the existing commitments of African Union Member States at sub regional, regional and international levels to build the information society. The Malabo Convention also provides legal recognition for electronic communications and signatures to facilitate secure electronic commerce. Zambia is a member state and has ratified the Malabo Convention.

3.5.1 KEY PROVISIONS UNDER THE MALABO CONVENTION

The Malabo Convention contains many key provisions that highlight matters of cyber security and data protection. Some of them include the criminalization of cyber offenses. The Convention requires that member states criminalize specific cybercrimes in order to ensure harmonization of the legal approach that member states have in order to combat cyber threats across Africa. This is stipulated under

[56] African Union Convention on Cyber Security and Personal Data Protection

Article 28 of the Convention. Under key provision under the Malabo Convention is the definition section as it defines many key terms elaborately. One of the definitions include that of the consent of the data subject which means any manifestation of express, unequivocal, free, specific and informed will by which the data subject or his/her legal, judicial or treaty representation accepts that his/her personal data be subjected to manual or electronic processing. This shows clearly what consent is and through whom it may be given. Another key provision is one that requires member states to create and develop national cybersecurity strategies. This is seen under ***Article 24(2)***[57] which states that state parties shall adopt the strategies they deem appropriate and adequate to implement the national cyber security policy, particularly in the area of legislative reform development, sensitization and capacity- building, public-private partnership and international cooperation, among other things. Such strategies shall define organizational structures, set objectives and timeframes for successful implementation of the cyber security policy and lay the foundation for effective management of cyber security incidents and international cooperation. This means that states are required to align with the Convention's principles, making sure that cybercrimes are legally defined and enforceable.

In terms of other key provisions, the Convention clearly highlights data subject rights that are afforded to data subjects in relation to how their personal data is being processed. These rights are stipulated under Section IV of the Convention and these rights include the right to object, the right to rectification, the right to access and the right to information. The right to information which is stipulated under ***Article 16***[58] states that the data controller must provide the data subject with information such as his/her identity and of his/her representative, the purposes of the processing of their data, categories of the data involved, recipients to which the data might be disclosed, the capacity to request to be removed from the file, the period for which the data is to be stored among other things. These rights ensure transparency and control over how personal information is used. Another key provision under Convention is one that speaks on data processing principles. This is stipulated under Article 13[59] which brings out the basic principles relating to the processing of personal data. The first

[57] African Union Convention on Cyber Security and Personal Data Protection
[58] African Union Convention on Cyber Security and Personal Data Protection
[59] African Union Convention on Cyber Security and Personal Data Protection

principle under this Article is the principle of consent and legitimacy of data processing which states that processing of personal data shall be deemed to be legitimate where the data subject has given their consent. The second principle if the principle of lawfulness and fairness of personal data processing which stipulates that the collection, recording, processing, storage and transmission of personal data shall be undertaken lawfully, fairly and non- fraudulently. The third principle is the principle of purpose, relevance and storage of processed personal data which states that data collection shall be undertaken for specific, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. The fourth principle is the principle of accuracy of personal data which stipulates that data collected shall be accurate and where necessary, kept up to date. This keeps from having inaccurate information being processed. The fifth principle is the principle of confidentiality and security of personal data processing which states that personal data shall be processed confidentially and protected, in particular where the processing involves transmission of the data over a network.

In term of electronic transactions, the Convention has a legal recognition of electronic communications as it provides guidelines for recognizing electronic signatures, contracts and communications as legally valid, fostering trust in e- commerce and digital trade. Another key provision is one that speaks on cross border e- commerce. ***Article 2***[60] states that member states shall ensure that e- commerce activities shall be exercised freely in all member states ratifying or acceding to this Convention except gambling, even in the form of legally authorized betting and lotteries, legal representation and assistance activities and activities exercised by notaries or equivalent authorities in application of extant texts.

3.6 THE EXTENT OF ALIGNMENT OF THE ZAMBIAN LEGAL FRAMEWORK AND THE INTERNATIONAL STANDARDS

In terms of alignment of the Data Protection Act with the GDPR, the Act incorporates several principles of the GDPR such as the right of data subjects to access, rectify and erase their personal data, the requirement for lawful, fair and transparent processing limited to explicit and legitimate purpose as well as mandatory notification of security breaches to both the regulator and affected individuals. The Act however diverges in

[60] African Union Convention on Cyber Security and Personal Data Protection

terms of the institutional setup and some enforcement mechanisms, in that that Data Protection Commissioner in Zambia operates under a Ministry which could potentially undermine their authority and autonomy. The Act also allows the Commissioner to override the consent of the data subject in certain situations and this conflicts with the GDPR's strong emphasis the data subject's consent and control. The Data Protection Act is also ambiguous in that the use of the term personal us in relation to processing is very vague unlike the GDPR's clear description.

In terms of alignment of the Cybersecurity Act with the Budapest Convention, Act no.3 of 2025 aligns in that it has established criminal offences related to cyber incidents, created institutional frameworks such as the Zambia Cyber Security Agency. The Act however diverges in that there is ambiguity in operational details of institutions like the Central Monitoring Coordination Centre and this raises questions as to the safeguards against abuse and this is more regulated in the Budapest Convention.

In terms of both Act no.3 of 2021 and Act no.3 of 2025 aligning with the Malabo Convention, there is a hinderance by the institutional limitations such as the lack of autonomy for regulatory bodies as well as limited public awareness.

3.7 CONCLUSION

Zambia's legal framework shows strong effort to align with international standards on data protection and cybersecurity as it incorporates principles from international standards such as the GDPR, Budapest Convention and the Malabo Convention. However, regardless of these efforts, there are still gaps that remain in the institutional frameworks, clarity of the scope as well as enforcement capacities. Bridging these gaps is important in order to enhance protection of personal data and cyber space. The next chapter will be illustrating the importance and the need for Zambia's legal framework to align with international set standards.

CHAPTER FOUR

THE NEED FOR ZAMBIA'S LEGAL FRAMEWORK TO ALIGN WITH INTERNATIONAL SET STRANDARDS SUCH AS THE GDPR, BUDAPEST CONVENTION AND THE MALABO CONVENTION IN GOVERNING CYBER SECURITY AND DATA PROTECTION

4.0 INTRODUCTION

This chapter shall provide a detailed examination of why it is imperative that Zambia's legal framework governing cyber security and data protection must align with international set standards such as the GDPR, Budapest Convention and the Malabo Convention. It will explicitly highlight the benefits of the two Acts that govern cyber security and data protection in Zambia aligning with the international set standards, highlighting how through the alignment, Zambia could achieve high standards of cyber security and data protection and comparing these with the pitfalls of non-alignment.

4.1 GENERAL ANALYSIS OF THE INTERNATIONAL STANDARDS

4.1.1GENERAL DATA PROTECTION REGULATION (GDPR)

The GDPR provides a robust framework for data protection, emphasizing important principles such as transparency amongst the data subjects and the data controllers in the way in which the data controller uses the personal data belonging to the data subject. It also emphasizes principles like accountability and user consent in the sense that it prioritizes consent of the data subject before any use in which the data may need to be used. Zambia has high chances of benefiting from adopting similar provisions as those contained in the GDPR especially in the sector of defining roles and responsibilities of data controllers and processors as well as establishing clear rights and freedoms of data subjects. These rights include the right to access which entails that individuals can request access to their information, the right to rectification which entails that individuals have the right to ask the data controllers to edit their information if it is not accurately presented, the right to erasure which entails that individuals can request that their information be deleted under certain conditions as well as the right to object which entails that individuals can object to having their data processed in certain situations. The GDPR has set a high standard for data protection as it emphasizes the importance of individual rights regarding personal data. It also places a need for organizations to implement robust data protection measures in order

to ensure that the people that fall under their organization are heavily protected and understand their rights under the Regulation.

4.1.2 BUDAPEST CONVENTION

The Budapest Convention emphasizes the need for criminalization of specific cyber offenses and the establishment of procedures for the purposes of international cooperation. The Convention outlines a number of criminal offenses such as offenses related to computer systems, data and illegal access of various digital platforms, data and system interference. It establishes rules for investigating and prosecuting cybercrimes and breaches of various provisions under the Convention and this includes expedited preservation of stored data, production orders, search and seizure of computer data and real time collection of traffic data. The Budapest Convention also highlights how different countries can exercise their jurisdiction when it comes to enforcing the provisions of the Budapest Convention. The Budapest Convention functions as a mutual legal assistance treaty, streamlining cooperation in investigations and prosecutions. Aligning with the Budapest Convention would enable the country to better address cyber-crimes and facilitate collaboration with other nations, enhancing its overall cyber security posture.

4.1.3 MALABO CONVENTION

The Malabo Convention is an African treaty that establishes a comprehensive legal framework or cybersecurity, electronic transactions and personal data protection across African nations. The convention criminalizes cyber offenses such as hacking, identity theft and cyber fraud while promoting international cooperation for investigation of breaches of the articles of the convention as well as prosecution of the different cybercrimes. It sets guidelines for the protection of personal data, ensuring that individuals' privacy is protected and it encourages cooperation among member states to combat cybercrime and enhance cybersecurity measures. This Convention mandates the establishment of institutions and procedures to identify, respond to cybersecurity incidents and promote international cooperation among African countries for investigating and prosecuting cybercrimes. The Malabo Convention requires the different countries to establish legal frameworks to protect fundamental rights and public freedoms, in particular personal data privacy. It also requires that member states create independent national data protection authorities tasked with ensuring proper regulation of data processing, it emphasizes principles such as

consent, lawfulness, confidentiality and transparency in personal data processing and lastly it addresses the rights of individuals concerning the protection of their personal data and information.

4.2 THE NEED FOR ALIGNMENT OF ZAMBIA'S LEGAL FRAMEWORK ON CYBER SECURITY AND DATA PROTECTION WITH INTERNATIONAL STANDARDS

Zambia increasingly adopts digital technologies as she navigates the ever changing and fast-growing economy which has evolved highly and has taken effect on the virtual platform. As a result of this, the need for very effective laws governing cyber security and data protection has increased drastically as it is exposed to more cyber threats and data privacy challenges. This gave rise to the enactment of the Cybersecurity Act no.3 of 2025 and the Data Protection Act no.2 of 2021 which attempted to address and tackle the vast growing issues relating to cyber security and data protection. Regardless of the enactment of these laws, there are still inadequacies in these Acts that can be mended through the alignment of these Acts with international conventions and standards such as the GDPR, Budapest Convention and the Malabo Convention.

4.2.1 ENHANCEMENT OF DATA PROTECTION AND SECURITY

As already established, there exist various international standards, conventions and documents that exist in relation to data protection, however this study focuses mostly on the GDPR which contains regulations on the protection of personal data and the Malabo Convention which contains clauses on both cyber security and data protection

and it applies for African countries that have ratified and are parties to it while the GDPR applies to European countries as it was created by the European Union. The GDPR contains strong regulations that ensure that personal information and data is stored, processed and utilised in a prescribed manner and is done in a lawful manner. The sanctions that are contained in the GDPR are very effective as they ensure that the compliance of data controllers to the provisions of the GDPR is strict in order to ensure that the rights of the data subject are not infringed in the use, collection or processing of their personal information. The same could be applied for the part of the Malabo Convention that addresses the protection of personal data and information. The Malabo Convention addresses the rights of individuals concerning the protection of their personal data and information in a manner that is understood and vast, it

covers a wide range of situations in which one's personal data is being used and clearly lays out their rights as data subjects wherever their personal data is concerned. The Malabo Convention ensures that consent overrides purpose when personal data is being used, the use of that personal data is for a specific purpose which indicates a limitation. In relation to data protection, the Malabo Convention mandates secure processing and storing of personal information and data. By aligning the Data Protection Act with these instruments and standards, Zambia would enhance her data protection by ensuring robust safeguards for personal information belonging to individuals, some consistency in the global standard of protecting information as well as transparency in the way that personal information is handled and processed.

4.2.2 IMPROVEMENT OF CYBERSECURITY

The Budapest Convention, which was established in Europe, provides an internationally recognized criminal law legal framework and it covers a wide range of definitions, clearly highlighting different cyber-crimes and their sanctions. This is a good initiative as it ensures that a wide variety of cybercrimes are encompassed, giving people vast knowledge of what is legal and what is illegal on the cyber space. The Budapest Convention enhances investigative capabilities by providing tools for securing electronic evidence and criminalizes specific offenses such as the illegal access and interception of a cyber space, data and system interference, copyright violations and offenses related to child pornography. The Budapest Convention also establishes liability for aiding and abetting offenses like data interference, forgery, computer related fraud and other related offenses. It also places requirements for protecting human rights and freedoms when it comes to the cyber security. The Malabo Convention also contains provisions on cybersecurity which criminalise a wide range of cyber offenses such as hacking, identity theft, cyber fraud, attacks on computer systems and data breaches. It also outlines procedures for investigating and prosecuting cybercrimes, giving a clear description on how to deal with the breach of certain crimes and the sanctions that would be placed on the people that breach the crimes stipulated in the Malabo Convention. Regardless of the fact that these Conventions are applied in different regions, they apply the same principles in relation to cybersecurity and cybercrimes as they also emphasise on harmonization of national laws in order to promote international cooperation in protecting the cyber space. Considering the fact that Zambia is a party to the Malabo Convention, it would be ideal

for her to adopt a lot of the ideals and principles stipulated in the Cybersecurity Act as it would allow for universal definitions of cybercrimes, the criminalisation of more acts, coordinated incident response mechanisms that would improve Zambia's resilience against cyber-attacks and enhanced enforcement of cybersecurity as these conventions have a wider, less ambiguous range of cybercrimes and stipulated sanctions for said crimes.

4.2.3 STRENGTHENING OF INSTITUTIONAL FRAMEWORKS

As already established, the bodies responsible for the enforcement of cybersecurity and data protection in Zambia are the Zambia Cybersecurity Agency and the Data Protection Commission respectively. One of the biggest issues that these institutions face is the aspect of absolute autonomy in their operations and this is due to the fact that the Acts establishing them does not give them absolute autonomy in their operations and in their finances. The Zambia Cybersecurity Agency is a body established under the Office of the President and it is responsible for the administration of the Cybersecurity Act under the direction of the President.[61] This shows how the Zambia Cybersecurity Agency is not able to fully exercise its powers as it is subject to direction from the office of the President and it is a clear indication that even if the Office of the President were to beach any of the provisions under the Cybersecurity Act, it would be difficult for the Agency to sanction the President as the President is in charge of the body. This also shows that the agency is not able to fully exercise their powers to the best of their abilities as the Act itself limits their powers by requiring them to seek consent from the President before acting upon anything related to cybersecurity. The Data Protection Commission is established in the Ministry responsible for communications and it is responsible for the regulation of data protection and privacy in the Republic.[62] This entails that the Data Protection Commission and the Data Protection Commissioner work under the directive of the Office of the Minister in charge of communications in the country. As established earlier, the Act is very unclear on who the minister in charge of communications is and where this ministry is, hence making it very hard to sanction the same ministry in a situation where there is a breach of certain provisions in the Act and when there is a need to impose the sanctions that are contained in the Act. Aligning the current

[61] Act 3 of 2025
[62] Act 3 of 2021

Cybersecurity Act and the Data Protection Act with the GDPR, Budapest Convention and the Malabo Convention encourages the establishment of autonomous, well-resourced regulatory bodies that are capable of ensuring that they carry out their duties diligently and effectively. They would be able to monitor compliance of the Act and impose the necessary sanctions and punishments on whoever breaches those provisions and the rights under the provisions and they would be able to investigate breaches thoroughly.

4.2.4 BOOSTING OF ECONOMIC GROWTH AND INVESTMENT

The world, as it develops in many different aspects, has developed the fast-growing use of technology for various reasons, some of which including cross border communication and international trade. As it stands, the current Cybersecurity Act and the Data Protection Act do not adequately provide for safeguards for international investors or local investors who would wish to invest in the companies and industries in the country. Outside of the institutional frameworks for both cybersecurity and data protection, the Acts themselves do not have strong and unambiguous safeguards to protect various stakeholders and considering the fact that the world is shifting into the digital era it is important for the country to align its laws with international standards in order to attract foreign investment. Foreign investment would boost the country's economy and having a legal framework that aligns with international standards would encourage this as an international investor is more likely to invest in a country that has strong cybersecurity laws and data protection laws as well as a country that shows a commitment to cybersecurity and data protection. In inhibiting the ideals contained in these various international standards, it will create an environment for the country in which foreign investors are free to invest and open their various companies into the country, thereby increasing the foreign currency in the country as well as increasing the employment rate and reducing the poverty levels. This is a clear indication how aligning with international standards has high economic benefits.

4.2.5 STRENGTHENING OF CONSUMER RIGHTS AND PROTECTIONS

It is important to note that international standards such as the GDPR make mention and emphasize consumer rights such as the right to access, the right to rectify as well

as the right to erase personal information and data. The Malabo Convention also places huge emphasis on the fact that data subjects are entitled to information on how their data is being used and the right to stop their data from being processed and this shows just how important consumer rights are and the high regard in which they are held. If Zambia aligns her laws on cybersecurity and data protection with these international standards like the GDPR and the Malabo Convention, the rights of consumers being the data subjects will be enhanced and there will be more safeguards for consumers and sanctions imposed on people and institutions who breach and go against the rights of the consumers. By adopting universally recognized frameworks, Zambia would be able to offer better protection for personal data, thereby enhancing public trust in digital services and it is crucial for fostering innovation and encouraging investment in the technology sector. It would also promote a culture of privacy and respect for personal data and personal information belonging to an individual whose information is being processed and used. This alignment with international standards is essential as we live in an era of time where cyber threats and data breaches are rampant and on high rise.

4.2.6 DIGITAL TRANSFORMATION AMPLIFIED

Considering the fact that Zambia embraces a digital platform for a lot of transactions taking after the fact that the world is shifting into a high percentage of digital transactions, it is important for the Republic to align its legal framework with international standards as it is critical for ensuring that digital services can be delivered safely and securely. The alignment with international standards of their legal framework can help facilitate the growth and development of electronic commerce, the development of digital banking as well as other sectors that are technology driven. Another sector is the sector of content creation, as Zambians are moving towards content creation for entertainment, recreation as well as a way of making money, the content creators would need strong safeguards ensuring that their information is being protected and that any violation of their rights would be punished and sanctioned.

4.2.7 ENHANCING LEGAL CERTAINTY AND CLARITY

Zambia ‘s legal framework on cybersecurity and data protection provide for thorough provisions that protect the people trying to enforce it however despite the fact that the

Act contains adverse provisions that aim to protect, these provisions are not elaborate enough and do not contain a clear understanding and interpretation of certain terms and important aspects. An example of this can be seen in the Data Protection Act which states under ***section 4***[63] that 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 meaning of the ministry in charge of communications is unclear as the Act does not clearly state which ministry this is. Aligning with the international standards provides a clear and predictable legal environment that benefits both individuals as well as businesses. In adopting a universally recognized frameworks like the GDPR, Budapest Convention and the Malabo Convention, Zambia is able to offer better protection for personal data, thereby enhancing public trust in digital services. The certainty in the legal frameworks is crucial for fostering innovation and encouraging investment in the technology sector.

4.3 GAPS AND SHORTCOMINGS OF THE CURRENT LEGAL FRAMEWORK GOVERNING CYBERSECURITY AND DATA PROTECTION

As already established, the Cybersecurity Act no.3 of 2025 and the Data Protection Act no.3 of 2021, in as much as they try to address many on-going legal problems across the digital space, they still have many shortcomings and gaps. One of these include the lack of clarity and autonomy in the institutional structures. This causes a weakness in enforcement of the provisions under the Act. Another shortcoming is the limited public awareness and technical capacity which restricts effective implementation. This is established in the sense that employees, some parts of leadership and the general public are not aware and do not fully understand the risks in terms of the nature and severity of cyber threats as well as the importance of protecting personal and sensitive data and information. They do not understand their role as stakeholders in terms of the simple preventative measures that they need to take in order to prevent their personal information and prevent cyber threats. They are not aware of the regulations that govern cybersecurity and data protection in terms of their rights and responsibilities under various data protection laws that exist and are enforceable in the country. In terms of it limiting effective implementation, when people lack awareness, they tend to act as the weakest link in the security chain, thereby

[63] Act 3 of 2021

giving rise to an influx of cyber threats. Another shortcoming in the two Acts is the ambiguities in legal provisions on data consent and derogations which undermine the protection of the users. These ambiguities in the Act make it difficult for users to adequately seek recourse as they may not be fully aware of which ways in which they can seek recourse and to which institutions they should visit to receive and seek said recourse.

4.4 PITFALLS AND CONSEQUENCES OF NON-ALIGNMENT

In a situation where Zambia chooses not to align her cybersecurity Act and her data protection Act with the international standards such as the GDPR, Malabo Convention and the Budapest Convention, some of the consequences include increased vulnerability to data breaches and cyber exploitation in the sense that the laws governing cybersecurity and data protection do not contain safeguards strong enough to protect users. Another consequence includes the fact that citizens and international investors and partners will lose trust in the virtual market in Zambia as the safeguards are not strong enough for adequate protection. Another pitfall that comes from non-alignment of the legal framework governing cybersecurity and data protection with international standards include economic setbacks due to barriers in cross-border digital business and compliance failures. Finally, another consequence that stems from non-alignment of the two Acts with international standards include the legal uncertainties that complicate enforcement and dispute resolution. Due to the fact that the Act contains so many ambiguities, it poses a challenge on the enforcers of the law in posing sanctions and punishments.

4.5 CONCLUSION

Aligning Zambia's cybersecurity and data protection framework with international standards is essential and necessary in order to safeguard the rights of citizens as well as enhancing national security and improving economic prospects in the digital age. It is essential as it would bridge the gap and current deficiencies, fortify institutional capacities and put Zambia at a position that allows her to be a proactive member in the global digital community. The next chapter will summarize the key findings from this study as well as providing recommendations for further research.

CHAPTER FIVE

CONCLUSIONS AND RECOMMENDATIONS

5.0 INTRODUCTION

This chapter shall focus on summarizing and concluding the study by summing up the key findings related to this study and in the preceding chapters of this dissertation that speak on the legal framework governing cyber security and data protection in Zambia. It will further draw conclusions based on the research objectives that were set and provide recommendations that are tailored to assist in resolving the problem identified in this dissertation which is the gaps and inconsistencies contained in legal framework governing cybersecurity and data protection in Zambia.

5.1 GENERAL CONCLUSION

The legal framework that governs Cybersecurity and Data protection in Zambia is one that needs proper attention and addressing. As has already been established, the use of digital platforms to transact, to trade, to conduct any form of business, to educate and to do many other things has grown significant across the globe over the years and Zambia has since joined the bandwagon in the use of technology for various reasons that aid in bettering the economy through, among other things, foreign direct investment. Due to the fact that Zambia has taken a keen interest and effort into trading and operating on the digital market with the use of technology, it is only imperative that there exist laws governing concepts that relate to such operations, these being cyber security and data protection. Zambia has made significant strides in establishing a legal framework for data protection and cybersecurity being the Data Protection Act no.3 of 2021 and the Cybersecurity Act no.3 of 2025 which are aimed at controlling the protection of personal data and the regulation of cybersecurity in the country.

Regardless of the fact that these strides have been taken, there are still a few shortcomings with the current legislation in governing cybersecurity and data protection. With regards to the Data Protection Act, there are some shortcomings in terms of the institutional framework. As already established, according to ***section 4 of***

the Data Protection Act[64] 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 country. This indicates that the office of the Data Protection Commissioner and the Commission itself have no outright autonomy and have many limitations in terms of their functions and the ways in which they can carry out their operations. This is due to the fact that the Commission is established under the Ministry in charge of Communications. Considering the fact that the Act does not stipulate which specific Ministry is responsible for communications, it makes it difficult to take recourse as an aggrieved party due to the fact that there is no clear indication of where said Ministry is and who is in charge of the Ministry as well as a detailed outline of how to carry out any recourse in relation to the Ministry as it oversees operations of the Data Protection Commission and is in charge of all operations that are carried out by the Commission. Another problem with the institutional framework established by the Data Protection Act is stipulated under ***section 3 of the Data Protection Act***[65] which brings out the scope of application of the Act. The section states that the Act applies to the processing of personal data performed wholly or partly by automated means and to any processing otherwise than by electronic means. Subsection 2 further goes on to state that the Act does not apply to the processing of personal data by an individual for personal use. This brings out the fact the term personal use is very subject as it is very difficult to determine from whose point of view the personal use is.

In relation to the Cybersecurity Act, there are problems with the institutional framework stipulated under the Cybersecurity Act. As already established under **section 3 of the Cybersecurity Act**[66] the Act establishes the Zambia Cybersecurity Agency which has, as one of its functions, the coordination of cybersecurity in the Republic which is a function that is stipulated under section 3(2) of the Cybersecurity Act[67]. According to subsection 1, the Agency is established under the Office of the President which is an indication that the Zambia Cybersecurity Agency has a lack of autonomy in terms of

[64] Act 3 of 2021
[65] Act 3 of 2021
[66] Act 3 of 2025
[67] Act 3 of 2025

their operations. This makes it difficult to sanction the office of the president due to the fact that the agency is established under their office.

As discussed, the legal framework governing cybersecurity and data protection in Zambia is inadequate with too many grey areas and needs to adopt principles and ideologies from international standards such as the GDPR, Budapest Convention and the Malabo Convention. This is in order to ensure proper sanctions imposed on people that breach said laws and also to ensure that there are no further cybersecurity beaches as well as violations of individuals' personal rights in relation to data protection.

5.2 SUMMARY OF CHAPTERS

This thesis constitutes of five (5) chapters which analyse the legal framework governing cybersecurity and data protection in Zambia, it's shortcomings and pitfalls as legislation that governs cybersecurity and data protection as well as analyse the aforementioned laws in comparison with international standards including the GDPR, Budapest Convention and Malabo Convention.

5.2.1 CHAPTER ONE

The first chapter identified the legal problem relating to this study which hence laid the foundation for this thesis. It introduced the topic, provided a background of the study, giving insight on the genesis and reasoning behind the need for the study and the background of the use of technology or a digital platform in Zambia. It also highlighted how Zambia's use of technology is fast growing and wide spread in the sense that small and big organisations have encompassed the use of technology in their day-to-day activities in order to make their operations easier and due to this fact, there is a higher chance of cyber-attacks and cyber threats as well as data breaches. The background of the study under this chapter emphasized and made much reference to the role of advancing technologies in enhancing connectivity and service delivery while introducing entirely new vulnerabilities in relation to the technology being used. The statement of the problem under this chapter identified different inadequacies in the laws governing cybersecurity and data protection in Zambia being the Cybersecurity Act no.3 of 2025 and Data protection Act no.3 of 2021. Some of these inadequacies include missing crimes that had been highlighted above such as sonar attacks and

swatting which were explained above in detail. Another inadequacy includes lack of institutional autonomy for both Zambia Cybersecurity Agency and Data Protection Commission, ambiguous safeguards for derogations and the allowance of consent being overridden by a data controller over that of the data subject. The General objective of this study was shared in this chapter as to critically analyse Zambia ‘s legal framework governing cybersecurity and data protection in relation to international standards such as the GDPR, Budapest Convention and Malabo Convention and the specific objectives under this chapter focusing an dissecting the examination of the local legal framework governing cybersecurity and data protection, assessing the alignment of the local legislation with international standards and the need for harmonization amongst the two. Alluding to this, this chapter also discussed the significance of the study which was identified as contributing to the limited scholarly work on the matter, promoting economic development through investor confidence with strong laws and facilitating international cooperation among nations.

5.2.2 CHAPTER TWO

The second chapter focused solely on analysing and examining the legal framework governing cybersecurity and data protection in Zambia, being the Cybersecurity Act no.3 of 2025 and Data Protection Act no.3 of 2021. In examining the Cybersecurity Act, it analysed the Zambia Cybersecurity Agency, which as aforementioned, is an agency established under the President’s office and its responsible for coordination of incidents relating to cybersecurity, taking measures in response to cyber incidents and disseminating information in relation to cyber threats. Another institution established under this chapter in relation to cyber security is the Central Monitoring and Coordination Centre and in this chapter was highlighted as the hub responsible for lawful interceptions. This chapter brought out key provisions as well which included the criminalization of unlicensed cybersecurity services and penalties for non-compliance. This chapter also brought out enforcement mechanisms that encompassed warrantless interceptions, investigations and emergency measures however weaknesses like institutional ambiguity and limited autonomy were also identified in this chapter. In relation to data protection, this chapter analysed the office of the Data Protection Commissioner which is responsible for registration, licensing and stakeholder engagements. Some of the key provisions that were stipulated under

this chapter in relation to the data protection Act include outlined data subject rights like right to access, right to erasure and right to rectification. It also outlined obligations of data controllers while the enforcement involved oversight, inspections and fines to be paid. The chapter highlighted that the Act protects personal information through principles of lawful processing, consent, notifications of breaches and localization requirements. In as much as it highlighted all the benefits of the Act, it also highlighted some of the pitfalls of the Act which included ministerial oversight that undermines independence, overriding of consent and vague scopes in terms of application of the Act. It was concluded in this chapter that the Zambia's framework was progressive however contained significant structural and operational deficiencies.

5.2.3 CHAPTER THREE

The third chapter focused on assessing the alignment of Zambia's legal framework with international standards, being the GDPR, Budapest Convention and Malabo Convention. The GDPR was presented as a benchmark for data protection as it emphasizes principles like lawful processing, data minimization and accountability while also highlighting robust data subject rights. The Budapest Convention focused on cybersecurity as it criminalizes offences such as illegal access, interception and system interference while promoting procedural tools and international cooperation. The Malabo Convention was also outlined in this chapter as one that integrates both cybersecurity and data protection, mandating criminalization of cybercrimes, national strategies, data processing principles and rights like confidentiality while recognizing electronic transactions. It terms of alignment, this chapter revealed convergences like the fact that Zambia's Acts incorporate data subject rights, breach notifications and cybercrime criminalization. Subsequently, the chapter also identified divergences like Zambia's lack of institutional autonomy as opposed to GDPR's independent authorities, ambiguous safeguards as opposed to Budapest convention's procedural clarity and limited awareness as opposed to the Malabo Convention's emphasis on harmonization. This chapter was concluded by establishing that there are gaps in the scope, enforcement and operational details hindered full compliance, underscoring the need for reforms to bridge these disparities.

5.2.4 CHAPTER FOUR

The fourth chapter articulated the necessity and importance for alignment of the local legislation with international standards, outlining the benefits of alignment and the pitfalls of non-alignment. This chapter outlined the fact that alignment would enhance data protection through robust safeguards, transparency and consistency with global norms; improve cybersecurity via universal crime definitions, coordinated response and human rights protections ;strengthen institutions by granting autonomy and resources; boost economic growth by attracting investment and facilitating digital trade; fortify consumer rights with clearer protections; amplify digital transformation in sectors like e-commerce and banking and ensure legal certainty. Comparative examples from jurisdictions adhering to these standards demonstrated reduced breaches and increased trust. Shortcomings in Zambia's legislation were also highlighted in this chapter such as institutional dependencies, ambiguities and limited capacity. Non alignment risks such as heightened vulnerabilities to breaches, economic barriers and legal uncertainties complicating enforcement were also highlighted in this chapter. The chapter concluded that alignment is vital for Zambia's proactive role in global digital governance.

5.3 RECOMMENDATIONS

Having discussed in depth the inadequacies of the Cybersecurity Act and the Data Protection Act, its level and extent of alignment with international standards and the need for alignment as well as pitfalls of non-alignment with said international standards, this research paper proceeds to make recommendations accordingly. The research recommendations are based on the amendments of both the Cybersecurity Act no.3 of 2025 and the Data Protection Act no.3 of 2021. The recommendations stand as follows;

1. **Institutional reforms under both Acts**

   There must be an amendment of both the Cybersecurity Act and the Data Protection Act in a manner that grants full operational, financial and structural autonomy to both the Zambia Cybersecurity Agency and the Data Protection Commission. This includes establishing them as independent bodies rather than bodies established under the Ministry in charge of communications or the office of

the president and the oversight provided by these organs. This in itself aligns with the GDPR's independent supervisory authorities. The need for autonomy is essential in order to ensure a lack of conflict of interest or a situation in which duties are not properly executed due to the fact that there is a need to work under the supervision of another body. The Acts could contain a provision that allows for a budget to be granted to each body under both Acts in order to ensure full financial autonomy. In order to mitigate resistance, this autonomy could be granted in phases in order to show its need and how essential it is.

2. Legislative Amendments

Under the Data protection Act, the term personal use should be expanded on in order to remove the ambiguity and in the Cybersecurity Act, there should be a stipulated location for the Central Monitoring Centre. There should also be a strengthening of safeguards for derogations and interceptions, ensuring proportionality and judicial oversight which is in line with the Budapest Convention. There should also be a prohibition of consent being overridden by the Data Protection Commissioner in order to uphold the emphasis on data subject control as established by the GDPR. Ambiguities and gaps in current laws lead to enforcement inconsistencies and leave unaddressed vulnerabilities that could be exploited in Zambia's fast growing digital infrastructure. Implementation could involve a parliamentary review committee to draft amendments that would incorporate definitions from the Budapest convention such as criminalizing illegal access and system interference with adequate and clear penalties. For data protection, prohibiting consent overrides would align with the principles outlined in the GDPR where the consent of the data subject is paramount over everything.

3. Harmonization with international standards

Zambia should ratify international instruments such as the Budapest Convention and fully implement the Malabo Convention principles. There must also be an adoption of the elements in the GDPR like data minimization, portability and stringent breach notification timelines. It is also imperative that the country develop national cybersecurity strategies with defined timelines and partnerships which emphasize cross border cooperation. Harmonization is essential as it fosters global

cooperation and is essential for combatting transnational cybercrimes. Ratifying the Budapest Convention would allow Zambia's laws to share evidence in an easier manner and conduct joint investigations. The benefits of this include a reduced number of cyber threats and risks through harmonized offences and procedural tools.

4. Economic and policy integration

The law should be amended so as to integrate cybersecurity and data protection into national economic policies that would act as a magnet to foreign investors. There should also occur a mandate that localizes data with exceptions only for consented international transfers, while promoting e- commerce through recognized electronic signatures. In order to test whether there is compliance by the public over these policies, regular audits and impact assessments should be conducted. It is important to note that strong frameworks boost economic growth by fostering trust in digital markets and improving investor confidence. In developing countries and economies, improved cybersecurity promotes inclusive growth which enables sectors like e- commerce and digital banking. The benefit of policy integration is that that will be a reduction of economic setbacks due to data breaches and cyber threats.

5. Public awareness campaigns

In order to ensure a culture of compliance with the law for citizens, raising public awareness regarding data protection rights and cybersecurity is crucial. It can be done in the manner of implementing national campaigns that have the sole purpose of educating citizens about their rights under the Data Protection Act and the importance and need for cybersecurity practices as individuals and for the republic at large. It can also be achieved through collaborating with large scale organisations in order to reach a broader audience and promote awareness of data protection issues. Examples of successful public awareness campaigns include the Stay safe online campaign which strengthens best practices on cyber hygiene, cybersecurity and privacy among citizens.[68] This campaign promotes online safety and security, providing resources for individuals and businesses to protect their

[68] Stay safe online accessed at https://staysafeonline.in on 7/11/2025

personal information. It contains educational material, social media outreaches and partnerships with businesses and organizations to spread awareness about safe online practices. This campaign is carried out by the National Cyber Security Alliance of the United States of America. Another example of a public awareness campaign is the #Cyber Aware which is launched by the Cybersecurity Agency of Singapore and it aims to educate the public about cyber hygiene and safe online behaviour. Some of its key features include engaging videos, interactive games and community events that encourage citizens to adopt safer online habits. Zambia engaging in such an activity would put Zambia on the map as one of the few African countries that have taken a keen interest in cyber security and data protection.

6. Enforcement and Capacity building

The country can take their resources and invest in technical expertise, training and other valuable resources such as ZICTA, the Zambia Cybersecurity Agency as well as the Data Protection Commission. It is also essential to establish dedicated cyber incident response teams with clear protocols that are easily comprehended and easily followed. Like mentioned above, the law makers should introduce mandatory public awareness campaigns and stakeholder collaborations that are like those in the Malabo Convention that are put in place to boost compliance and reporting. It is important to understand that limited expertise and awareness on the matter, that is data protection and cybersecurity in the country, hinder practical application as noted in developing countries where institutional reforms often fail without supporting capacity building.[69] Implementation strategies include partnering with international bodies for training programs in order to increase knowledge obtained from first world countries. This could include the Council of Europe for training programs on Budapest Convention tools which enhance investigative capabilities. The World Bank has aided over 100 countries in building cyber resilience through national strategies that include incident response teams and awareness initiatives that lead inevitably to reduced breach impacts.[70] In Asia, cybersecurity measures have improved healthcare digitalization by controlling institutional malfunctions. In Zambia this could aid institutions such as those under finance in the country. Public

[69] Lilly Pijenburg Muller, Cyber Security Capacity Building in Developing Countries: Challenges and Opportunities 2015 accessed on https://cybilportal.org on 7/11/2025

[70] Enhancing Cyber Resilience in Developing Countries accessed on https://worldbank.org on 7/11/2025

campaigns could use media and schools to educate on data rights, similar to South Africa's Protection Information Act efforts. Challenges like funding shortages can addressed through grants from donors like the UN. Some of the benefits of this action include stronger enforcement which can be seen through Ethiopia's recent data law implementation which included capacity building to handle rising breaches.

BIBLIOGRAPHY

STATUTES

Constitution Act no.2 of 2016

Cybersecurity Act no.3 of 2025

Data Protection Act no.3 of 2021

BOOKS

C Hewage and L Yakasethu, Data Protection: the wake of AI and machine learning 2024

E Martin, Oxford dictionary of law (7th edition)

R Manglik, Cybersecurity and Law (EduGorilla Prep Experts, 2024) 269

S Howard and P Alex, New Solutions for Cybersecurity (The MIT Press,2017)

INTERNET SOURCES

Data auditing and analytics accessed at https://www.secoda.com on 13/08/2025

Enhancing Cyber Resilience in Developing Countries accessed on https://worldbank.org on 7/11/2025

Institutional frameworks – an overview accessed at https://www.sciencedirect.com on 13/08/2025

Lilly Pijenburg Muller, Cyber Security Capacity Building in Developing Countries: Challenges and Opportunities 2015 accessed on https://cybilportal.org on 7/11/2025

S F Cinini, the trends of cybersecurity and its emerging challenges in Africa available at www.link.springer.com accessed on 14/04/2025

S Christine and S P Alice, advancing cybersecurity measures to safeguard critical infrastructure and data: is Zambia ready? Available at https://ictjournal.icict.org.zm accessed on 14/04/2025

Sonic attacks suffered by US diplomats likely caused by microwave energy accessed at www.cnn.com on 16/04/2025

Stay safe online accessed at https://staysafeonline.in on 7/11/2025

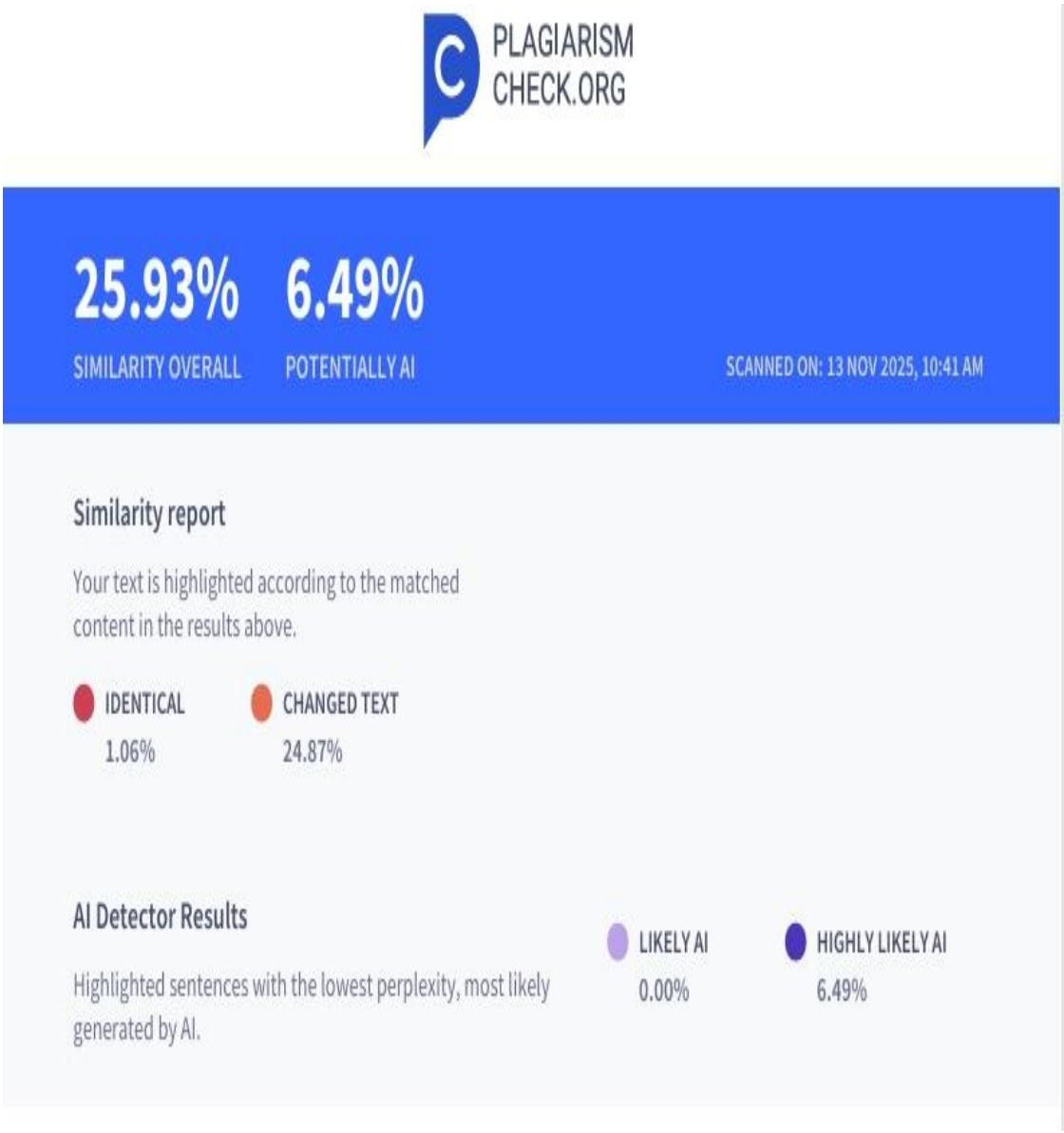
Swatting accessed at https://www.fortinet.com on 16/04/2025

INTERNATIONAL TREATIES

African Union Convention on Cyber Security and Personal Data Protection

Budapest Convention- Treaty 185

General Data Protection Regulation


PLAGIARISM CHECK.ORG
25.93%
SIMILARITY OVERALL
6.49%
POTENTIALLY AI
SCANNED ON: 13 NOV 2025, 10:41 AM
Similarity report
Your text is highlighted according to the matched content in the results above.
IDENTICAL
1.06%
CHANGED TEXT
24.87%
AI Detector Results
Highlighted sentences with the lowest perplexity, most likely generated by AI.
LIKELY AI
0.00%
HIGHLY LIKELY AI
6.49%

UNIVERSITY of LUSAKA

SCHOOL OF LAW

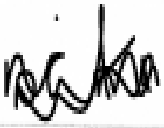
L400B / Dissertation II – DIRECTED RESEARCH (OBLIGATORY ESSAY)

RESEARCH CLEARANCE FORM

NAME: Namasiku Anakoka STUDENT NUMBER: LLB22113403

SUPERVISOR: K.K Mwauluka TOPIC: A Critical Analysis of The Legal Framework Governing Data Protection And Cyber Security In Zambia: Lessons From International Standards.

Stage	Supervisor's Comments	Supervisor's Signature & Date	Student's Signature & Date
Research Proposal	APPROVED		30/07/25
Chapter 1 – Introduction	APPROVED		05/08/25
Chapter 2 –	APPROVED		20/08/25
Chapter 3 –	APPROVED		05/09/25
Chapter 4 –	APPROVED		15/10/25

Chapter 5 – Conclusions & Recommendations	APPROVED		 02/11/25
Abstract, Table of Contents, Bibliography and Appendices	APPROVED		 03/11/25
First Draft	APPROVED		 09/11/25
Second Draft	APPROVED		 12/11/25
Final Draft	APPROVED		

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