**ADDIS ABABA UNIVERSITY**

**COLLEGE OF LAW AND GOVERNACE STUDIES**

**SCHOOL OF LAW**

**LL.M Program in Human Rights Law**

**Research as a Partial Fulfillment for the LLM Thesis**

# Safeguarding the Right to Digital Privacy under the New Personal Data Protection Law of Ethiopia: A Comparative Study


**By**

**Biruktawit Dereje**

**Advisor**

**Assistant professor, Jetu Edosa**


**August, 2025**

**ADDIS ABABA UNIV ERSITY**

**SCHOOL OF GRADUATES STUDIES LLM**

**PROGRAM I N HUMAN RIG HTS LAW**

**(APPROVAL SHEET)**

**Safeguarding the Righht to Digital Privacy Under the New Personal Data Protection Law of Ethiopia: A Com pa rative Study**

**A Thesis submitted of Law of Addis Ababa University in Partial Fulfillment of the Requirement for the Master of Laws (LLM) Degree in human Right**

**BY Dirtiktau it Dereje** **Signature**

**Advisor: Jet u Edosa (Ph D)**

**ADDIS ABABA UNIVERSITY**

**SCHOOL OF GRADUATES STUDIES**

**LLM PROGRAM IN HUMAN RIGHTS LAW**

**DECLARATION**

**Safeguarding the Right to Digital Privacy under the New Personal Data Protection Law of Ethiopia: A Comparative Study**

A Thesis submitted to School of Law of Addis Ababa University in Partial Fulfillment of the Requirement for the Master of Laws(LLM) Degree in Human Right Law.

The research is reviewed for plagiarism and AI generated text report through Turnitin software, and the similarity index doesn‘t exceed the maximum allowable limit of 20%, as per University‘s guidelines.

BY Biruktawit Dereje Signature

Advisor: Jetu Edosa(PhD) _____

Examiners:

1. _____

2. _____

# *% detected as AI

AI detection includes the possibility of false positives. Although some text in this submission is likely AI generated, scores below the 20% threshold are not surfaced because they have a higher likelihood of false positives.

**Caution: Review required.**

It is essential to understand the limitations of AI detection before making decisions about a student's work. We encourage you to learn more about Turnitin's AI detection capabilities before using the tool.

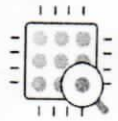
Disclaimer
Our AI writing assessment is designed to help educators identify text that might be prepared by a generative AI tool. Our AI writing assessment may not always be accurate (it may misidentify writing that is likely AI generated as AI generated and AI paraphrased or likely AI generated and AI paraphrased writing as only AI generated) so it should not be used as the sole basis for adverse actions against a student. It takes further scrutiny and human judgment in conjunction with an organization's application of its specific academic policies to determine whether any academic misconduct has occurred.

## Frequently Asked Questions

**How should I interpret Turnitin's AI writing percentage and false positives?**
The percentage shown in the AI writing report is the amount of qualifying text within the submission that Turnitin's AI writing detection model determines was either likely AI-generated text from a large-language model or likely AI-generated text that was likely revised using an AI paraphrase tool or word spinner.

False positives (incorrectly flagging human-written text as AI-generated) are a possibility in AI models.

AI detection scores under 20%, which we do not surface in new reports, have a higher likelihood of false positives. To reduce the likelihood of misinterpretation, no score or highlights are attributed and are indicated with an asterisk in the report (*%).



The AI writing percentage should not be the sole basis to determine whether misconduct has occurred. The reviewer/instructor should use the percentage as a means to start a formative conversation with their student and/or use it to examine the submitted assignment in accordance with their school's policies.

**What does 'qualifying text' mean?**
Our model only processes qualifying text in the form of long-form writing. Long-form writing means individual sentences contained in paragraphs that make up a longer piece of written work, such as an essay, a dissertation, or an article, etc. Qualifying text that has been determined to be likely AI-generated will be highlighted in cyan in the submission, and likely AI-generated and then likely AI-paraphrased will be highlighted purple.

Non-qualifying text, such as bullet points, annotated bibliographies, etc., will not be processed and can create disparity between the submission highlights and the percentage shown.

# Safeguarding the Right to Digital Privacy under the New Personal Data Protection Law of Ethiopia: A Comparative Study

ORIGINALITY REPORT

| 15% | 10% | 1% | 9% |
|---|---|---|---|
| SIMILARITY INDEX | INTERNET SOURCES | PUBLICATIONS | STUDENT PAPERS |

PRIMARY SOURCES

| | | |
|---|---|---|
| 1 | dpoacademy.gr<br>Internet Source | 8% |
| 2 | Submitted to Erasmus University of Rotterdam<br>Student Paper | 3% |
| 3 | Submitted to Brunel University<br>Student Paper | 1% |
| 4 | Submitted to University of Washington<br>Student Paper | 1% |
| 5 | Samuel Frank Matinou, Conrad Tucker, Isobel Acquah, Prasenjit Mitra, Rdiwan Oloyede, Arnold Joshua Kabatsi. "Beyond Borders: Exploring Data Embassies as a Strategy for Digital Sovereignty in Africa", Cambridge University Press (CUP), 2025<br>Publication | 1% |
| 6 | Daniel Gervais. "Not Quite Like Us? — Can Cyborgs and Intelligent Machines Be Natural Persons as a Matter of Law?", Qeios Ltd, 2023<br>Publication | <1% |
| 7 | Valmir Jesus dos Santos. "A crítica teatral por Mariangela Alves de Lima, uma ruminante da experiência estética", Universidade de São Paulo. Agência de Bibliotecas e Coleções Digitais, 2025<br>Publication | <1% |

# Table of Content

Page


Table of Content ..... i

Acronyms ..... iii

Acknowledgment ..... iv

Abstract ..... v

Chapter One ..... 1

Introduction ..... 1

1.1 Background of the Study ..... 1

1.2 Statement of the Problem ..... 4

1.3 Literature review ..... 6

1.4 Research Questions ..... 7

1.5 Objectives of the Study ..... 8

1.5.1 General objectives ..... 8

1.5.2 Specific objective ..... 8

1.6 Research methodology and methods ..... 8

1.7 Scope of the Study ..... 9

1.8 Limitations of the Study ..... 9

1.9 Significance of the Study ..... 9

1.10 Organization of the study ..... 10

Chapter Two ..... 11

2. Theoretical and Legal Framework of Digital Privacy ..... 11

2.1 Concept of Digital Privacy and Personal Data Protection ..... 11

2.2 Legal Foundations of Privacy Rights ..... 13

2.3 Global Standards and Best Practices in Data Protection ..... 16

2.3.1 General Data Protection Regulation ..... 16

2.3.2 The African Convention on Cyber Security and Personal Data Protection (The Malabo Convention) ..... 22

2.4 The Role of Technology in Digital Privacy Protection ..... 24

Chapter Three ..... 27

3. Ethiopia‘s Personal Data Protection Law ..... 27

3.1 Overview of Ethiopia‘s Legal Framework for Data Protection.....27
3.2 Key Provisions of the Personal Data Protection Proclamation.....31
3.3 Rights of Data Subjects Under the Personal Data Protection Proclamation.....35
3.4 Obligations of Data Controllers and Processors.....38
3.5 Institutional and Enforcement Mechanisms.....41
Chapter Four.....43
4. Comparative Analysis of Ethiopia‘s Data Protection Law.....43
4.1. Comparison with the European Union‘s GDPR.....43
4.2. Comparison with the Data Protection Law of South Africa (POPIA).....52
4.3. Strengths and Weaknesses of Ethiopia‘s Law in a Global Context.....57
4.4. Challenges in Implementation and Compliance.....61
Chapter Five.....64
5. Conclusion and Recommendations.....64
5.1 Conclusion.....64
5.2 Recommendations.....65
Bibliography.....67

## Acronyms

| | |
|---|---|
| AI | Artificial intelligence |
| AU | African Union |
| EC | European commission |
| ECHR | European Convention on Human Right |
| EU | European Union |
| FDRE | Federal Democratic Republic of Ethiopia |
| GDPR | General Data Protection Regulation |
| ICCPR | International covenant on Civil and Political Right |
| OECD | Organization for Economic Co-operation and Development |
| PDPP | Personal Data Protection Proclamation |
| POPIA | Protection of Personal Information Act |
| TEU | Treaty on European Union |
| UDHR | Universal Declaration of Human Right |

## Acknowledgment

Above all I would like to thanks and praise the almighty God for his help throughout my life.

Then I would like to express my heartfelt gratitude to Addis Ababa University College of Law and Governance Master of Human Right department of law for initiation of this paper. Also, I would like to thanks my advisor DR. Jetu Edosa for his valuable and genuine advice and constructive criticisms contributing to quality of this paper he has much credit through guiding and commenting me on this paper.

# Abstract

In light of international data protection standards, including the Protection of Personal Information Act (POPIA) of South Africa and the General Data Protection Regulation (GDPR) of the European Union, this paper critically evaluates Ethiopia's Personal Data Protection Proclamation (PDPP). The study evaluates the PDPP's enforcement and corrective measures, finds institutional and legal flaws, and investigates how well it protects the right to digital privacy.

Using a doctrinal and comparative legal research technique, the paper compares the GDPR and POPIA and examines pertinent policy documents, academic literature, and legislative legislation. According to the findings, the PDPP has serious flaws even though it incorporates globally accepted data protection principles and gives data subjects substantive rights, making it a historic move in Ethiopia's digital rights landscape. These include ambiguous legal definitions, a lack of institutional autonomy, a lack of ability to enforce the law, and inadequate provisions pertaining to cutting-edge technology like algorithmic profiling, biometric identification, and artificial intelligence.

In contrast to the GDPR, the PDPP has a smaller extraterritorial reach, less severe fines, and less supervisory control. It also does not have the independent enforcement framework that POPIA does. These shortcomings run the risk of eroding public confidence, compromising safeguards against data abuse, and restricting Ethiopia's participation in international digital commerce.

The study comes to the conclusion that strengthening Ethiopia's data protection regime requires focused legislative reform, institutional reorganization, and improved technology safeguards. Establishing an independent supervisory body, defining important legal terms, enforcing harsher penalties, incorporating cutting-edge technological protections, and conforming to regional and global norms like the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention) are some of the recommendations.

# Chapter One

# Introduction

## 1.1 Background of the Study

The digital age has ushered in an era of unprecedented connectivity, transforming the way we live, work, and communicate.[1] Due to this, the advent of the internet, mobile devices, social media platforms, and sophisticated data analytics has led to an unprecedented volume and granularity of personal information being collected, processed, and shared.[2] However, the collection and use of those data also raise important privacy and security concerns.

The term ―Privacy‖ means the right that determines the nonintervention of secret surveillance and the protection individual‘s information. Privacy is about protecting people.[3] Henceforward, in the domain of human right instruments, Privacy is a fundamental human right. It also covers a very wide range concept. Hence, the origins of this right can be traced back to the pivotal document of Universal Declaration of Human Right, adopted on December 10, 1948. Stating, ―No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.‖[4] International Covenant on Civil and Political Rights under article 17 also puts the same protection for privacy right.

Initially, privacy laws were shaped by concerns over physical rights and interfering on someone‘s space without authorization. But due to the rapid growth of digital world the dimension of the right to privacy concern goes beyond the physical right.

The digital transformation has brought about unprecedented opportunities for economic development, innovation, and connectivity. [5] However, it has also raised significant concerns about personal data protection and the safeguarding of privacy. General Data Protection

[1] Ikhtiyorovna, K.G.Z. (2023). Embracing Technological Changes for a Better Future. American Journal of Language, Literacy and Learning in STEM Education (2993-2769), 1(9), 339- 344.
[2] Reis, Eneh, Ehimuan, Anyanwu, Olorunsogo, & Abrahams, PRIVACY LAW CHALLENGES IN THE DIGITAL AGE: A GLOBAL REVIEW OF LEGISLATION AND ENFORCEMENT, P.No. 73-88
[3] Bryan A Garner (ed), *Black's Law Dictionary* (11th edn, Thomson Reuters 2019) 1458.
[4] United Nation General assembly, Universal declaration of human rights instrument, Article 12 (1948)
[5] Reis, Eneh, Ehimuan, Anyanwu, Olorunsogo, & Abrahams, Privacy Law Challenges in The Digital Age: A Global Review of Legislation and Enforcement, P. 73-88

Regulation (GDPR) under article 5; personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.[6] Also those data collected for specified, explicit and legitimate purposes and not further processed in such manner that is incompatible with those purpose.[7] In which this regulation provide overview on the way that personal data should be collected, used and protected.

The General Data Protection Regulation (GDPR) establishes six core principles that govern the processing of personal data within the European Union. First, personal data must be processed lawfully, fairly, and in a transparent manner in relation to the data subject. Second, it must be collected for specified, explicit, and legitimate purposes and not further processed in a way that is incompatible with those purposes. Third, the data collected should be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed. Fourth, personal data must be accurate and, where necessary, kept up to date, with every reasonable step taken to ensure that inaccurate data is erased or rectified without delay. Fifth, personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. Finally, it must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage through appropriate technical or organizational measures.[8]

In addition, to that African union adopted convention on cyber security and personal data protection (Malabo convention) thus aims to address the regulatory challenges posed by increasing cyber-crime in the continent and also providing framework for a compatible legislation on data protections.[9] The convention gives a clear insights on the data subjects, how

[6] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) [2016] OJ L119/1, art 5(1)(a)

[7] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) [2016] OJ L119/1, art 5.

[8] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) [2016] OJ L119/1, art 5(1)(a-f).

[9] African Union, African Union Convention on Cyber Security and Personal Data Protection adopted 27 June 2014,

to collect and stored such kind of data, transfer of data and it caters the principle of transparency and accountability. It also allows notification in case of data processing and data breaches.[10] It also server‘s as a benchmark for measuring whether member states legislation comply or not.

Ethiopia, as a nation undergoing rapid digitalization, faces challenges in ensuring robust data protection mechanisms while fostering the growth of its digital economy. The primary legislation that lays the foundation for data protection rules is the Constitution of the Federal Democratic Republic of Ethiopia. The Constitution recognizes the right to privacy and inviolability of the correspondences of individuals. [11]The Ethiopian Civil Code also provides certain privacy rights but none of them provide a comprehensive legal frame work on protection of personal data. A Personal Data Protection Proclamation was recently introduced in Ethiopia with the goal of protecting people's rights online. In contrast to well-established legislative frameworks like the Protection of Personal Information Act (POPIA) of South Africa and the General Data Protection Regulation (GDPR) of the European Union, concerns are raised about its efficacy in guaranteeing digital privacy.

In a time of swift technical development and the expanding digital economy, personal information has grown in value. Privacy rights are seriously threatened by the way governments, private organizations, and multinational businesses gather, use, and store personal data. Ethiopia and other developing nations are still in the early phases of putting strong legal frameworks in place, whereas wealthy nations have enacted comprehensive data protection laws. Ethiopia's data protection policies must be in line with worldwide best practices in order to successfully secure digital privacy, considering the global nature of digital interactions.

There are advantages and disadvantages to the Ethiopian Personal Data Protection Proclamation's implementation. On the positive side, the proclamation marks a significant step toward aligning Ethiopia‘s legal framework with international data protection standards such as the GDPR, promoting lawful, fair, and transparent processing of personal data.[12] It establishes the Personal Data Protection Commission, mandates data subject rights, and introduces

[10] African Union, African Union Convention on Cyber Security and Personal Data Protection adopted 27 June 2014,

[11] The federal democratic republic of Ethiopia constitution, article 26, (1995)

[12] Regulation (EU) 2016/679 (General Data Protection Regulation) [2016] OJ L119/1; see also Proclamation No. 1285/2023, Federal Negarit Gazette (Ethiopia), art 5

obligations for data controllers and processors, which enhances accountability and public trust in digital systems.[13] Furthermore, it provides a legal foundation for cross-border data transfers, which is vital for Ethiopia's participation in the global digital economy.[14]However, the proclamation also, presents challenges. Critics have pointed out that the law lacks strong enforcement mechanisms and the institutional independence of the supervisory authority may be questionable due to government influence.[15]Moreover, the proclamation's vague language on certain key concepts—such as ―legitimate interest‖ or ―public interest‖—risks undermining the clarity and predictability required for legal compliance.[16]

Although it represents an important step in acknowledging the right to digital privacy, questions still surround its application, methods of enforcement, and general conformity to internationally recognized data protection standards. This study aims to assess its shortcomings and advantages.

## 1.2 **Statement of the Problem**

Personal information has grown to be a significant resource for people, companies and governments in the digital age. As Ethiopia undergoes rapid digital transformation marked by the expansion of internet connectivity, e-commerce, digital ID systems and mobile telecommunications; the volume and sensitivity of personal data collected by public and private actors have increased significantly. Despite this development, legal and institutional safeguards for personal data protection remain insufficient, raising serious concerns about the impact of these changes on individuals' right to privacy given the limitations of comprehensive data protection legislation and enforcement mechanisms.[17] While the FDRE Constitution guarantees the right to privacy[18] and Ethiopia is a state party to international human rights instruments such as the International Covenant on Civil and Political Rights (ICCPR)[19], the practical enforcement of this right remains underdeveloped. Historically, Ethiopia lacked a comprehensive data

[13] Proclamation No. 1285/2023, arts 10–22
[14] Ibid, arts 23–26
[15] Kinfe Michael Yilma, *'Ethiopia's New Personal Data Protection Law: Key Features and Challenges Ahead'* (2023)
[16] Berhan Taye and Roman Teshome, *'Privacy and Personal Data Protection in Ethiopia'* (2018)
[17] Kinfe Micheal Yilma, *Data Privacy Law and Practice in Ethiopia*, Vol. 6(1) Journal of Media Law and Ethics, P. 21, (2022)
[18] FDRE Constitution, Article 26, (1995)
[19] Ethiopia has become a state party to ICCPR in 1993. As per Article 9/4 of the FDRE Constitution, ICCPR is an integral part of the law of the land.

protection regime and personal data was regulated by fragmented laws such as Freedom of the Mass Media and Access to Information Proclamation, Telecom Fraud Offences Proclamation, Registration of Vital Events and National Identification Cards Proclamation, Computer Crime Proclamation, Electronic Signature Proclamation, the Ethiopian Digital ID Proclamation, etc. These instruments failed to provide harmonized and strong data governance which created legal uncertainty and gaps.

In 2024, Ethiopia adopted the Personal Data Protection Proclamation (PDPP) with the aim of addressing these challenges. While this law represents a critical step forward, it exhibits several substantive and structural deficiencies. These include vague definitions of key terms, weak enforcement mechanisms, and the absence of a clear institutional framework. A key concern lies in the lack of an independent and specialized data protection authority. The Proclamation designates the Ethiopian Communication Authority as the implementing body, despite its primary mandate over the telecommunications sector. This dual regulatory role may lead to conflicts of interest and weak oversight.

Furthermore, the PDPP does not sufficiently address the challenges posed by emerging technologies such as artificial intelligence, biometrics and big data analytics. There are also inconsistencies between the PDPP and existing sectoral laws, creating potential conflicts and undermining effective implementation. Additionally, there are inadequate safeguards and limited clarity on procedures for cross-border data transfers and the protection of data subjects‘ rights.

While Ethiopia‘s PDPP is substantively modeled on the GDPR, significant differences remain in its enforcement mechanisms, institutional independence, and regulatory approach, which leave it weaker in practice despite formal alignment. These gaps not only expose individuals to risks such as data misuse, surveillance and profiling but also undermine trust in digital services and hinder Ethiopia‘s ability to fully participate in global digital trade and cooperation.

Given these challenges, a critical legal analysis of Ethiopia‘s personal data protection framework is necessary. Useful perspectives for evaluating Ethiopia‘s data protection system‘s effectiveness are the GDPR and POPIA. The POPIA in South Africa provides a regional viewpoint specific to the African setting, even if the GDPR is considered the gold standard in data protection. The

objective of this study is to identify areas for development, highlight significant shortcomings, and make recommendations to strengthen Ethiopia's data privacy regime by analyzing its legal provisions in the context of these established laws.

## 1.3 **Literature review**

Review of literature indicates that, this research literary inquiry will be done particularly on the right to virtual or digital privacy under the new personal data protection law of Ethiopia. Thus, the reviewed literatures are below. Mainly, Privacy and Personal Data Protection in Ethiopia by Berhan Taye and Roman Teshome and Data privacy Law And Practice in Ethiopia by Kinfe Micheal Yilma, also Towards Data Protection Law in Ethiopia by Alebachew Birhanu Enyew, will be used in order to get a comprehensive picture of Ethiopian legal framework on the right of digital or virtual privacy right under the current data protection proclamation.

―Balancing Privacy, Personalization and Human Rights in the Digital Age‖ by Ashish K. Saxena explores the complex issue of protecting privacy in the digital age and it also highlights the urgent need for a harmonized approach that ensures technological progress does not come at the expense of fundamental human rights. A book titled ―Privacy, Data Protection and Cybersecurity in Europe‖ which is edited by Wolf J. Schünemann and Max-Otto Baumann is another one that discussed the data privacy rights, the surveillance problem, data security and data processing issues in the context of European countries.

Additionally, ―Securing Rights: Legal Frameworks for Privacy and Data Protection in the Digital Era‖ by John Babikian, the main objective of the paper is to provide a comprehensive analysis of the legal foundations and regulatory frameworks governing privacy and data protection in the digital age. The Lee A. Bygrave book titled ―Data Protection Law: Approaching Its Rationale, Logic and Limits‖ is another one that deals with the origin, rationale and character of data protection laws; values and interests safeguarded by data protection laws; scope, principles and enforcement mechanisms of data protection and the data protection rights of private collective entities and regulation of profiling by data protection laws.

Furthermore, Privacy Law Challenges in the Digital Age: A Global Review of Legislation and Enforcement by Oluwatosin Reis provides a comprehensive global review of privacy legislation

and enforcement mechanisms, shedding light on the challenges posed by the digital age. Also it evaluates the impact of recent high-profile privacy incidents on shaping legislative responses and enforcement strategies. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data is another document that consists of the recommendation of the council, guidelines and the explanatory report of the guidelines.

From European perspective, the most comprehensive data protection law is the General Data Protection Regulation. Researches that were conducted on GDPR were also reviewed. The first one is ―EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation‖ by Peter Hustinx which comparative analysis of GDPR in light of its predecessor the Data Protection Directive 95/46/EC. The European Union General Data Protection Regulation: What It Is and What It Means by Chris Jay Hoofnagle et al., is the other paper that discusses the strategic approach to regulating personal data, the normative foundations of the GDPR and the GDPR's implications. Moreover, ―Understanding EU Data Protection Policy‖ by the European Parliament Research Service is a document that shows the legal framework of data protection in Europe.

From African standpoint, the first reviewed documents was Privacy and Personal Data Protection in Africa; A Rights-Based Survey of Legislation in Eight Countries which include the experience of eight African countries including Ethiopia in data protection laws. Moreover, ―Regulating Data Protection and Cybersecurity in Africa: Findings from the Global Data Regulation Diagnostic‖ is a paper prepared by the World Bank that focuses on the regulatory landscape of data protection in Africa. ―Data Protection Laws in Africa: A Pan-African Survey and Noted Trends‖ by Brian Daigle explores the data protection laws of African countries and conduct case studies in five African countries.

## 1.4 Research Questions

1. What are the key legal and institutional gaps in Ethiopia's Personal Data Protection Proclamation in safeguarding the right to digital privacy?
2. To what extent does Ethiopia's data protection framework align with the six core principles of the GDPR, and what gaps exist in comparison?

3. What kinds of detection mechanisms are available in Ethiopia‘s personal data protection framework to identify and address breaches of personal data?
4. What options are available for resolving personal data breaches once detected under Ethiopia's system for protecting personal data?

## 1.5 Objectives of the Study

### 1.5.1 General objectives

To evaluate digital personal data protection safeguarding rights under the Ethiopia‘s personal data protection proclamation in light of international data protection standards, especially the GDPR and POPIA. The study aims to identify legal and institutional gaps and provide recommendations to strengthen Ethiopia‘s digital data protection framework.

### 1.5.2 Specific objective

1. To examine the extent to which Ethiopia‘s Personal Data Protection Proclamation safeguards the right to digital privacy in line with recognized international standards.
2. To evaluate Ethiopia's adherence to the six fundamental GDPR principles: lawfulness, equity, and transparency; purpose limitation; data minimization; accuracy; validity and confidentiality; and storage limitation.
3. To assess how well Ethiopia's personal data protection framework's breach detection measures are working.
4. To investigate available remedies for breaches involving personal data in Ethiopia.

## 1.6 Research methodology and methods

Doctrinal legal research and comparative legal analysis are the main methods used in this qualitative study. The doctrinal approach entails a thorough analysis of South Africa's Protection of Personal Information Act (POPIA), the European Union's General Data Protection Regulation (GDPR), and Ethiopia's Personal Data Protection Proclamation. Desk-based research will be used to collect data, which will involve analyzing academic literature, policy documents, legal texts, and pertinent case law. Furthermore, case studies will be carried out to investigate the practical implementation of data protection laws in South Africa, the EU, and Ethiopia.

Because of the GDPR's standing as the globally accepted gold standard for data protection and POPIA's applicability as a model from another African jurisdiction with comparable socioeconomic and legislative development circumstances, the EU and South Africa have been chosen for comparative study. The comparison centers on essential aspects of protecting personal data, such as legal principles (including lawfulness, fairness, and transparency), rights of data subjects, data processing specifications, enforcement tools, and breach response strategies. This comparative method seeks to determine areas for reform and improvement as well as how Ethiopia's framework compares to or differs from these more established regimes.

## 1.7 Scope of the Study

The study will focus on Ethiopia‘s Personal Data Protection Proclamation and its effectiveness in safeguarding digital privacy. In order to identify any gaps and possible areas for development, it will compare itself to the GDPR, African Convention on Cyber Security and Personal Data Protection and POPIA. Legal frameworks, enforcement strategies, and policy consequences will all be covered in the study; however, technological cyber security issues or the larger regulatory landscape for digital governance and telecommunications will not be covered.

## 1.8 Limitations of the Study

There are several restrictions on this research. First of all, it mostly uses secondary sources and legal research, which might not adequately represent the difficulties of real-time enforcement. Second, Ethiopia's data protection law is still in its infancy, therefore its effects and actual applications are still mostly unknown.

## 1.9 Significance of the Study

The goal of this study supports law makers alongside law experts and technology professionals in creating strong online security by studying Ethiopian initiatives as well as making recommendations. The research thoroughly evaluates Ethiopia's privacy laws by examining their positive points as well as their limitations within the existing framework. These findings act as guidelines for developing nations to modernize their privacy protection laws because they help officials rewrite current policies or create enforceable regulations which protect individual

privacy throughout digital transformation. The research investigates practical scenarios to evaluate enforcement systems and proposes methods that will maintain compliance among people and business entities and government officials. This research provides a comprehensive analysis of digital privacy conditions in Ethiopia while recommending policy changes based on global data protection practices to enhance stakeholder privacy rights knowledge among businesses and policy makers and general community members.

### 1.10 Organization of the study

The research is structured in to four chapters. Chapter one covers background of the story, problem of the statement, research objective, research question, research methodology and literature review. Chapter two explores theoretical and legal framework of digital privacy especially from the General Data Protection Regulation and African Convention on Cyber Security and Personal Data Protection perspective. Chapter three covers overview of Ethiopia‘s Legal Framework for Data Protection. Chapter four will provide a Comparative Analysis of Ethiopia‘s Data Protection Law with global contexts. Chapter five will conclude the research by identifying the legal framework gaps, challenges and suggest recommendations to strength the protection of the Right to Virtual or Digital Privacy in Ethiopia.

# Chapter Two

# 2. Theoretical and Legal Framework of Digital Privacy

## 2.1 Concept of Digital Privacy and Personal Data Protection

Defining personal data is a crucial task in determining the scope of data protection laws.[20] The European Union General Data Protection Regulation defines personal data as any information relating to the identified or identifiable natural person.[21] GDPR further defined identifiable person as a natural person who can identified by referring to his/her name, identification number, location data, etc.[22] The GDPR has been criticized for its expansive definition of personal data which may lead to abuse of rights and unreasonable application.[23] One commentator opined that by covering every aspect of personal data, GDPR could be seen as the law of everything.[24]

Determining whether certain data are personal or not is essential since data protection laws become effective upon the processing of personal data.[25] One scholar on the subject matter proposed that a data should be regarded as personal when it poses a risk to fundamental rights.[26] To assess the risk, the about, purpose and result elements can be used. The about element is that if a processing data gives insight to the private life of an individual, then it is a personal data.[27] The purpose element is that if the data are used to evaluate, treat in a certain way or influence the status or behavior of an individual, then it is a personal data.[28] The result element is that if a data can have a negative effect on the individual‘s rights and interests, then it is personal data.[29]

Another issue that should be discussed is what are privacy and data protection. Usually, there is a tendency to treat these concepts interchangeably but despite substantial overlap, privacy and data

[20] Nadezhda Purtova, The Law of Everything: Broad Concept of Personal Data and the Future of EU Data Protection Law, Law, Innovation & Tech, Vol. 10 No. 1, P. 43, (2018).
[21] European Union Regulation 2016/679 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, O.J. (L 119) 1, Art. 4/1, (2016). (Herein after GDPR).
[22] Ibid.
[23] Nadezhda Purtova, The Law of Everything: Broad Concept of Personal Data and the Future of EU Data Protection Law, Law, Innovation & Tech, Vol. 10 No. 1, P. 41, (2018).
[24] Ibid.
[25] GDPR, Art. 2/1.
[26] Valentin Rupp and Max Von Grafenstein, Clarifying ―Personal Data‖ and the Role of Anonymization in Data Protection Law: Including and Excluding Data from the Scope of the GDPR (More Clearly) Through Refining the Concept of Data Protection, Computer and Security Review, Vol. 52, P. 2, (2024).
[27] Ibid, P. 8.
[28] Ibid, P. 13.
[29] Ibid, P. 16.

protection have differences with regards to their scope and limitation.[30] This distinction has gotten special attention under the European Union Charter of Fundamental Rights. Under the charter, both the right to privacy and right to data protection are recognized as separate rights.[31] The right to privacy ensures that an individual shall be protected from any interference in four aspect of his life; private life, family life, home and communication.[32]

On the other hand, the right to data protection ensures protection of personal data of an individual concerning him/her.[33] In this regard, data processors are obliged to comply with principles such as fairness, limited to specified purpose, consent-based and other legitimate basis laid under the law in processing of personal data.[34] Even though the charter is groundbreaking in separately recognizing the right to privacy and the right to data protection, it failed to specify what makes these rights distinct from one another and their sphere of application.[35]

The right to privacy and the right to data protection have some differences. The first one is their substantive scope in which privacy can be invoked in relation to sensitive data that have bearing on the individual‘s private life, while data protection can be applicable to any personal data that can be used to identify an individual.[36] Hence, the substantive scope of data protection is broader than privacy.[37] However, in terms of personal scope, data protection protects the rights of natural persons, whereas, privacy is applicable to natural and legal persons alike.[38]

Another important distinction between privacy and data protection under the charter is that the charter envisaged the establishment of an independent authority in the case of data protection that controls compliance of data controllers and data processors with the rules.[39] However, there is no independent authority in the case of privacy.[40] The other distinction is that in traditional

[30] Juliane Kokott and Christoph Sobotta, The Distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR, IDPL, Vol. 3 No. 4, P. 222, (2013).
[31] Charter of Fundamental Rights of the European Union OJ C 326/391, Arts. 7 and 8, (2012).
[32] Ibid, Art. 7.
[33] Ibid, Art. 8/1.
[34] Ibid, Art. 8/2.
[35] Ibid, Arts. 7 and 8.
[36] Juliane Kokott and Christoph Sobotta, The Distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR, P. 225, (2013).
[37] Ibid.
[38] Ibid.
[39] Charter of Fundamental Rights of the European Union, Arts. 8/3.
[40] Ibid, Art. 7.

sense privacy is a mechanism that protects individuals from the interference of the government.[41] However, unlike privacy, data protection is not only a limitation to the government but also to the private parties that may misuse personal data.[42]

The other aspect that should be discussed is the dimension that current digital age has given to the general data protection framework. Technologies have led to shifts of boundaries between what is considered public or private at different times.[43] In recent years, the rapid technological advancements, proliferation of big data and the emergence of artificial intelligence (AI) pose new challenges to the data protection laws.[44]

For instance, in the case of AI, it poses two risks; pattern recognition and data parity.[45] The pattern recognition risk is that the advanced AI's can derive sensitive information from publicly available data.[46] This may lead to powerful institutions including the government with access to AI to guess the need of every individual.[47] The other challenge is data parity in which a few institutions monopolized the access to data and they use the data protection argument to refuse to share any data even though it may be beneficial to the society.[48]

### 2.2 Legal Foundations of Privacy Rights

Various international organizations are active in harmonization of laws that have direct effect on right to privacy including the United Nations, Council of Europe as well as European Union, Organization for Economic Cooperation and Development and other regional organizations.[49]

---

[41] Peter Erik Blume, *Data Protection and Privacy: Basic Concepts in a Changing World*, in *Scandinavian Studies in Law*, ICT Legal Issues, Vol. 56, P. 153, (2010).
[42] Ibid.
[43] Oskar J. Gstrein and Anne Beaulieu, How to Protect Privacy in a Datafied Society? A Presentation of Multiple Legal and Conceptual Approaches, Philosophy and Technology, Vol. 35 No. 3, P. 7, (2022).
[44] John Babikian, Securing Rights: Legal Frameworks for Privacy and Data Protection in the Digital Era, Law Research Journal, Vol. 1 No. 2, P. 94, (2023).
[45] Ryan Calo, *Artificial Intelligence Policy: A Primer and Roadmap,* **U.C.D L. Rev.**, Vol. 51 No. 2, P. 420, (2018).
[46] Ibid, P. 420-421.
[47] Ibid, P. 421.
[48] Ibid, P. 424-425.
[49] Ian Walden, Privacy and Data Protection in Chris Reed Edited Computer Law, Oxford University Press, 578, (7th Ed. 2011).

These international organizations aim to discourage organizations from avoiding data protection controls and to ensure a free flow of information.[50]

The United Nations is one of the international organization that actively working to ensure right to privacy. One of its efforts is the inclusion of the right to privacy under UDHR and ICCPR.[51] The right to privacy under these two treaties is a verbatim copy and it prohibits arbitrary and unlawful interference of individual's privacy, family, home and correspondence.[52] The Human Rights Committee provides that state authorities as well as natural and legal persons shall refrain from arbitrarily and unlawfully interfering with the individual's right to privacy.[53] Moreover, it provides that the right to privacy should encompass gathering and holding of personal information on computers, data banks and other devices.[54]

The Council of Europe is another international organization which adopted two treaties that protect personal data. The first one is ECHR which provides that an individual's right to respect for his private life, family life, home and correspondence shall be ensured.[55] However, the right may be limited as per the law and necessary in a democratic society if it is in the interest of national security, public safety, the economic well-being of the country, prevention of crime, protection of health or morals and protection of rights and freedoms of others.[56]

The second one is Convention 108[57] which was the foundation for international data protection law for fifty six member countries.[58] The Convention 108 and its modernized version the Convention 108+ are open to non-members of Council of Europe and in this regard Russia, three

[50] Ibid.
[51] Universal Declaration of Human Rights, G.A. Res. 217A (III), U.N. Doc. A/810, Art. 12, (1948) and International Covenant on Civil and Political Rights, 1966, 999 U.N.T.S. 171, Art. 17, (entered into force 1976).
[52] Ibid.
[53] Human Rights Committee, General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence and Protection of Honor and Reputation, U.N. Doc. HRI/GEN/1/Rev.9 (Vol. I), (1988).
[54] Ibid.
[55] ECHR, Art. 8/1. Convention for the Protection of Human Rights and Fundamental Freedoms, 1950, 213 U.N.T.S. 221 (entered into force 1953) (Herein after ECHR).
[56] ECHR, Art. 8/2.
[57] **Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 1981, C.E.T.S. No. 108 (entered into force 1985) (Herein after Convention 108).**
[58] Council of Europe, Explanatory Report on Convention for the protection of individuals with regard to the processing of personal data (Convention 108 +), P. 15, (2018).

Latin American and 6 African countries ratified the Convention 108.[59] The Convention 108 has incorporated basic principles of data protection and obliges the state parties to take a necessary measure for the adoption of these basic principles in their domestic legislations.[60] The other issue is that the Convention 108 was applicable to automatic processing of personal data but the recent amendment incorporates both automatic and manual processing to its scope.[61]

The European Union is the other international organization that is active in data protection sphere that is distinct from Council of Europe. The most important treaties of European Union are the Charter of Fundamental Rights[62] and the Data Protection Directive[63] which replaced by the GDPR recently.[64] As previously mentioned, the Charter is the first treaty that recognizes right to privacy and right to data protection separately. The other law is the Data Protection Directive which was adopted to ensure consistency that the Convention 108 failed to achieve.[65]

In 2018, the Data Protection Directive is replaced by the GDPR. The GDPR, unlike the directive which requires a national legislation to be effective, can be effective on all European Union member states.[66] The main reason for the adoption of the GDPR is to bridge the gap between the law and the practice created by the directive.[67] One should note that the GDPR has not changed the core principles of the directive but modernize the rules to reflect the changes in the world and introduce certain rights to the data subjects.[68]

---

[59] Graham Greenleaf, The New Data Protection Convention 108+ and its Importance for Asia, Presented at the Asian Privacy Scholars Network (APSN) Conference, P. 1, (2024).
[60] **Convention 108, Art. 4/1.**
[61] Council of Europe, Modernized Convention for the Protection of Individuals with Regard to the Processing of Personal Data, C.E.T.S. No. 108, Art. 3, opened for signature 2018.
[62] Charter of Fundamental Rights of the European Union OJ C 326/391, Arts. 7 and 8, (2012).
[63] **Directive 95/46/EC** on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31.
[64] European Union Regulation 2016/679 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, O.J. (L 119) 1, (2016).
[65] Peter Hustinx, *EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation*, **SCRIPTed, Vol. 9 No. 1, P. 9**, (2012).
[66] Bart Van Der Sloot & Frederik Zuiderveen Borgesius, *The EU General Data Protection Regulation: A New Global Standard for Information Privacy*, **Eur. Data Prot. L. Rev.** Vol. 6 No. 1, P. 1, (2020).
[67] Ibid.
[68] European Union Agency for Network and Information Security (ENISA), *Privacy by Design in Big Data: An Overview of Privacy Enhancing Technologies in the Era of Big Data Analytics*, P. 16, (2015).

The Organization for Economic Cooperation and Development has also adopted a guideline on data protection in 1980.[69] The guideline is applicable to personal data that is processed by public or private parties and the processing pose a risk to privacy and individual liberties.[70] Even though the guideline has no binding power, it has influenced international data protection frameworks including the GDPR and national laws.[71] The aim of the guideline is to create a balance between stringent data protection and facilitate a free data flow across the border.[72]

There are also other regional treaties that explicitly recognize the right to privacy. The first one is the American Convention on Human Rights which gives protection to the individual's privacy, family, home and correspondence.[73] The other one is the Arab Charter on Human Rights which provides the same protection as the American Convention on Human Rights to the individual's privacy, family, home and correspondence.[74] The other treaty is the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention) which has been adopted in 2014 as the first African instrument that addresses personal data protection.[75]

### 2.3 Global Standards and Best Practices in Data Protection

#### 2.3.1 General Data Protection Regulation

The General Data Protection Regulation (GDPR) is the recent law adopted by the European Union to govern data protection.[76] The GDPR ensures the data protection rights of natural persons and facilitate a free movement of data within the European Union.[77] The GDPR rules are applicable to extraterritorial entities that process personal data of individuals who lives in European Union.[78] The GDPR also states that its rules applies to processing of personal data

[69] Organization for Economic Cooperation and Development, Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data, (1980).
[70] Ibid, Art. 2.
[71] Waseem Zafer and Floris Huider, *OECD Guidelines and International Law: Navigating Data Protection and Privacy Regulations*, https://doi.org/10.13140/RG.2.2.14840.35849, P. 3-4, (2008).
[72] Ibid, P. 4.
[73] American Convention on Human Rights, 1969, 1144 U.N.T.S. 123, Art. 11, (entered into force 1978).
[74] Arab Charter on Human Rights, 2004, reprinted in Volume of 12 International Human Rights Reports 893 (2005), (entered into force Mar. 15, 2008).
[75] African Union Convention on Cyber Security and Personal Data Protection, 2014, O.A.U. Doc. EX.CL/846(XXV) (not yet in force).
[76] European Union Regulation 2016/679 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, O.J. (L 119) 1, (2016). (Herein after GDPR).
[77] Ibid, Art. 1.
[78] Ibid, Art. 3/2

wholly or partly by automated means and processing other than automatic which form a filing system or intended to form part of a filing system.[79]

The GDPR provides four instances in which the regulation does not apply. The first instance is when the issue is outside the scope of the European Union laws such as national security related data processing.[80] The second instance is when member states of the European Union carry out activities that fall under Chapter Two of Title V of Treaty of European Union which relates to common foreign and security policy.[81] The third instance is when a natural person process data simply for personal or household purposes.[82] The fourth instance is when competent authorities' process data to prevent, investigate, detect and prosecute criminal offences.[83]

The GDPR incorporates multiple principles in which any processing of personal data shall adhere to. The first principle is lawfulness, fairness and transparency.[84] The lawfulness requirement is that data processing shall be compliant with the rules of the GDPR, the fairness requirement can be compared to a good faith requirement and transparency is about disclosing ant processing Activity to the data subject.[85] The second principle is a purpose limitation in which the data should be processed for specified purpose not for other incompatible purposes.[86] The purpose should be specific, vague purposes such as ―…promoting consumer satisfaction, product development or optimizing services …‖ shall be prohibited.[87]

The third principle is data minimization in which the collected data shall be limited to what is necessary I relation to the purposes for which they are processed.[88] This principle prohibits collection of data that is not relevant for the purpose of the process at the time but could be in the future which in effect rejects big data analytics business models.[89] The fourth principle is data

[79] Ibid, Art. 2/1.
[80] Ibid, Art. 2/2/a.
[81] Ibid, Art. 2/2/b.
[82] Ibid, Art. 2/2/c.
[83] Ibid, Art. 2/2/d.
[84] Ibid, Art. 5/1/a.
[85] Chris Jay Hoofnagle et al., *The European Union General Data Protection Regulation: What It Is and What It Means*, Info. & Comm. Tech. L., Vol. 28, P. 77, (2019).
[86] GDPR, Art. 5/1/b.
[87] Chris Jay Hoofnagle et al., *The European Union General Data Protection Regulation: What It Is and What It Means*, P. 77, (2019).
[88] GDPR, Art. 5/1/c.
[89] Chris Jay Hoofnagle et al., *The European Union General Data Protection Regulation: What It Is and What It Means*, P. 78, (2019).

accuracy in which the personal data shall be accurate and up-to-date and inaccurate data shall be erased or rectified.[90] This principle does not require full accuracy of every aspect of the personal data rather accuracy regarding the purpose of which the personal data is processed.[91]

The fifth principle is the storage limitation in which a personal data shall not be stored longer than is necessary.[92] However, this principle has exceptions, in which the personal data is processed for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.[93] This principle is essential to protect the data from becoming irrelevant, excessive inaccurate or out of date.[94] The sixth principle is integrity and confidentiality which protects personal data security risks such as unauthorized and unlawful processing, accidental loss, destruction or damage.[95] The security risks can be curbed by adopting anonymization, encryption and deletion functionalities to the protection measures.[96]

The GDPR recognized various rights that data subjects are entitled to. The first one is the right to information and transparency in which the data controller shall disclose information.[97] The right of data subjects to information includes data obtained directly from the data subject and from other sources.[98] The right to access personal data is another right which includes being informed of purpose of processing, categories of data, recipients, retention period and the right to lodge a complaint with a supervisory authority.[99]

---

[90] GDPR, Art. 5/1/d.

[91] Chris Jay Hoofnagle et al., *The European Union General Data Protection Regulation: What It Is and What It Means*, P. 78, (2019).

[92] GDPR, Art. 5/1/e

[93] Ibid.

[94] European Public Service Union (EPSU), *The General Data Protection Regulation (GDPR): An EPSU Briefing*, P. 12, (2019).

[95] GDPR, Art. 5/1/e

[96] European Public Service Union (EPSU), *The General Data Protection Regulation (GDPR): An EPSU Briefing*, P. 24, (2019).

[97] GDPR, Art. 12.

[98] Ibid, Art. 13 and 14. These two provisions provides that data controllers shall communicate with data subjects the identity and contact details of the data controller and representative (if applicable), contact details of the Data Protection Officer (DPO) (if applicable), purpose of processing and legal basis, legitimate interests pursued by the data controller (if relevant), recipients or categories of recipients of the personal data, information on transfers to third countries and safeguards used. Article 14 provides two additional rights in which to be informed of the categories of the personal data concerned and source of personal data.

[99] Ibid, Art. 15/1.

The data subjects also have the right to rectify inaccurate personal data as well the right to have incomplete personal data completed.[100] The data subjects also have the right to request the erasure of their personal data if the personal data is no longer necessary, they withdraw their consent or object to the processing, the data was processed unlawfully, there is a legal obligation to erase the personal data and a requirement under Article 8/1 of the GDPR is fulfilled.[101] The data subjects have the right to temporarily restrict processing if the accuracy of the personal data is contested, processing is unlawful and the data subject prefers restriction over erasure, the personal data is no longer necessary and the requirement under Article 21/1 is fulfilled.[102]

The right to portability which ensures data subject‘s right to receive his/her personal data from data controller and transfer it to another controller is also protected provided that the processing is conducted based on consent and carried out by automatic means.[103] The data subjects have the right to object to the processing of personal data unless the data controller shows legitimate reason that overrides the rights of the data subjects.[104] The data subjects have the right to refuse decision solely based on automated means including profiling unless it is necessary for the performance of contract between data subject and data controller, it is authorized by the European Union or members states law or it is based on data subject‘s explicit consent.[105]

The other right that data subjects entitled to is withdrawal of consent.[106] The GDPR empowered the data subjects to withdraw their consent at any time and required that withdrawing of consent shall be as easy as giving consent.[107] In case where the processing of personal data infringes the GDPR rules, the data subject can lodge a complaint with a supervisory authority without prejudice to other administrative and judicial remedies.[108] Moreover, data subjects have the right to effective judicial remedies against the decision of the supervisory authority.[109]

[100] Ibid, Art. 16.
[101] Ibid, Art. 17.
[102] Ibid, Art. 18.
[103] Ibid, Art. 20.
[104] Ibid, Art. 21.
[105] Ibid, Art. 22.
[106] Ibid, Art. 7/3.
[107] Ibid.
[108] Ibid, Art. 77.
[109] Ibid, Art. 78.

The obligation of the data controllers under the GDPR closely corresponds to the rights that are granted to the data subjects. Hence, rights of data subjects that are previously discussed create comparable obligation on data controllers. However, besides these obligations, the GDPR recognized certain obligations. The first one is the obligation to record processing activities.[110] The record shall contain the name and contact detail of data controller, the purposes of processing, categories of data subjects and personal data, categories of recipients, transfer to third countries and safeguards, time limit for erasure and security measures.[111]
The data controller has an obligation to take security measures by taking into account the risk and the severity of its effect on data subjects including techniques such as pseudonymization and encryption of personal data, ensure confidentiality and integrity of processing systems, the ability to restore access to personal data in the event of accident, regularly checking the effectiveness of technical and organizational security measures.[112] However, despite these security measures, if personal data breach occurs, the data controller has an obligation to notify the supervisory authority without undue delay, where feasible, within seventy two hours.[113]

The data controller is required to assign data protection officer if the processing is conducted by public body except court‘s in their judicial role, if the core activities of the data controller involves large-scale, regular and systemic monitoring of data subjects and if the core activities of the data controller involves special category of data or data relating to criminal cases.[114] The other obligation of data controller is to conduct impact assessment where the processing uses new technologies and poses risks to the rights of data subjects.[115]

The other issue that should be discussed is the rules on cross-border transfer of personal data. The GDPR envisages three instances where personal data can be transferred across border.[116] The first one is the adequacy decision in which the transfer of personal data may be made where the European Commission decides the recipient ensures adequate level of protection.[117] If adequacy decision does not apply, the personal data shall be transferred if the recipient provides

[110] Ibid, Art. 30/1
[111] Ibid, Art. 30/1/a-g.
[112] Ibid, Art. 32/1.
[113] Ibid, Art. 33/1.
[114] Ibid, Art. 37/1.
[115] Ibid, Art. 35/1.
[116] Ibid, Art. 44.
[117] Ibid, Art. 45.

safeguards on the condition that enforceable rights and legal remedies are available to data subjects.[118]

In the case where adequacy decision and appropriate safeguards do not apply, the transfer of data shall take place if the data subject gives his/her consent for the transfer, the transfer is necessary for the performance of the contract between the data controller and data subject, if the transfer is necessary for the performance of the contract concluded between data controller and third party in the interest of data subject, the transfer is necessary for public interest, the transfer is necessary for establishment, exercise or defend legal claims, the transfer is necessary to protect interest of data subject when he/she cannot give his/her consent, the transfer is made from register to a person who can show legitimate interest.[119]

The other issue is enforcement and sanction of personal data protection rules. Under the GDPR, the supervisory authorities have investigative, corrective and authoritative & advisory power.[120] Investigative powers include ordering data controller to produce information, investigating in the form of data protection audits, accessing premises of the data controller, etc.[121] Corrective powers include issuing warning to the data controller, reprimanding data controller, ordering data controller to comply with the request of the data subject.[122] The authoritative and advisory powers includes issuing an opinion and approve draft codes of conduct, adopting standard data protection clauses, approving binding corporate rules, etc.[123]

The main problems of other European data protection instruments were lack of effective sanctions and low fines.[124] The GDPR incorporates provisions that resolve these issues including the recognition of data subject‘s right to compensation and data controller‘s liability in case of damage caused of processing of data that does not comply with the GDPR.[125] The administrative

[118] Ibid, Art. 46.
[119] Ibid, Art. 49.
[120] Ibid, Art. 58.
[121] Ibid, Art. 58/1
[122] Ibid, Art. 58/2
[123] Ibid, Art. 58/3
[124] Bart Van Der Sloot & Frederik Zuiderveen Borgesius, *The EU General Data Protection Regulation: A New Global Standard for Information Privacy*, P. 48, (2020).
[125] GDPR, Art. 82.

fine has been significantly changed[126] in which the fine is set to ten million euro or in case of undertaking two percent of preceding year annual worldwide turnover.[127]

### 2.3.2 The African Convention on Cyber Security and Personal Data Protection (The Malabo Convention)

The Malabo Convention provides the scope of its implementation. It governs any collection, processing, transmission, storage or use of personal data by natural person, the state, local communities, private or public corporate bodies.[128] The Malabo Convention applies in any processing activities whether it is automated or non-automated.[129] The territorial application of the Malabo Convention is set to be the territory of the state party.[130] The Malabo Convention also governs data processing in public security, defence, research, criminal prosecution and state security subject to exceptions provided under other extant laws.[131] The Malabo Convention does not apply in case of data processing undertaken by natural person for personal or household activities and on temporary copes produced to transmit or access personal data.

The Malabo Convention includes various principles of data protection. The first principle is consent in which the data processing is regarded as legitimate only if the data subject has given his/her consent.[132] The second principle is that collection, recording, processing, storage and transmission of personal data shall be conducted lawfully, fairly and non-fraudulently.[133] The third principle is that data processing shall have specific purpose and data collection shall not be excessive in relation to the purpose; in addition to that the personal data shall not be kept for longer than is necessary for the purpose.[134]

The fourth principle is that the data shall be accurate and up-to-date and inaccurate or incomplete personal data, having regard to the purposes for which they are collected and processed, shall be

[126] Bart Van Der Sloot & Frederik Zuiderveen Borgesius, *The EU General Data Protection Regulation: A New Global Standard for Information Privacy*, P. 49, (2020).
[127] GDPR, Art. 83/4.
[128] Malabo Convention, Art. 9/1/a.
[129] Ibid, Art. 9/1/b.
[130] Ibid, Art. 9/1/c.
[131] Ibid, Art. 9/1/d.
[132] Ibid, Art. 13/Principle 1.
[133] Ibid, Art. 13/Principle 2.
[134] Ibid, Art. 13/Principle 3.

erased or rectified.[135] The fifth principle is transparency in which the data controller shall disclose information on personal data.[136] The sixth principle is confidentiality and security in that the data controller shall protect the personal data particularly during transmission and ensure the implementation of security measures under the Malabo Convention.[137]

The Malabo Convention recognizes the rights of data subjects. The first one is the right to information in which the data subjects shall be informed of the identity of the data controller, the purpose of the processing, categories of data, recipients of the data, the right to request for erasure, the right to access and rectify the personal data, the period for which the data are stored and proposed transfer to third countries.[138] The second one is the right to access information relevant to evaluate or object processing, confirmation on whether data subject‘s personal data are being processed, communicate the processing personal data and their source and the purpose of processing, categories of personal data and recipients of personal data.[139]

The third one is the right to object, on legitimate grounds, the processing of the personal data.[140] Under this right, the data subjects have the right to be informed of any disclosure of personal data for the first time to third parties or usage of personal data for marketing purposes and shall be afforded the right to object to such disclosure or uses.[141] The fourth one is that data subjects have the right to demand the data controller to rectify, complete, block or erase the personal data if the personal data is inaccurate, incomplete, equivocal or out to date or the collection, use, disclosure or storage of that personal data is prohibited under the law.[142]

The Malabo Convention also provides four obligations of the data controller. The first one is that processing of data shall be confidential and undertaken by persons under the authority and on instructions of the data controller.[143] The second one is that the data controller shall take precautions to prevent data from being altered, destroyed or accessed by unauthorized parties.[144]

[135] Ibid, Art. 13/Principle 4.
[136] Ibid, Art. 13/Principle 5.
[137] Ibid, Art. 13/Principle 6.
[138] Ibid, Art. 16.
[139] Ibid, Art. 17.
[140] Ibid, Art. 18.
[141] Ibid.
[142] Ibid, Art. 19.
[143] Ibid, Art. 20.
[144] Ibid, Art. 21.

The third one is that the personal data shall not be kept for no longer than is necessary for the purpose for which the personal data is collected or processed.[145] The fourth one is that the data controller shall take measures to ensure that the processed personal data can be used regardless of the technical device employed in the process.[146]

The Malabo Convention provides that states parties shall establish an independent administrative authority that ensures the implementation of this convention in the processing of personal data.[147] These national authorities are responsible to respond to every request for an opinion regarding personal data processing, inform data subjects and data controllers their rights and obligations, authorize processing of personal data particularly sensitive data, etc.[148] The national authority can issue warning to data controllers who breach the Malabo Convention and send an official warning letter to stop the breaches.[149] If the data controller fails to comply with the official warning letter, the national authority can impose temporary withdrawal of authorization, permanent withdrawal of authorization or monetary fine.[150]

### 2.4 The Role of Technology in Digital Privacy Protection

The advancement of technology has brought many changes to the regulatory framework of the personal data protection.[151] The advancement has brought three types of instruments. The first is that the technologies that ensure personal data protection. One of these technologies is Privacy-Enhancing Technologies (PETs) which are designed to process and share personal data while protecting the privacy of the data subject.[152] PETs use differential privacy[153] and homomophic encryption[154] to protect the personal data.[155]

---

[145] Ibid, Art. 22.
[146] Ibid, Art. 23.
[147] Ibid, Art. 11/1.
[148] Ibid, Art. 12/2.
[149] Ibid, Art. 12/3.
[150] Ibid, Art. 12/4.
[151] John Babikian, Securing Rights: Legal Frameworks for Privacy and Data Protection in the Digital Era, Law Research Journal, P. 94, (2023).
[152] Nisha Tusharkumar Gajjar, *Data Privacy and Protection in the Digital Age: Emerging Trends and Technologies*, **IJEASM, Vol. 5 No. 4,** P. 2, (2024).
[153] Ibid. Differential privacy is a technique which adds randomness to datasets to obscure individual data points.
[154] Ibid. Homomorphic encryption is a technique which enables computations on encrypted data without needing to decrypt it.
[155] Ibid.

The other advancement is in terms of anonymization in which personal data is modified in such a way that data subjects cannot be re-identified and no information can be learned.[156] Anonymization is a stronger technique than de-identification which involves only to removal of possible identifiers from the personal data.[157] There is a tension between utility and privacy in anonymization in which less anonymization ensures utility of the personal data but compromise the privacy of the data subject, whereas, the strong anonymization can protect the privacy of the data subject but compromise the utility of the personal data.[158]

The other technique that protects personal data is encryption which transforms data in way only the authorized persons can read it.[159] However, there should be a mechanism where a person can conduct search and other computations on the file without the need to decrypt it.[160] In this regard, encrypted search is essential to retrieve information without disclosing personal data.[161] In this regard, the homomorphic encryption techniques that enable the analysis of the cipher text the same as the plain text with decrypting it has become important.[162]

The second is the infrastructural and security technologies. One of these technologies is blockchain which is known for its strong security features due to its decentralized approach to data management.[163] Blockchain is resistant to any tampering and suitable to financial transactions, supply chain management and voting systems.[164] The other technology is quantum cryptography in which it uses quantum mechanics to encrypt a data that is unbreakable by any other computed including quantum computer.[165]

The third one is analytical and monitoring technologies. AI is the main technology under this category which may threaten or protect privacy based on how it is utilized. In the negative aspect, AI has a potential to derive a sensitive data from publicly available data which could

[156] European Union Agency for Network and Information Security (ENISA), *Privacy by Design in Big Data: An Overview of Privacy Enhancing Technologies in the Era of Big Data Analytics*, Final Version 1.0, P. 27, (2015).
[157] Ibid.
[158] Ibid.
[159] Ibid, P. 38.
[160] Ibid.
[161] Ibid.
[162] Ibid, P. 40.
[163] Nisha Tusharkumar Gajjar, *Data Privacy and Protection in the Digital Age: Emerging Trends and Technologies*, P. 2, (2024).
[164] Ibid.
[165] Ibid.

compromise the data subjects privacy.[166] On the other hand, AI is transforming data protection strategies in threat detection and response in which it analyzes datasets quickly and identify potential security breaches or vulnerabilities of the dataset.[167]

[166] Ryan Calo, *Artificial Intelligence Policy: A Primer and Roadmap,* P. 420-421, (2018).
[167] Nisha Tusharkumar Gajjar, *Data Privacy and Protection in the Digital Age: Emerging Trends and Technologies*, P. 2, (2024).

# Chapter Three

# 3. Ethiopia's Personal Data Protection Law

## 3.1 Overview of Ethiopia's Legal Framework for Data Protection

Until recently, Ethiopia did not have a comprehensive legislation that protects personal data.[168] However, there are multiple laws that include provisions that deal with data protection. The first one is the FDRE Constitution which recognizes the right to privacy and then mentions what constitutes privacy such as one's person, home, property, notes, correspondence and communication by the means of telephone, telecommunication and electronic devices.[169] The wording of the provision suggests that it extends to cover the right to data protection.[170] Especially sub-article 2 protects personal data in digital space.[171]

This provision obliges the government not just to refrain from interfering but to protect it from other private or legal persons who may infringe it.[172] This provision also provides exceptional circumstances where the right to privacy may be restricted. These circumstances are required to be applied during compelling circumstances and based on specific law and their purpose shall be protection of national security or public peace, prevention of crimes, protection of health, protection of public morality or protection of the rights and freedoms of others.[173]

In relation to the FDRE Constitution, the status of international treaties shall also be mentioned. The FDRE Constitution explicitly recognized that any international treaty that is ratified by Ethiopia is integral part of the law of the land.[174] In this regard, Ethiopia has ratified ICCPR in 1993 G.C which makes the ICCPR part of the Ethiopian law. Moreover, government institutions are obliged to interpret the human rights under Chapter Three of the FDRE Constitution in light

[168] The Personal Data Protection Proclamation has issued in 2024 G.C.
[169] Proclamation of the Constitution of the Federal Democratic Republic of Ethiopia, (1995), Art. 26/1&2, Proclamation No 1, Neg. Gaz. Year 1 No. 1. (Hereinafter FDRE Constitution).
[170] Kinfe Micheal Yilma & Alebachew Birhanu, *Safeguards of the Right to Privacy in Ethiopia: A Critique of Laws and Practices*, **JEL, Vol. 26, No. 1, P.** 116-117, (2013).
[171] Berhan Taye & Roman Teshome, *Privacy and Personal Data Protection in Ethiopia*, CIPESA, P. 10, (2018).
[172] Ibid.
[173] FDRE Constitution, Art. 26/3.
[174] Ibid, Art. 9/4.

of UDHR, ICCPR and other international treaties.[175] These two provisions enable the provisions of these treaties on right to privacy to be applicable in Ethiopia.

There are also multiple subsidiary legislations that deal with personal data protection. One of those legislations is the Ethiopian Digital Identification Proclamation.[176] According to this proclamation, personal data consists of biometric data such as fingerprints, iris and facial photo[177] and demographic data such the name, nationality, date of birth, gender and domicile address.[178] The proclamation also separately provides what sensitive data consists of and these are racial or ethnic origin, genetic data, physical or mental health condition, political opinion, religious belief and information regarding criminal offences.[179]

The proclamation has rules on protection of personal data. One of the rules is that the registrant, as an owner of the personal data, has to give his/her consent for authentication process and this consent shall be given in standard consent form.[180] If a witness testifies for the registrant, he/she shall also fill in a standard consent form.[181] Without the registrant‘s consent, no one can collect, distribute, print, use, modify, provide data or transfer to third parties.[182]

However, if it is authorized by the law or the court order, the personal data may be disclosed or transferred to the relevant legal entities.[183] The only instance where personal data can be share without the authorization of the law or the court order is when the data is a summarized demographic report and statistical data.[184] In this regard, this data can be transferred only to legally authorized entities not other third parties.[185]

Digital ID Institution is also obliged to ensure confidentiality during collection, registration, authentication, storage and processing of personal data.[186] To ensure confidentiality, the

[175] Ibid, Art. 13/2.
[176] Ethiopian Digital Identification Proclamation, (2023), Proclamation No. 1284, Neg. Gaz., Year 29 No. 19.
[177] Ibid, Art. 2/5.
[178] Ibid, Art. 2/6 and 9/2.
[179] Ibid, Art. 18.
[180] Ibid, Art. 17/1 and 17/10.
[181] Ibid, Art. 17/11.
[182] Ibid, Art. 17/4 and 17/5.
[183] Ibid, Art, 17/6.
[184] Ibid, Art. 17/7.
[185] Ibid, Art. 17/9.
[186] Ibid, Art, 17/2.

Institution shall employ administrative, legal, procedural and technical measures.[187] Moreover, the collected personal data shall be organized and stored in secure database.[188] The proclamation also includes a data minimization principle which limits the collection of data to that which direct supports to the system.[189] The collected data shall be used only to the purpose it is collected for and any usage that is incompatible with that purpose is prohibited.[190]

The Freedom of the Mass Media and Access to Information Proclamation has also some provisions that have bearing on privacy.[191] The proclamation ensures that everyone has a right to seek, obtain or communicate any information held by public institutions and this right can only be restricted by the provisions of this proclamation.[192] The exceptional circumstance that warrants restriction of this right is if it causes unreasonable disclosure of personal information about third party including a person who passed away less than twenty years ago.[193]

Registration of Vital Events and National Identification Cards Proclamation provides that data shall be disclosed unless the individual gives consent or the court orders.[194] However, if the disclosure prejudiced a public interest, a personal data shall not be shared to third parties even if the individual gives consent.[195] The proclamation provides instances where a personal data can be disclosed without obtaining the individual‘s consent or court order, these are national intelligence and security services, crime prevention and investigation, tax collection, administrative and social services, implementation of risk management systems of financial institutions and other purposes authorized by law.[196]

Electronic Signature Proclamation is another law that deals with data protection.[197] Under the proclamation there are certificate providers who provide a digital certificate, encryption service

[187] Ibid, Art. 17/12.
[188] Ibid, Art. 17/13.
[189] Ibid, Art. 17/3.
[190] Ibid, Art. 17/8&9.
[191] Freedom of the Mass Media and Access to Information Proclamation, (2008), Proclamation 590, Neg. Gaz., Year 14 No. 64. The provisions of this proclamation concerning mass media are repealed by the Media Proclamation No. 1238/2021.
[192] Ibid, Art. 12/1 and 15/1.
[193] Ibid, Art. 16/1.
[194] Registration of Vital Events and National Identification Cards Proclamation, (2012), Art. 64/3, Proclamation No. 760, Neg. Gaz. Year 18 No. 58.
[195] Ibid, Art. 64/5.
[196] Ibid, Art. 64/1.
[197] Electronic Signature Proclamation, (2018), Proclamation No. 1072, Neg. Gaz., Year 24 No. 25.

and time stamp service.[198] The certificate providers are obliged to adhere to two rules.[199] The first rule is that certificate provides are obliged to keep the personal information confidential except for grounds provided by law.[200] The second is that the certificate providers shall keep the information for two years but failed to provide what should be done in the aftermath.[201]

The other law is the Telecom Fraud Offence Proclamation which provides that police can conduct a covert search upon a court warrant if a telecom fraud offence has been committed or is likely to be committed.[202] Moreover, any evidence that is gathered through digital or electronic devices, evidences gathered through interception and surveillance and information obtained through interception by foreign enforcement body are admissible in court.[203]

The Computer Crime Proclamation is another law that somehow protects and also threatens individual's privacy right. The proclamation includes a provision that requires service providers to retain computer traffic data for one year but in the meantime this data shall not be disclosed unless there is a court order.[204] However, in relation to computer crime prevention, the investigators are empowered to conduct interception and surveillance upon court warrant.[205] This law even goes to the extent that it allows the Attorney General to order interception and surveillance without court warrant if there are reasonable grounds and urgent cases that the computer crime can damage critical infrastructure.[206]

The Criminal Code has included certain provisions that criminalize the act which infringes the individual's privacy rights.[207] In this regard, entering to a home without the consent of the lawful occupant can entail criminal liability.[208] Moreover, opening a business or private letter, envelope or correspondence; or access electronic, telegram, telephone of communication correspondence;

[198] Ibid, Art. 22/1.
[199] Ibid, Art. 29.
[200] Ibid, Art. 29/2.
[201] Ibid, Art. 29/1.
[202] Telecom Fraud Offence Proclamation, (2012), Art. 14, Proclamation No. 761, Neg. Gaz., Year 18, No. 61.
[203] Ibid, Art. 15.
[204] Computer Crime Proclamation, (2016), Art. 24, Proclamation No. 958, Neg. Gaz., Year 22 No. 83.
[205] Ibid, Art. 25/1.
[206] Ibid, Art. 25/3.
[207] Criminal Code, (2004), Arts. 604-606, Proclamation No, 414, Neg. Gaz.
[208] Ibid, Art. 604/1.

or opening a packet, a sealed parcel or consignment that is addressed to another person whether it is intentional or negligent can entail criminal liability.[209]

### 3.2 Key Provisions of the Personal Data Protection Proclamation

Ethiopia did not have a data protection law before 2024.[210] A year before its enactment, the Ethiopian Digital Identification Proclamation came into effect, which brought with it some protection mechanisms for data collected for digital identification purposes.[211] However, the proclamation only applied to data collected by the National ID, leaving other government institutions and private parties who process personal data outside its scope. In this regard, the Personal Data Protection Proclamation has been essential to fill the legal gap.[212]

The PDPP has defined it scope of application from three standpoints; subject-matter, material and territorial scope. The subject-matter scope of the PDPP is clearly defined in that it applies to any entity whether public or private institution in federal and regional governments including the Addis Ababa and Dire Dawa City administrations.[213] The wording of the provisions shows that any institution that collects and process personal data is governed by the PDPP.[214]

The material scope of the PDPP is also defined from the perspective of the data processing mechanism that is used by the data controller. The processing of data shall be subject to the PDPP if it employs wholly or partly one of these two processing mechanisms.[215] The first one is that the processing of personal data shall be made by an automated device.[216] The automated device is defined under the PDPP as ―A device that makes decisions, initiates or implements actions without interventions based on certain environmental conditions, time or data based on pre-arranged algorithm and configuration.‖[217]

The second one is that data processing which is not conducted by automated devices can be subject to the PDPP if the personal data form part of a filing system or are intended to form part

[209] Ibid, Art. 606/1.
[210] DLA Piper, Data Protection Laws of the World: Full Handbook, P. 353-356, (2023).
[211] Ethiopian Digital Identification Proclamation, Art. 5.
[212] Personal Data Protection Proclamation, (2024), Proclamation No. 1321, Neg. Gaz., Year 30 No. 35. (Herein after PDPP).
[213] Ibid, Art. 3/3
[214] Ibid.
[215] Ibid, Art. 3/1
[216] Ibid
[217] Ibid, Art. 2/26.

of a filing system.[218] A filing system is defined under the PDPP as ―A structured set of personal data which is accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis‖.[219] However, the proclamation has not provided what evidence should be adduced to prove that the personal data were intended to be part of the filing system. And in case of dispute, which has the burden of prove this fact; the data subject, the data controller or the regulator is not clear.

The territorial application of the PDPP is also provided. In this regard, the PDPP applies to data controller if either of these two requirements is met. The first one is that if the data controller is established in Ethiopia and the personal data is processed in the context of that establishment, it can be subject to the PDPP.[220] The second one is that non-resident data controller can be subject to the PDPP if it uses equipment physically located in Ethiopia for processing or personal data and the data controller has representative in Ethiopia.[221] However, if the personal data is merely transiting through Ethiopia the PDPP is not applicable.[222]

In recent years, the global data flow has significantly increased, which raises concerns about privacy and data protection.[223] Currently, countries follow four approaches regarding personal data protection in case of cross-border transfer.[224] The first one is that countries with no data protection law such as Afghanistan, Haiti and Turkmenistan. The second one is countries that hold the company that transfers data across the border accountable if something goes wrong such as Australia, Brazil, and South Korea. The third one is that countries rely on the determination of adequacy through binding corporate rules, contractual clauses and consent such as Canada, European Union member states, Japan, etc. The fourth one is countries requiring relevant authorities' approval on a case-by-case basis such as China, India and Russia.

The PDPP incorporates the third and fourth approaches. Consistent with the third approach, the PDPP empowers data controllers to transfer data across borders after they determine that the

[218] Ibid, Art. 3/1.
[219] Ibid, Art. 2/25.
[220] Ibid, Art. 3/2/a.
[221] Ibid, Art. 3/2/b.
[222] Ibid.
[223] Anvesha Singh, Cross-Border Data Transfers: Legal Challenges and Solutions in the Globalized Digital Economy, IJIRL, Vol. 4 No. 1, P. 357, (2024).
[224] OECD Going Digital Toolkit, Trade and Cross-Border Data Flows, Policy Note, P. 10, (2021).

third-party jurisdiction has the appropriate level of protection, if they secure the consent of the data subject, it the transfer is necessary or the transfer is made from the register which is intended to provide information to the public.[225] The fourth approach is also present in the PDPP, in which the Ethiopian Communication Authority has a mandate to prohibit, suspend or subject the transfer to such conditions as may be determined.[226]

The transfer of personal data to third-party jurisdiction shall be subject to the PDPP and the third-party jurisdiction shall guarantee an appropriate level of protection.[227] To determine whether the third-party jurisdiction has the appropriate level of safeguards, all circumstances surrounding the transfer should be considered.[228] These factors are the nature of the data, the country of origin and destination and the laws of third-party jurisdiction.[229] The transfer of personal data to third party jurisdictions that do not have appropriate safeguards is prohibited.[230] However, the Ethiopian Communication Authority can facilitate limited transfer despite the absence of appropriate safeguards provided that the data subject‘s rights are not violated, the data subject has given consent and severance and reduction of those aspects of personal data.[231]

The PDPP also provides various principles in which data processing shall be complied with. The first one is lawful, fair and transparent processing of data.[232] This principle is indispensable because all principles embrace this principle.[233] Lawfulness principle requires that any processing shall be made if the data subject has given his/her consent, out of necessity for contractual performance with the data subject, necessary to comply with legal obligation, necessary to protect the vitally important interest of the data subject, necessary to respond to national emergency and necessary for the purposes of legitimate interests.[234] Fair and transparent

[225] PDPP, Art. 20/1.
[226] Ibid, Art. 21/2.
[227] Ibid, Art. 18.
[228] Ibid, Art. 19/1.
[229] Ibid, Art. 19/2.
[230] Ibid, Art. 19/5.
[231] Ibid, Art. 19/3&4.
[232] Ibid, Art. 6/1.
[233] Lee A. Bygrave, Data Protection Law: Approaching Its Rationale, Logic and Limits, Kluwer International Law, Information Law Series-10, 58, (2002).
[234] PDPP, Art. 7/2.

principle is another one that informs data subjects of the process and it entails an obligation to data controller to provide information in concise, intelligible and accessible format.[235]

The purpose limitation principle is a cluster of three principles which are the purpose shall be specified, the purpose shall be lawful and the purpose in which the data is further processed shall be compatible with the purpose in the first place.[236] To fulfill this obligation, the data controller shall give notice to the data subject or description to the Ethiopian Communication Authority.[237] Data minimization is another principle that complements the purpose limitation principle.[238] To fulfill the data minimization principle, the data shall be adequate, relevant and not-excessive in relation to the purpose.[239] The wording of this provision shows that it aims to ensure data minimization at the stage of the data collection.[240]

There is also a principle that governs the minimization of data at subsequent stages and it requires the erasure or anonymization of the personal data.[241] The principle is the storage limitation in which personal data shall be stored and retained for a reasonable period of time that is necessary to achieve the purpose.[242] However, the personal data may be retained indefinitely if it is provided by the law, the data subject gives his/her consent, necessary for lawful purposes and necessary for historical, statistical, literary and research purposes.[243]

Data accuracy is another principle which emphasizes that the personal data shall not only be valid but also up-to-date.[244] The PDPP provides negative definition for data accuracy in which if the data controller takes reasonable steps to verify the accuracy and if the data subject notified the data controller about the inaccuracy and the data indicates that fact, then the inaccuracy shall not be regarded to contravene the PDPP.[245] Accountability is another principle which requires

[235] Ibid, Art. 12/1.
[236] Lee A. Bygrave, Data Protection Law: Approaching Its Rationale, Logic and Limits, 61, (2002).
[237] PDPP, Art. 13/1.
[238] Samuel Worku, The Right to Privacy in the Age of Surveillance: Personal Data Protection in Ethiopia, Master's Thesis, Addis Ababa University School of Law, P. 43, (2024).
[239] PDPP, Art. 6/3.
[240] Lee A. Bygrave, Data Protection Law: Approaching Its Rationale, Logic and Limits, 60, (2002).
[241] Ibid.
[242] PDPP, Art. 15/1.
[243] Ibid, Art. 15/2.
[244] Samuel Worku, The Right to Privacy in the Age of Surveillance: Personal Data Protection in Ethiopia, P. 46, (2024).
[245] PDPP, Art. 14.

processing of personal data to comply with the rules of the PDPP and other relevant laws.[246] This principle creates a framework in which a regulatory authority can require reports and impose sanctions on data controllers in case of non-compliance with the PDPP.[247]

The principle of integrity and confidentiality requires the data controller to ensure that the employees are reliable and external data processors provide sufficient guarantee of protection.[248] Hence, the data controller has to conduct regular testing, assessment and evaluation to ensure integrity and confidentiality.[249] The principle of security requires data controllers to take appropriate measures against unauthorized or unlawful processing, accidental loss, destruction or damage to the personal data.[250] The measures in this regard shall be proportionate to the level of risk and take the state of the art and cost of the implementation of these measures.[251]

### 3.3 Rights of Data Subjects Under the Personal Data Protection Proclamation

In the processing of personal data, data subjects have extensive rights under the PDPP. The first one is the right to be informed of the name and contact details of the data controller, the purposes of the processing, the lawful basis of the processing, the recipients of the personal data, the right to withdraw consent, etc.[252] If the personal data are obtained from third party, the data controller has to provide information to the data subject of the categories of the personal data and the source of personal data.[253] This right shall also include that right to be informed if the purpose of the processing has changed before the processing takes place.[254]

The data subject has a right to access his/her personal data free of charge but for any further copies requested, the data controller can charge a reasonable fee to cover administrative cost.[255] The data subject has a right to obtain the confirmation of the processing of his/her personal data,

[246] Ibid, Art. 52.
[247] Samuel Worku, The Right to Privacy in the Age of Surveillance: Personal Data Protection in Ethiopia, P. 49, (2024).
[248] PDPP, Art. 16/1.
[249] Samuel Worku, The Right to Privacy in the Age of Surveillance: Personal Data Protection in Ethiopia, P. 49, (2024).
[250] Ibid, Art. 17/1.
[251] Lee A. Bygrave, Data Protection Law: Approaching Its Rationale, Logic and Limits, 68, (2002).
[252] PDPP, Art. 24/1.
[253] Ibid, Art. 24/2.
[254] European Public Service Union (EPSU), *The General Data Protection Regulation (GDPR): An EPSU Briefing*, P. 17, (2019).
[255] Bart Van Der Sloot & Frederik Zuiderveen Borgesius, *The EU General Data Protection Regulation: A New Global Standard for Information Privacy*, **Eur. Data Prot. L. Rev.** Vol. 6 No. 1, P. 35, (2020).

all available information of their origin, the duration of data storage, etc.[256] The data controller can refuse to disclose the personal data where the disclosure would unjustifiably invade another person's privacy, the data pertains to legal privilege, the personal data concerns health and medical information and disclosure could harm the data subject, etc.[257]

The data subjects have a right to rectify inaccurate personal data by using different mechanism such as adding supplementary statement.[258] Under the PDPP, where the data is inaccurate, incomplete, misleading, not-up-to-date or is processed contrary to the PDPP, the data subject shall have the right to request the data controller to correct the data.[259] The data controller shall disclose the correction to another data controller or third person to whom the data has been disclosed during the one year before the request.[260]

The data subjects have the right to request the erasure of personal data where the personal data are no longer necessary for the purpose of collection or processing, the data subject withdraws his/her consent for the processing of the personal data, the data subjects object the processing or the personal data has been processed unlawfully.[261] The right to erasure may be restrict for reasons of public interest, historical, statistical or scientific research, to comply with a legal obligation and to establish, exercise or defend a legal claim.[262] In this regard, the right to erasure is conditional not absolute and in certain circumstances data controllers may refuse to erase the personal data by adducing a legitimate ground that override the data subjects rights.[263]

The data subjects have a right to object to the processing of personal data at any time in written form for purposes such as direct marketing including profiling to the extent the is related to the direct marketing.[264] However, the data controller can refuse the request of data subjects by demonstrating in writing compelling legitimate grounds that override the data subject's rights.[265]

---

[256] PDPP, Art. 25/1.
[257] Ibid, Art. 26/1.
[258] Bart Van Der Sloot & Frederik Zuiderveen Borgesius, *The EU General Data Protection Regulation: A New Global Standard for Information Privacy*, P. 36, (2020).
[259] PDPP, Art. 27/1.
[260] Ibid, Art. 27/2.
[261] Ibid, Art. 28/1.
[262] Ibid, Art. 28/3.
[263] European Public Service Union (EPSU), *The General Data Protection Regulation (GDPR): An EPSU Briefing*, P. 19, (2019).
[264] PDPP, Art. 29.
[265] Ibid, Art. 29/1.

The data controller has to stop processing the personal data when it receives the objection but the objection does not imply that the personal data shall be erased.[266]

The right to restriction of processing is another right that limits the way the data controller can use the personal data.[267] This right can be exercised where the accuracy of the personal data is contested for the period to verify the claim, the data controller is no longer needs the personal data and the data subjects need that to establish, exercise or defend legal claims, the processing is unlawful bit the data subject prefers restriction over erasure of personal data, objection is made under Article 29 pending the verification of whether the data controller‘s legitimate grounds override the data subject rights.[268] During restriction, the data controller can only store or process the personal data with the data subjects consent to establish, exercise or defend the legal claim, to protect the rights of others or for the reasons of public interest.[269]

Data subjects have a right not to be subject to a decision based solely on automated processing including profiling, to require human intervention and to express their view on the issue.[270] However, the right can be restricted if it is necessary to enter and perform contract between the data subject and the data controller, authorized by a law or it is based on the data subjects explicit consent.[271] Even these restrictions exist; automated processing that intends to evaluate certain personal aspects of the data subjects shall not be based on sensitive personal data.[272] This right ensures that data subjects are informed of the logic involved in the automated decision-making process.[273] In this regard, the data controller shall take measures to prevent bias, discrimination and error in the automated decision-making process.[274]

[266] European Public Service Union (EPSU), *The General Data Protection Regulation (GDPR): An EPSU Briefing*, P. 20, (2019).
[267] Ibid, P. 19.
[268] PDPP, Art. 30/1.
[269] Ibid, Art. 30/2.
[270] Ibid, Art. 31/1
[271] Ibid, Art. 31/2
[272] Ibid, Art. 31/3.
[273] European Public Service Union (EPSU), *The General Data Protection Regulation (GDPR): An EPSU Briefing*, P. 21, (2019).
[274] Ibid.

The right to portability is the other one that enables the free flow of the personal data and assists data subjects to switch service providers.[275] Data subjects have the right to receive the data they provide to the data controller in a structured, commonly used and machine-readable format.[276] Data subjects can also transmit the personal data they received to another data controller and if the technology allows they can request the data controller to transmit the personal data to another data controller directly.[277] However, the right shall not be applicable if the processing is necessary to the performance conducted under the public interest or exercise of official duty or it adversely affects the rights and freedoms of others.[278]

### 3.4 Obligations of Data Controllers and Processors

Under the PDPP, the data controller is a natural or legal person who processes personal data and determines the purpose and means of processing personal data.[279] Data processors are also natural or legal person other than the data controller's employee who processes personal data on behalf of the data controller.[280] To process personal data, the data controller and data processor shall be registered with the Ethiopian Communication Authority.[281] The Ethiopian Communication Authority has the power to reject the application for registration where the particulars provided for inclusion are insufficient.[282] The obligation of the data controllers corresponds to the rights of the data subjects. Hence, the rights of the data subjects create comparable obligation on the data controllers.

The data controller has an obligation to take technical and organizational measures by taking into account the nature, scope, context, and purposes of the processing and the risks for the data subject's rights.[283] The required obligations are implementing data security and organizational

[275] Ibid, P. 20.
[276] PDPP, Art. 32/1.
[277] Ibid, Art. 32/2&3.
[278] Ibid, Art. 32/4.
[279] Ibid, Art. 2/10 and 2/39.
[280] Ibid, Art. 2/11 and 2/39.
[281] Ibid, Art. 33/1.
[282] Ibid, Art. 34/1.
[283] Bart Van Der Sloot & Frederik Zuiderveen Borgesius, *The EU General Data Protection Regulation: A New Global Standard for Information Privacy*, P. 30, (2020). These security measures can include pseudonymization and encryption; the ability to ensure the ongoing confidentiality; integrity, availability, and resilience of systems and services processing personal data; the ability to restore the availability and access to data in a timely manner in the event of a physical or technical incident; and a process for regularly testing, assessing, and evaluating the effectiveness of security measures.

measures, keeping the record of processing, performing data protection impact assessment, obtain prior authorization or consultation with the Ethiopian Communication Authority and assigning data protection officer.[284] To ensure verification of the effectiveness of these measures, the data controller is required to implement internal policies and mechanisms.[285]

The data controller is obliged to assign a data protection officer in three instances.[286] The first one is that when the processing of personal data is conducted by the government institutions except the courts in their judicial capacity.[287] The second one is when the core activities of the data controller require regular and systematic monitoring of data subjects on a large scale.[288] The third one is when the core activities of the data controller require processing of sensitive personal data on a large scale.[289] The data protection officer, other than monitoring the compliance of with the law, he/she can act as a contact point for the supervisory authority.[290]

A failure to ensure data security can entail personal data breach and in this context breach can be defined broadly to include incidents that affect the confidentiality, integrity and availability of the personal data.[291] The data controller has an obligation to notify personal data breach to the Ethiopian Communication Authority within seventy two hours after becoming aware of it.[292] The data controller shall also notify the personal data breach to the data subjects after becoming aware of it without undue delay.[293] The notification to the Ethiopian Communication Authority and the data subject shall include the nature of the personal data breach, the name and contact

[284] PDPP, Art. 42/1&2.
[285] Ibid, Art. 42/3.
[286] Ibid, Art. 40/1.
[287] Ibid, Art. 40/1/a
[288] Ibid, Art. 40/1/b.
[289] Ibid, Art. 40/1/c.
[290] Bart Van Der Sloot & Frederik Zuiderveen Borgesius, *The EU General Data Protection Regulation: A New Global Standard for Information Privacy*, P. 32, (2020). The PDPP under Article 41/1 provides that: The responsibility of a data protection officer shall be to: a) Support the data controller or data processor and their employees on data processing requirements provided under this Proclamation or any other law; b) Ensure on behalf of the data controller or data processor that this Proclamation is complied with; c) Facilitate capacity building of staff involved in data processing operations; d) Provide advice on data protection impact assessment; and e) Cooperate with the Authority and any other authority on matters relating to data protection.
[291] Samuel Worku, The Right to Privacy in the Age of Surveillance: Personal Data Protection in Ethiopia, P. 47, (2024).
[292] PDPP, Art. 43/1.
[293] Ibid, Art. 44/1.

details of the data protection officer, the likely consequences of the personal data breach, the measures taken or proposed to be taken to address the personal data breach.[294]

The data controller is obliged to maintain a record of processing activities including logging.[295] The record shall consists of the name and contact detail of the data controller, the purpose of the processing, categories of data subjects and personal data, recipients of the personal data, transfer to other countries and the safeguards, the time limit to erase the personal data and the mechanism of the data security.[296] This rule is adopted to replace the requirement that data controllers shall notify the supervisory authority before processing personal data.[297]

The data controller shall conduct a data protection impact assessment[298] on the impact of the processing activities on the data subject‘s rights by taking into account their nature, scope, context and purposes.[299] The processing activities are systemic and extensive evaluation of personal aspects of individuals based on automated processing including profiling, processing of sensitive personal data on a large scale, systemic monitoring of publicly accessible areas on a large scale and any other processing activities which require consultation with the Ethiopian Communication Authority.[300] The impact assessment shall include a description of the processing and its purpose including any legitimate interest, evaluation of the necessity and proportionality of the processing, assessment of risks to data subjects‘ rights and measures and safeguards to address risks and ensure compliance.[301]

Where there are risks, the data controller shall consult the data protection officer and after that the supervisory authority before processing the personal data.[302] Under the PDPP, where the data controller cannot provide an appropriate safeguard in relation to the transfer of personal data to other country, it shall obtain the authorization from the Ethiopian Communication Authority to

[294] Ibid, Art. 43/4 and 44/2.
[295] Ibid, Art. 46/1.
[296] Ibid, Art. 46/2.
[297] Bart Van Der Sloot & Frederik Zuiderveen Borgesius, *The EU General Data Protection Regulation: A New Global Standard for Information Privacy*, P. 28-29, (2020).
[298] Ibid, P. 32. The idea of conducting impact assessment on data protection is inspired by environmental law.
[299] PDPP, Art. 47/1.
[300] Ibid, Art. 47/2.
[301] Ibid, Art. 47/3.
[302] European Data Protection Supervisor, *Accountability on the Ground Part II: Data Protection Impact Assessments & Prior Consultation, P. 19, (2019).*

ensure compliance with the PDPP and mitigate the risks.[303] This authorization shall be sought when the impact assessment indicates that the processing activities are likely to present a high risk or the Ethiopian Communication Authority decides that prior consultation is necessary for processing activities that are likely present a high risk.[304]

### 3.5 Institutional and Enforcement Mechanisms

The Ethiopian Communication Authority is mandated to ensure the enforcement of the PDPP, the compliance of data processing with the principles under the PDPP, determine in issues relating to cross-border transfer, etc.[305] The monitoring activity of the Ethiopian Communication Authority may arise from the its staff's regular activities or from complaints submitted by any interested party.[306] If the Ethiopian Communication Authority determines that the data controller contravene the PDPP, certain measures can be taken:- these are enforcement order, administrative sanction and criminal sanction.

Where the data controller has contravened, is contravening or is about to contravene the PDPP, the Ethiopian Communication Authority may issue an enforcement order.[307] The enforcement order shall specify the provision of the PDPP that has been, is being or is likely to be contravened, the measures that shall be taken, the period not less than twenty one days within which the measures shall be implemented, the availability of the right to appeal.[308]

The Ethiopian Communication Authority can impose administrative penalties where the data controller contravenes the PDPP.[309] The administrative penalties shall be effective, proportional and dissuasive.[310] Where the offence is committed by an institution, in relation to sensitive data or against the personal data of a minor, the offence will be punishable by a fine up to 4% of the data controller‘s total worldwide turnover of the preceding financial year.[311]

[303] PDPP, Art. 48/1.
[304] Ibid, Art. 48/2.
[305] Ibid, Art. 5.
[306] Ibid, Art. 57.
[307] Ibid, Art. 55/1.
[308] Ibid, Art. 55/2.
[309] Ibid, Art. 60/1.
[310] Ibid, Art. 59/1.
[311] Ibid, Art. 60/2.

Any person, who fails to notify a data breach, does not implement technical and organizational measures when a breach is committed or processes personal data in contravention of the PDPP shall be punished by simple imprisonment from one to three years or fined from sixty thousand to one hundred thousand birr or both.[312] Moreover, any person who violates the rights of the data subject such as the right to erasure, the right to object, the right to restrict processing or the right against automated decisions shall be punished by imprisonment from three years to five years or fined from one hundred thousand to two hundred thousand birr or both.[313]

Any person who re-identifies personal data which has been de-identified, processes the re-identified personal data, sells or offers to sell personal data, transfers the personal data outside of Ethiopia in violation of the PDPP, shall be punished with serious imprisonment from five years to ten years or fined from two hundred thousand to six hundred thousand or both.[314] However, if the aforementioned offences have been committed by an institution, have caused any damage and became serious offence, have been committed in relation to sensitive data or have been committed in relation to personal data of a minor, it shall be punishable with a fine up to four per cent of its total worldwide turnover of the preceding financial year.[315]

[312] Ibid, Art. 64/1.
[313] Ibid, Art. 64/2
[314] Ibid, Art. 64/3.
[315] Ibid, Art. 64/4.

# Chapter Four

# 4. Comparative Analysis of Ethiopia's Data Protection Law

## 4.1. Comparison with the European Union's GDPR

The GDPR and the PDPP have shared various rules on data protection with some explicit differences that make them distinct. One of benchmarks that these two laws should be contrasted is the scope of their application.[316] The first one is the subject-matter jurisdiction of both laws in which in case of the GDPR protects natural persons with the objective of governing processing of personal data and free movement of personal data.[317] In the case of the PDPP, it is similar to the GDPR in its application to natural persons and to processing of personal data.[318] The GDPR includes the rule on free transfer of personal data between the European Union countries[319] and provide separate rules for cross-border transfer to third party jurisdictions.[320]

Both the GDPR and the PDPP have the same material scope in which if the processing of personal data is conducted wholly or partly by automated means or other than automated means which forms part of filing system or is intended to form part of filing system it should be under the scope of the laws.[321] However, unlike the GDPR, the PDPP provides definition for what automated device and filing system means.[322] Thus, automated device is ―A device that makes decisions, initiates or implements actions without interventions based on certain environmental conditions, time or data based on pre-arranged algorithm and configuration.‖[323] A filing system is ―A structured set of personal data which is accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis‖.[324]

The GDPR has a territorial jurisdiction in two instances.[325] The first one is that when the data controller is established in the European Union in which case the GDPR is applicable even if the

[316] GDPR, Art. 1-3 and PDPP, Art. 3 and 53.
[317] GDPR, Art. 1/1.
[318] PDPP, Art. 3/1.
[319] GDPR, Art. 1/3.
[320] Ibid, Art. 44-50.
[321] GDPR, Art. 2/1 and PDPP, Art. 3/1.
[322] PDPP, Art. 2/25 and 2/26
[323] Ibid, Art. 2/26.
[324] Ibid, Art. 2/25.
[325] GDPR, Art. 3.

processing of personal data takes place outside of European Union.[326] The second instance is where the data controller is not established in European Union in which the GDPR is applicable if the processing relates to offering of goods or services to data subjects in the European Union or the monitoring of their behavior which takes place within the European Union.[327] The PDPP also provides two instances for its territorial application.[328] The first one is that the data controller is established in Ethiopia and the personal data is processed in that establishment.[329] The second one is if a non-resident data controller uses equipment physically located in Ethiopia for processing of personal data and the data controller has representative in Ethiopia.[330]

The PDPP differs from the GDPR in its territorial scope. Under the PDPP, resident data controllers are subject to the law if they process the personal data in the context of their Ethiopian establishment.[331] However, the GDPR is applicable to resident data controllers even if the processing of personal data takes place outside of European Union.[332] The other difference concerns non-resident data controllers in which the GDPR is applicable to non-resident data controllers if the processed personal data relates to offering of good and services and monitoring of behavior of data subjects regardless of the processing takes place in European Union.[333] In contrast to the GDPR, the PDPP is applicable only if the data controller uses equipment physically located in Ethiopia and has representative in Ethiopia.[334]

The limitation on the scope of the GDPR and the PDPP has both similarity and difference. The similarity is that both the GDPR and the PDPP exclude the processing of personal data by an individual for a personal or household activity.[335] The other similarity is that both the GDPR and the PDPP are not applicable in cases of national security, defence and public security.[336] However, the GDPR and the PDPP each contain distinct exceptions that limit their respective scope of application. For instance, in case of the GDPR, it provides that activities which fall

[326] Ibid, Art. 3/1.
[327] Ibid, Art. 3/2.
[328] PDPP, Art. 3/2.
[329] Ibid, Art. 3/2/a.
[330] Ibid, Art. 3/2/b.
[331] Ibid, Art. 3/2/a.
[332] GDPR, Art. 3/1.
[333] Ibid, Art. 3/2.
[334] PDPP, Art. 3/2/b.
[335] GDPR, Art. 2/2/c and PDPP, Art. 3/4/a.
[336] GDPR, Art. 2/2/a & 2/2/d and PDPP, Art. 53/2/a.

within the scope of Chapter 2 of Title V of the TEU including the foreign policy and processing for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties are excluded from its scope.[337]

In the case of the PDPP, the exceptions that limit its scope are the processing relates to the exchange of information between government agencies where such exchange is required on a need-to-know basis; originating from a country outside of Ethiopia and merely transiting through Ethiopia to the third country; historical, statistical and scientific research; an objective of general public interest including an economic or financial interest of the country and the protection of judicial independence and judicial proceedings.[338]

In the case of principles of processing of personal data both the GDPR and the PDPP provides principles that have similar contents. The first one is that both the GDPR and the PDPP requires that processing of personal data shall be lawful, fair and transparent.[339] Lawfulness principle requires that any processing shall be made if the data subject has given his/her consent, out of necessity for contractual performance with the data subject, necessary to comply with legal obligation, necessary to protect the vitally important interest of the data subject, necessary to respond to national emergency and necessary for the purposes of legitimate interests.[340] Fair and transparent principle is another one that entails an obligation to data controller to provide information in concise, transparent, intelligible and easily accessible format.[341]

The purpose limitation principle is the other than in which both the GDPR and the PDPP provides that the purpose shall be specified, the purpose shall be lawful and the purpose in which the data is further processed shall not be incompatible with those purposes.[342] Moreover, both the GDPR and the PDPP provides data minimization principle in which the data that is collected shall be adequate, relevant and limited to the purpose of the processing.[343] In addition to that,

[337] GDPR, Art. 2/2/b and 2/2/d.
[338] PDPP, Art. 3/4/b & 3/4/d and Art. 53/2/b, 53/2/c & 53/2/d.
[339] GDPR, Art. 5/1/a and PDPP, Art. 6/1.
[340] GDPR, Art. 6/1 and PDPP, Art. 7/2.
[341] GDPR, Art. 12/1 and PDPP, Art. 12/1.
[342] GDPR, Art. 5/1/b and PDPP, Art. 6/2.
[343] GDPR, Art. 5/1/c and PDPP, Art. 6/3.

data accuracy is another principle which requires data controllers to ensure that the personal data is accurate and when necessary kept up-to-date.[344]

The other principle that both the GDPR and the PDPP recognize is the storage limitation in which a personal data shall not be stored longer than is necessary except for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.[345] Principle of security is another principle which requires that processing shall ensure the integrity, confidentiality and security of the personal data.[346] Both the GDPR and the PDPP further specify the type of threats such as unauthorized and unlawful processing, accidental loss, destruction or damage as well as the possible measures such as organizational and technical ones.[347] Accountability is another principle under the GDPR and the PDPP which requires the data controller to comply with other principles provided under the laws.[348]

More or less, the principles provided under the GDPR and the PDPP are the same in terms of their contents. The only difference between these two laws is that the PDPP recognizes the data sovereignty principle.[349] Data sovereignty is a principle that requires the storage of personal data in a server or data center located in Ethiopia.[350] The Ethiopian Communication Authority has the power to designate certain categories of personal data as critical, requiring they shall only be processed in Ethiopia based on the strategic interests of the country.[351] This principle makes the PDPP more stringent than the GDPR which lacks such kind of requirement.

Both the GDPR and the PDPP recognize a wide range of rights of data subjects. The right to be informed is the first one which requires the disclosure of the name and contact details of the data controller, the purposes of the processing, the lawful basis of the processing, the recipients of the personal data, the right to withdraw consent, etc.[352] Both the GDPR and the PDPP require that in

[344] GDPR, Art. 5/1/d and PDPP, Art. 6/4.
[345] GDPR, Art. 5/1/e and PDPP, Art. 15/2.
[346] GDPR, Art. 5/1/e and PDPP, Art. 6/6.
[347] GDPR, Art. 5/1/f and PDPP, Art. 17/1.
[348] GDPR, Art. 5/2 and PDPP, Art. 52.
[349] PDPP, Art. 22.
[350] Ibid, Art. 22/1.
[351] Ibid, Art. 22/2.
[352] GDPR, Art. 13/1 and PDPP, Art. 24/1.

case where the personal data is obtained from third party, the information regarding the categories of the personal data and the source of personal data shall be disclosed.[353]

Both the GDPR and the PDPP provide the data subjects right to get confirmation on whether their personal data is processed, if so, to access the personal data and other relevant information free of charge.[354] However, the GDPR provides that for any further copies requested, the data controller can charge a reasonable fee to cover administrative cost.[355] Unlike the GDPR, which provides exceptions that are applicable on all rights,[356] the PDPP provides exceptions that are applicable explicitly on the right to access; these are where the disclosure would unjustifiably invade another person's privacy, the data pertains to legal privilege, the personal data concerns health and medical information and disclosure could harm the data subject, etc.[357]

The right to rectify the inaccurate and complete the incomplete personal data is also recognized under both the GDPR and the PDPP.[358] However, the PDPP further provides that the right to rectification can extend to personal data that are misleading, not up-to-date or is otherwise being processed contrary to the PDPP.[359] Under the PDPP, the right to rectification entails to the data controller the obligation to notify about the correction to the third party to whom that personal data has been disclosed one year before the correction.[360]

Both the GDPR and the PDPP protect the data subject's right to erasure where the personal data are no longer necessary for the purpose of processing, the data subject withdraws his/her consent, the data subjects object the processing or the personal data has been processed unlawfully.[361] Under both the GDPR and the PDPP, The right to erasure may be restricted for reasons of public interest in the area of public health, historical, statistical or scientific research, to comply with a legal obligation and to establish, exercise or defend a legal claim.[362] However, the GDPR further

[353] GDPR, Art. 4/1/d & 14/2/f and PDPP, Art. 24/2.
[354] GDPR, Art. 15/1 and PDPP, Art. 25/1.
[355] GDPR, Art. 15/3.
[356] Ibid, Art. 23.
[357] PDPP, Art. 26/1.
[358] GDPR, Art. 16 and PDPP, Art. 27/1.
[359] PDPP, Art. 27/1.
[360] Ibid, Art. 27/2.
[361] GDPR, Art. 17/1 and PDPP, Art. 28/1.
[362] GDPR, Art. 17/3 and PDPP, Art. 28/3.

provides that exercising the freedom of expression and the right to get information is another restriction to the right to erasure of personal data.[363]

The right to restriction of processing is another one that is provided under both the GDPR and the PDPP which can be exercised where the accuracy of the personal data is contested for the period to verify the claim, the data controller is no longer needs the personal data but the data subjects need that to establish, exercise or defend legal claims, the processing is unlawful but the data subject prefers restriction over erasure of personal data, objection is made pending the verification of whether the data controller's legitimate grounds override the data subject rights.[364] Except for storing the personal data, the data controller shall fulfill certain grounds to process the personal data; these are the data subject consent, to establish, exercise or defend the legal claim, to protect the rights of others or for the reasons of public interest.[365]

The right to portability is the other which both the GDPR and the PDPP recognize to consist of the right to receive the data they provide to the data controller in a structured, commonly used and machine-readable format.[366] However, the GDPR provides two qualifications to exercise this right which are the processing is carried out based on consent or contract and the processing is conducted by automated means.[367] Both the GDPR and the PDPP enable data subjects to transmit the personal data they received to another data controller and, if technically feasible, to request the data controller to transmit the personal data to another data controller directly.[368] However, under both the GDPR and the PDPP, the right is restricted if the processing is necessary to the performance of the task carried out in the public interest or exercise of official duty or it adversely affects the rights and freedoms of others.[369]

The right to object is another one that is recognized in both the GDPR and the PDPP but have different content. Under the GDPR, the right to object is exercised in three instances; first, where processing is necessary for the performance of a task in the public interest or in the exercise of

[363] GDPR, Art. 17/3/a.
[364] GDPR, Art. 18/1 and PDPP, Art. 30/1.
[365] GDPR, Art. 18/2 and PDPP, Art. 30/2.
[366] GDPR, 20/1 and PDPP, Art. 32/1.
[367] GDPR, Art. 20/1.
[368] GDPR, Art. 20/1 & 20/2 and PDPP, Art. 32/2 & 32/3.
[369] GDPR, Art. 20/3 & 20/4 and PDPP, Art. 32/4.

official authority and processing is necessary for the purposes of the legitimate interests[370]; second, where the processing is conducted for direct marketing purposes[371] and third, where personal data are processed for scientific, historical or statistical research purposes unless the processing is necessary for reasons of public interest.[372] When it comes to the PDPP, the wording of the provision shows that it enables the right to objection in all aspects of processing and it emphasizes the right to object in case of direct marketing including profiling.[373] Furthermore, the PDPP requires the objection to be made in writing.[374]

Data subjects have a right under both the GDPR and the PDPP not to be subject to a decision based solely on automated processing including profiling.[375] Both the GDPR and the PDPP further provide that the data subjects have the right to require human intervention and to express their view.[376] The right can be restricted if it is necessary to enter and perform contract between the data subject and the data controller, authorized by a law or it is based on the data subjects explicit consent.[377] Even these restrictions exist; automated processing that intends to evaluate certain personal aspects of the data subjects shall not be based on sensitive personal data.[378]

The other right that data subjects entitled to under the GDPR and the PDPP is to withdraw their consent at any time.[379] The GDPR further provides that withdrawing of consent shall be as easy as giving consent.[380] The other right under the GDPR and the PDPP is the right to lodge a complaint to the supervisory authority if the processing of the personal data infringes the laws.[381] However, regarding the judicial remedies, the GDPR recognizes that data subjects can access judicial remedies directly independent of any complaint to supervisory authority or other

[370] GDPR, Art. 21/1.
[371] Ibid, Art. 21/2.
[372] Ibid, Art. 21/6.
[373] PDPP, Art. 29.
[374] Ibid, Art. 29/1.
[375] GDPR, Art. 22/1 and PDPP, Art. 31/1.
[376] GDPR, Art. 22/3 and PDPP, Art. 31/1
[377] Ibid, Art. 31/2
[378] Ibid, Art. 31/3.
[379] GDPR, Art. 7/3 and PDPP, Art. 8/3.
[380] GDPR, Art. 7/3.
[381] GDPR, Art. 77 and PDPP, Art. 58/1.

remedies[382], whereas; in the PDPP data subjects can access judicial remedies by submitting an appeal against the decision of the Ethiopian Communication Authority.[383]

Both the GDPR and the PDPP impose obligation on the data controller. One of the obligations under the GDPR and the PDPP is to take technical and organizational measures to ensure that processing of data is in compliance with the laws.[384] The PDPP has not specified what should be considered when such measures are taken but the GDPR provides that the nature, scope, context and purposes of processing as well as the risks for the rights and freedoms of natural persons shall be taken into account.[385] The PDPP, on the other hand, specifies these measures including implementing data security and organizational measures, keeping the record of processing, performing data protection impact assessment, obtain prior authorization or consultation with the Ethiopian Communication Authority and assigning data protection officer.[386]

Both the GDPR and the PDPP require the data controller to assign data protection officer in cases where the processing of personal data is conducted by the government institutions except the courts in their judicial capacity, where the core activities of the data controller require regular and systematic monitoring of data subjects on a large scale and where the core activities of the data controller require processing of sensitive personal data on a large scale.[387] The responsibility of a data protection officer shall be to support the data controller on data processing requirements of the laws, ensure that the laws are complied with, facilitate capacity building of staff involved in data processing operations, provide advice on data protection impact assessment; and cooperate with the supervisory authority.[388] The GDPR further provides that the data protection officer can act as a contact point for the supervisory authority.[389]

The data controller has an obligation to notify personal data breach to the supervisory authority within seventy two hours after becoming aware of it.[390] However, under the GDPR, if the personal data breach does not pose a risk to the rights and freedoms of the data subjects, the data

[382] GDPR, Art. 78.
[383] PDPP, Art. 58/3.
[384] GDPR, Art. 24/1 and PDPP, Art. 42/1.
[385] GDPR, Art. 24/1.
[386] PDPP, Art. 42/2.
[387] GDPR, Art. 37/1 and PDPP, Art. 40/1/c.
[388] GDPR, Art. 39/1 and PDPP, Art. 41/1.
[389] GDPR, Art. 39/1/e.
[390] GDPR, Art. 33/1 and PDPP, Art. 43/1.

controller is not obliged to notify the supervisory authority.[391] The data controller also has an obligation to notify the personal data breach to the data subjects without undue delay.[392] However, under the GDPR, the data controller is obliged to notify the data subject if the personal data breach can pose a high risk to the rights and freedoms of the data subjects.[393] The notification of personal data breach shall include the nature of the personal data breach, the name and contact details of the data protection officer, the likely consequences of the personal data breach, the measures taken or proposed to be taken to address the personal data breach.[394]

The data controller is obliged to maintain a record of processing activities.[395] The record shall consists of the name and contact detail of the data controller, the purpose of the processing, categories of data subjects and personal data, recipients of the personal data, transfer to other countries and the safeguards, the time limit to erase the personal data and the mechanism of the data security.[396] Under the GDPR, an organization that employs less than 250 persons is not obliged to maintain records of processing activities unless the processing is likely to pose a risk to the rights and freedoms of data subjects, the processing is not occasional, the processing includes special categories of data or personal data relating to crime.[397]

Where the processing of the personal data, taking into account their nature, scope, context and purposes; is likely to pose a risk to the rights and freedoms of data subjects, the data controller shall conduct a data protection impact assessment on the impact of the processing on the protection of personal data.[398] The impact assessment is required where the processing is systemic and extensive evaluation of personal aspects of individuals based on automated processing including profiling, processing of sensitive personal data on a large scale, systemic monitoring of publicly accessible areas on a large scale.[399] The impact assessment shall include a description of the processing and its purpose including any legitimate interest, evaluation of the

[391] GDPR, Art. 33/1.
[392] GDPR, Art. 34/1 and PDPP, Art. 44/1.
[393] GDPR, Art. 34/1.
[394] GDPR, Art. 33/2 and PDPP, Art. 43/4 and 44/2.
[395] GDPR, Art. 30/1 and PDPP, Art. 46/1.
[396] GDPR, Art. 30/1 and PDPP, Art. 46/2.
[397] GDPR, Art. 30/5.
[398] GDPR, Art. 35/1 and PDPP, Art. 47/1.
[399] GDPR, Art. 35/3 and PDPP, Art. 47/2.

necessity and proportionality of the processing, assessment of risks to data subjects‘ rights and measures and safeguards to address risks and ensure compliance.[400]

Under both the GDPR and the PDPP, where the processing of personal data is likely to pose a risk to the rights and freedoms of data subjects, the data controller shall obtain the authorization from the supervisory authority to ensure compliance with the laws and mitigate the risks.[401] This authorization shall be sought when the impact assessment indicates that the processing is likely to present a high risk for the rights and freedoms of data subjects.[402] However, under the PDPP, prior consultation can be initiated by the Ethiopian Communication Authority.[403] Moreover, under the PDPP, prior consultation is not confined to the issues of processing of personal data; it can also extend to the transfer of personal data.[404]

### 4.2. Comparison with the Data Protection Law of South Africa (POPIA)

The scope of the POPIA and the PDPP is similar. For instance, the material scope of the POPIA is similar with the PDPP in that any processing of personal data by automated means and non-automated means which forms part of filing system or is intended to form part of filing system is under the scope of both laws.[405] Moreover, unlike the GDPR, the POPIA has provided the definition of automated means which is equipment capable of operating automatically in response to instructions given for the purpose of processing information.[406]

When it comes to the territorial application of the POPIA, it closely resembles the PDPP rule in that if the data controller is established in that country, then their processing activities on personal data will be constituted under the scope of the law.[407] In the case of non-resident data controller, both the POPIA and the PDPP provide that if the processing is conducted using automated and non-automated means that situate in the country, then the activity is under the scope of the law.[408] However, the PDPP provides that non-resident data controller shall have a

[400] GDPR, Art, 35/7 and PDPP, Art. 47/3.
[401] GDPR, Art. 36/1 and PDPP, Art. 48/1.
[402] GDPR, Art. 36/1 and PDPP, Art. 48/2/a.
[403] PDPP, Art. 48/2/b.
[404] PDPP, Art. 48/1.
[405] Protection of Personal Information, Act, No. 4, South African Government Gazette, Section 3/1/a, (2013). Herein after POPIA.
[406] POPIA, Section 3/4. However, the POPIA fails to provide what non-automated means are.
[407] POPIA, Section 3/1/b/i and PDPP, Art. 3/2/a.
[408] POPIA, Section 3/1/b/ii and PDPP, Art. 3/2/b.

representative for the PDPP to be applicable.[409] Both the POPIA and the PDPP provide that personal data that transit through the country is excluded from the scope of the law.[410]

The excluded processing activities under the POPIA and the PDPP have some similarity. For instance, under both the POPIA and the PDPP, processing of personal data for personal or household activity, processing of personal data involving national security and processing of personal data in relation to judicial function are excluded from the scope of the law. However, the POPIA and the PDPP each contain distinct exceptions that limit their respective scope. In the case of the POPIA, it is provided that processing of personal data that is de-identified that cannot be re-identified, processing of personal data for the journalistic, literary and artistic purposes and processing of personal data for the prevention, detection, investigation and prosecution of crimes are excluded from the scope of the POPIA.[411]

The PDPP is also provides processing activities that are excluded from its scope; these are the processing relates to the exchange of information between government agencies where such exchange is required on a need-to-know basis; historical, statistical and scientific research; an objective of general public interest including an economic or financial interest of the country.[412] The wording of the POPIA is that it is blanket exclusion, whereas, the PDPP is discretionary exemption that shall be necessary and proportionate measure in a democratic society.[413]

The other comparison point is the principles that are recognized under the POPIA and the PDPP. The POPIA and PDPP oblige that any processing of personal data shall be lawful.[414] Furthermore, under both the POPIA and the PDPP, the personal data can be processed if the data subject gives consent, processing is necessary to perform a contract which the data subject is a party, processing complies with law, processing protects a legitimate interest of the data subject, processing is necessary for the proper performance of a public law duty or processing is

[409] PDPP, Art. 3/2/b.
[410] POPIA, Section 3/1/b/ii and PDPP, Art. 3/2/b.
[411] POPIA, Sections 6 and 7.
[412] PDPP, Art. 3/4/b & 3/4/d and Art. 53/2/b, 53/2/c & 53/2/d.
[413] POPIA, Section 6 and PDPP, Art. 53/1.
[414] POPIA, Section 9 and PDPP, Art. 7.

necessary for protect the legitimate interests of the data subject.[415] However, the POPIA does not explicitly recognize the fairness and transparency principle.[416]

The principle of data minimization is the same under both the POPIA and the PDPP in that the personal data is adequate, relevant and not excessive in light of the purpose of the processing.[417] Under both the POPIA and the PDPP, any collection and processing of personal data shall be for specified, explicit and lawful purpose.[418] Both the POPIA and the PDPP also specifies that personal data must not be retained any longer than is necessary for achieving the purpose for which the data was collected or processed.[419] However, the personal data may be retained if it is authorized by law, the data subject consents or it is necessary for lawful purposes.[420] The PDPP further provides additional ground for the retention of the personal data which is for historical, statistical, literally and research purposes.[421]

Under both the POPIA and the PDPP, the requirement that the personal data shall be complete, accurate, not misleading and up-to-date is recognized as a principle.[422] The PDPP relives the data controller from its obligation to maintain accurate personal data if the data controller takes reasonable steps to ensure the accuracy or the personal data indicates the inaccuracy.[423] Principle of security is the other one which both the POPIA and the PDPP state that the data controller shall take reasonable technical and organizational act to stop personal data from being lost or damaged and unlawful access to personal data.[424] Unlike the PDPP, and the same as the GDPR, the POPIA does not recognize the data sovereignty principle.[425]

Both the POPIA and the PDPP provide various rights of data subjects. The first one is the right to be informed of the collection and processing of personal data.[426] This right enables the data subjects to be aware of any activity that pertain to their personal data by providing relevant

[415] POPIA, Section 11 and PDPP, Art. 7/2 and 8/1.
[416] POPIA, Sections 8-25.
[417] POPIA, Section 10 and PDPP, Art. 6/3.
[418] POPIA, Section 13/1 and PDPP, Art. 6/2.
[419] POPIA, Section 14/1 and PDPP, Art. 15/1.
[420] POPIA, Section 14/1 and PDPP, Art. 15/2.
[421] PDPP, Art. 15/2/d.
[422] POPIA, Section 16/1 and PDPP, Art. 14.
[423] PDPP, Art. 14.
[424] POPIA, Section 19/1 and PDPP, Art. 17/1.
[425] PDPP, Art. 22.
[426] POPIA, Section 18/1 and PDPP, Art. 24/1.

information on the data controller and its activities.[427] The POPIA provides the grounds of non-compliance; these are where the data subject consents, non-compliance would not affect the data subject‘s legitimate interests, compliance would prejudice the lawful purpose of the collection, compliance is not practicable, the personal data will not be used in a way in which the data subject may be identified or it will be used for historical, statistical or research purposes.[428]

The other one is the right to access in which the data subject under both the POPIA and the PDPP can request the data controller to confirm the collection and processing of personal data and require accessing any information related to that personal data within reasonable time free of any charge.[429] Unlike the POPIA, the PDPP provides exceptions to the right to access personal data; these are if the disclosure would unjustifiably invade another person‘s privacy, the data pertains to legal privilege, the personal data concerns health and medical information and disclosure could harm the data subject, etc.[430]

The POPIA, unlike the PDPP[431], treats the right to rectification and erasure as one right in that the data controller shall correct or delete personal data that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully.[432] Personal data can also be deleted or destroyed if the data controller can no longer retain it.[433] Both the POPIA and the PDPP bestow the power on the data subject have the right to oppose the processing of personal data.[434] Unlike the PDPP, which provides unrestricted right to object, the right under the POPIA has limited scope in that it should applies only when the processing is based on protecting the legitimate interests of the data subject, performing a public law duty, or pursuing the legitimate interests of the data controller or a third party, as well as for purposes of direct marketing.[435] Both the POPIA and the PDPP enables the data subject to revoke his/her consent, if the processing of personal data is conducted based on the latter consent.[436]

[427] Ibid.
[428] POPIA, Section 18/4.
[429] POPIA, Section 23/1 and PDPP, Art. 25/1.
[430] PDPP, Art. 26/1.
[431] PDPP, Art. 27 and 28.
[432] POPIA, Section 24/1/a.
[433] Ibid, Section 24/1/b.
[434] POPIA, Section 11/3 and PDPP, Art. 29/1.
[435] POPIA, Section 11/3/a.
[436] POPIA, Section 11/2 and PDPP, Art. 8/1.

Both the POPIA and the PDPP state that the data subject has a right not to be subject to automated decision making including profiling that result in legal consequences or substantially affects him/her.[437] The POPIA further elaborate about the intended purpose of profiling including to provide information on the data subjects performance at work, credit worthiness, reliability, location, health, personal preferences or conduct.[438] Both the POPIA and the PDPP recognize that the data subject has a right to submit a complaint to the supervisory body in writing[439] and in case of dissatisfaction he/she can appeal to the court.[440]

Unlike the POPIA, the PDPP recognizes the data subject‘s right to request restriction of processing of personal data which enables data subjects to temporarily stop any processing activity while the legitimacy or accuracy of the data is verified, the data is needed for legal claims, the processing is contested as unlawful or an objection is pending.[441] Moreover, the PDPP recognizes the right to portability which enables the data subjects to receive and transfer their personal data to other data controller or where technically feasible, to request direct handover of their personal data from one data controller to the other.[442]

The POPIA and the PDPP also impose comparable obligations on data controllers. The first one is that under both the POPIA and the PDPP, the data controller has an obligation to assign a data protection officer.[443] However, unlike the PDPP which requires a designation of data protection officer in limited circumstances[444], under the POPIA all public and private body is required to assign data protection officer.[445] The role of data protection officer under the POPIA and the PDPP is similar in that providing support to the data controller, ensuring compliance with the law and working with the supervisory authority to ensure protection of personal data.[446]

Both the POPIA and the PDPP prescribe the obligation to conduct an assessment.[447] Unlike the PDPP, which can be conducted by the data controller[448], the POPIA provides that it can be

[437] POPIA, Section 71/1 and PDPP, Art. 31/1.
[438] POPIA, Section 71/1.
[439] POPIA, Section 74/1 and PDPP, Art. 58/1.
[440] POPIA, Section 97/1 and PDPP, Art. 58/3.
[441] PDPP, Art. 30.
[442] Ibid, Art. 32.
[443] POPIA, Section 56 and PDPP, Art. 40.
[444] PDPP, Art. 40/1.
[445] POPIA, Section 56.
[446] POPIA, Section 55 and PDPP, Art. 41/1.
[447] POPIA, Section 89 and PDPP, Art. 47.

conducted by the supervisory authority.[449] The other obligation under both the POPIA and the PDPP is the requirement to secure prior authorization from the supervisory authority in limited cases where ensuring the compliance with the law and protecting the personal data is essential.[450] Under the PDPP, prior authorization may be sought if the data protection impact assessment shows a high risk to the data subject's privacy rights or the Ethiopian Communication Authority requires it.[451] Under the POPIA, prior consultation may initiated if the processing concerns with unique identifiers such as for a purpose other than the one intended at collection, processing on criminal behavior or processing information for the purposes of credit reporting, etc.[452]

Both the POPIA and the PDPP require the data controller to maintain a record of processing of personal data.[453] However, the POPIA make reference to the Promotion of Access to Information Act without providing the detailed rules.[454] Whereas, the PDPP prescribes what should be included in the record including the name and contact detail of the data controller, the purpose of processing, the categories of data subjects and personal data, etc.[455] Both the POPIA and the PDPP require the data controller to notify both the regulatory authority and the data subject if personal data breach occurred.[456] The POPIA require the notification to be made in a reasonable time[457], while PDPP require the notification to be made in 72 hours.[458]

### 4.3. Strengths and Weaknesses of Ethiopia's Law in a Global Context

The PDPP exhibits both strengths and weaknesses in the protection of personal data. One of its strengths is that it is comprehensive in which all rights, obligations and responsibilities of actors of personal data protection[459] is clearly defined. Moreover, the PDPP provides that personal data shall be processed for limited grounds and the main one is the data subject's consent.[460] The PDPP, similar to the GDPR, provide substantive and procedural requirements for consent in

[448] PDPP, Art. 47.
[449] POPIA, Section 89/1.
[450] POPIA, Section 57 and PDPP, Art. 48.
[451] PDPP, Art. 48/2.
[452] POPIA, Section 57/1.
[453] POPIA, Section 17 and PDPP, Art. 46.
[454] POPIA, Section 17.
[455] PDPP, Art. 46/2.
[456] POPIA, Section 22 and PDPP, Art. 43.
[457] POPIA, Section 22/2.
[458] PDPP, Art. 43/1.
[459] The actors are data subjects, data controller and/or data processor and supervisory authority.
[460] PDPP, Art. 8.

which it must be freely given, specific, informed and unambiguous. Hence, data controllers cannot process the personal data simply because the data subject does not object rather they are required to secure his/her consent to processing of his/her personal data.[461]

The PDPP also has additional strengths such as that it is aligned with international best practices.[462] The PDPP incorporates various rights of data subjects that are recognized under other laws for protecting the data subjects personal data including the right to be informed of processing, the right to access, the right to rectify, the right to erasure, the right to object, the right to restriction of processing, the right not to be subject to automated decision making, the right to portability, the right to withdraw consent and the right to lodge a complaint.[463]

The PDPP not only grant rights to data subjects but also imposed comparable obligations on the data controllers including the requirement to assign data protection officer, perform data protection impact assessment, maintain the record of processing activities, notify the personal data breach, prior authorization and other security measures.[464] These obligations align with the rules under the GDPR in that data controllers are the primary party that are responsible for upholding the data protection principles.[465]

The PDPP also prescribes a proactive regulatory mechanism in that the data controller is required to seek prior authorization from the Ethiopian Communication Authority if the data protection impact assessment indicates a high risk to the rights and freedoms of data subjects.[466] It further provides that even if the data protection impact assessment does not show a high risk, the Ethiopian Communication Authority with its own initiative taking the nature, scope and purpose of processing operations, can require prior consultation with the data controller.[467]

The other strength of the PDPP is the explicit recognition of sensitive data such as data subject‘s racial or ethnic origin, genetic or biometric data, physical or mental health and provides more

[461] Chris Jay Hoofnagle et al., *The European Union General Data Protection Regulation: What It Is and What It Means*, P. 79, (2019).
[462] See the previous section about the GDPR and the POPIA.
[463] PDPP, Art. 8/3, Art. 24-32 and Art. 58.
[464] Ibid, Arts. 40-48.
[465] Bart Van Der Sloot & Frederik Zuiderveen Borgesius, *The EU General Data Protection Regulation: A New Global Standard for Information Privacy*, P. 27, (2020).
[466] PDPP, Art. 48/2/a
[467] Ibid, Art. 48/2/b.

stringent rules for its protection.[468] The stringency is apparent in the rule that prohibits the processing of sensitive personal data except for a few grounds.[469] Compared to the GDPR and the POPIA, the PDPP recognize the data localization principle which mandates that the personal data shall be stored in Ethiopia.[470] This rule requires the approval of the Ethiopian Communication Authority to transfer sensitive personal data across the border which provides a strong regulatory framework for data protection.[471]

The PDPP also has its weaknesses. One of the weaknesses is that even though the data localization principle is enables to strictly regulate cross-border transfer of personal data, it also poses challenges in free flow of personal data. The world economy is increasingly driven by data and the free flow of personal data enables innovation around the world.[472] Moreover, data localization impedes businesses from operating globally and since they cannot state-of-the-art facilities and curtailed from the other world, they are exposed to cyber security and fraud.[473] Data localization also has an economic impact in that to comply with the rule, the data controller has to bear the cost relating to hiring locally and building infrastructure, efficiency losses due to disruptions and limiting access to the best talent and increased compliance expenses due to unclear and unpredictable regulatory requirements.[474]

The other problem of the PDPP is the procedural and formal requirement that reduce the usability of rights. For instance, to exercise the right to object the data subject has to submit its objection to the data controller in writing.[475] This requirement is unique to the PDPP since neither the GDPR nor the POPIA impose such a requirement.[476] The other weakness of the PDPP is the vague exemptions that are bestowed on certain processing activities. For instance, in cases of national security, defence, public security, general public interest and other grounds; the

[468] Ibid, Art. 2/5
[469] Ibid, Art. 9.
[470] Ibid, Art. 22.
[471] Ibid, Art. 22/3
[472] Institute of International Finance, Data Localization: Costs, Tradeoffs, and Impacts across the Economy, P. 1, (2020).
[473] Chiara Del Giovane et. al., The Nature, Evolution and Potential Implications of Data Localization Measures, OECD Trade Policy Paper, P. 27, (2023).
[474] Dan Jerker B. Svantesson, Data Localization Trends and Challenges; Considerations for the Review of the Privacy Guidelines OECD Digital Economy Papers, P. 20, (2020).
[475] PDPP, Art. 29/1.
[476] GDPR, Art. 21 and POPIA, Section 11/3.

application of the PDPP may be restricted.[477] The PDPP does not define these grounds and any data controller can interpret its activities to be exempted from the PDPP without an oversight.[478] Even the Ethiopian Communication Authority cannot verify this interpretation; it can only institute a case to court if it's convinced that it is not necessary and proportionate.[479]

Most data protection laws establish a national data protection authority which is an independent administrative body entrusted with implementing the law.[480] The national data protection authority shall be independent from executive branch of the government since it regulates both the public and private sector.[481] The draft PDPP reflects this approach[482] but when the PDPP adopted the power is rather bestowed on the Ethiopian Communication Authority.[483] This policy choice garnered controversy due to the skepticism towards near-total control of personal data regulation and impartiality of the Ethiopian Communication Authority.[484]

The other weakness is the complaint mechanism. Under the PDPP, the data subject whose privacy right has been violated can access the court only after submitting his/her complaint to the Ethiopian Communication Authority.[485] The court can entertain the case in appellate jurisdiction which confined it to review the decision of the Ethiopian Communication Authority not the facts of the case.[486] This rule is contrary to the GDPR which recognizes the data subject's right to access court without being required to submit complaint to the supervisory authority.[487] The cost of complying with the PDPP is another weakness. The PDPP require data controllers to assign data protection officer, implement technical and organizational measures, maintain records of processing activities and perform data protection impact assessment that can incur substantial costs especially for data controllers that have limited capacity.[488]

---

[477] PDPP, Art. 53/2.
[478] PDPP, Art. 53.
[479] PDPP, Art. 53/3.
[480] Kinfe Yilma, Follies of Ethiopia's Data Protection Legislation, Global Privacy Law Review, Vol. 6, No. 2 P. 1-2, (2025),
[481] Ibid, P. 2.
[482] Ibid.
[483] PDPP, Art. 5.
[484] Ashenafi Endale, Critics Fear Comms Authority Personal Data Dominion, Impartiality in Legislative Wrangle, The Reporter (2024), https://www.thereporterethiopia.com/38279/, (accessed 12 August 2025).
[485] PDPP, Art. 53.
[486] Ibid, Art. 53/3.
[487] GDPR, Art. 78.
[488] PDPP, Art. 40, Art. 42, Art. 46 and Art. 47.

### 4.4. Challenges in Implementation and Compliance

The data protection regime is challenged by various issues that come with the digital era. One of the challenges is the advancement of technology and its implication on personal data protection. The technologies that pose challenges to the data protection include big data analytics and artificial intelligence (AI).[489] AI shows a capacity to process a vast dataset which enables it to analyze data that is not possible before.[490] Especially, AI's ability to infer, aggregate and reclassify non-personal data and derive identifiable personal data from that raises concerns regarding the data subject's privacy rights.[491]

Another challenge that data protection regimes face is the issue of cross-border transfer. Some countries such as the United States allow data transfer without restriction and other countries restrict cross-border data transfer.[492] The countries that restrict cross-border data transfer falls into two categories; the first one is a one-off exception which permits cross-border transfer for grounds that are specified prior to the transfer; the second one is ongoing exceptions which assess whether the destination country provide sufficient data protection mechanisms.[493] During cross-border transfer of personal data various challenges may occur.[494] The challenges include the jurisdictional conflict due to the existence of various laws; technical problems due to data loss, programming error, hacking; security risks; obtaining permit from the supervisory authority in time, regulatory complexities especially for non-lawyers.[495]

The other issue is balancing between the data subject's data protection rights and other public interests including national security. Some laws exclude the processing of personal data in relation to national security from their scope.[496] This exclusion, albeit essential to the public

[489] John Babikian, Securing Rights: Legal Frameworks for Privacy and Data Protection in the Digital Era, Law Research Journal, P. 94, (2023).
[490] Immaculeta Chidera Onyekwe, AI and Data Privacy in the Internet of Things (IoT): A New Frontier in the Connected World, IJDPP, Nigeria Data Protection Commission, P. 27, (2025).

[491] Ibid, P. 27.
[492] United Nations Conference on Trade and Development, Data Protection Regulations and International Data Flows: Implications for Trade and Development, United Nations, P. 12-13, (2016).
[493] Ibid, P. 13.
[494] Damilola M. Adeniyi and Oluwakamiye T. Olorunfemi, Cross-Border Data Transfers: Compliance Challenges and Best Practices for Prevention of Data Breaches, IDDPP, National Data Protection Commission, P. 148, (2025).
[495] Ibid, P. 148-150.
[496] GDPR, Art. 2/a, POPIA, Section 6/1/c and PDPP, Art. 53/2.

interest, can be detrimental to the data subject's privacy rights.[497] In this regard, one of the issues is surveillance which many laws failed to explicitly address.[498] The rise of cloud services enables countries to conduct surveillance in their citizens as well as foreigners.[499] The Edward Snowden revelation of surveillance activities in the United States caused improved governance, restrictions on mass surveillance of US citizens and extension of some rights to foreigners.[500]

The other challenge is the difficulty to enforce.[501] In the case of public bodies; due to their mandate they retain a sensitive data which enables them to misuse it, it is difficult to penalize them, they violate the rules by enacting laws, etc.[502] For instance, the Kenya Communication Authority once ordered telecom service providers to install Data Management System that can be used to detect fake mobiles.[503] However, this rule is later reversed by the court.[504] In the private sector, when the business grows and interacts with the global community, it will be subject to extraterritoriality requirement.[505] Hence, the business is required to comply with the domestic data protection law and the GDPR to continue its business operations in Europe.[506]

The data protection laws are burdensome in terms of cost to businesses.[507] One of the burdens is the requirement to register which requires navigating regulatory complexity and obligation to pay certain fee for the supervisory authority.[508] Moreover, the data controller is required to appoint data protection officer, conduct data protection impact assessment and maintain records of processing activities.[509] In addition to that, due to data localization rules, data controllers are required to establish data centers in local jurisdictions.[510] Data protection laws can impose

[497] The government institutions can abuse their discretion at the expense of the data subjects.
[498] United Nations Conference on Trade and Development, Data Protection Regulations and International Data Flows: Implications for Trade and Development, P. 15, (2016).
[499] Ibid.
[500] Ibid.
[501] Justin Bryant, Africa in the Information Age: Challenges, Opportunities, and Strategies for Data Protection and Digital Rights, Stan. Tech. L. Rev., Vol. 24, P. 403, (2021).
[502] Ibid, P. 403-406
[503] Ibid, P. 404.
[504] Ibid.
[505] GDPR, Art. 3/2.
[506] Justin Bryant, Africa in the Information Age: Challenges, Opportunities, and Strategies for Data Protection and Digital Rights, P. 403, (2021).
[507] United Nations Conference on Trade and Development, Data Protection Regulations and International Data Flows: Implications for Trade and Development, P. 15, (2016).
[508] PDPP, Art. 5/3.
[509] PDPP, Art. 40-48.
[510] United Nations Conference on Trade and Development, Data Protection Regulations and International Data Flows: Implications for Trade and Development, P. 15, (2016).

substantial costs which can be absorbed by large companies but can pose substantial challenges to small businesses that have limited resources.[511]

[511] Justin Bryant, Africa in the Information Age: Challenges, Opportunities, and Strategies for Data Protection and Digital Rights, P. 408, (2021).

# Chapter Five

# 5. Conclusion and Recommendations

## 5.1 Conclusion

The study aim was to evaluate whether Ethiopia's Personal Data Protection Proclamation (PDPP) sufficiently protects the right to digital privacy in accordance with international data protection standards, specifically referencing the Protection of Personal Information Act (POPIA) of South Africa and the General Data Protection Regulation (GDPR) of the European Union. Additionally, it assesses for institutional and legal gaps, evaluated enforcement strategies, and assessed remedies for personal data breaches.

The PDPP represents a major normative advancement in Ethiopia's data protection law system, according to the report. In line with globally acknowledged best practices, it integrates fundamental concepts such as lawfulness, fairness, openness, purpose limitation, data minimization, accuracy, storage limitation, integrity, confidentiality, and accountability. Additionally, it gives data subjects a wide range of rights, including the right to access, rectification, deletion, restriction of processing, portability, objection, and protection against automated decision-making. These rights are in line with many of the GDPR's provisions included in articles 5, 12, and 23.

These legislative safeguards address Ethiopia's rapid digital transition, which is marked by a rise in internet usage, the growth of e-commerce, and a dependence on digital identity systems. They signify a significant recognition of Ethiopia's responsibilities under Article 26 of the FDRE Constitution and Article 17 of the International Covenant on Civil and Political Rights (ICCPR). However, a number of significant and systemic flaws compromise the PDPP's efficacy. First, a number of crucial terms are not clearly defined, which increases the possibility of inconsistent interpretation and compromises predictability. These phrases include legitimate interest, public interest, and suitable safeguards for cross-border data transfers. Second, the Ethiopian Communication Authority's dual role as a supervisor of data protection and a regulator of telecommunications limits its enforcement capacity, raising questions about its independence, impartiality, and possible political interference. Third, the PDPP's ability to provide effective cross-border protection is weakened by the absence of strong contractual safeguards and explicit

adequacy assessment standards, even though it governs breach notifications and foreign data transfers.

When compared to the GDPR, the PDPP has a smaller extraterritorial reach, offers less effective control of state surveillance, and levies smaller administrative penalties. Established under Article 52 of the GDPR, the supervisory authorities have broad investigation and corrective powers, as well as more powerful deterrent penalties under Article 83. They are also institutionally independent.

Furthermore, the regulatory issues raised by advanced technologies like algorithmic profiling, biometric identification, and big data analytics, and artificial intelligence (AI) have not yet been covered by the PDPP. Ethiopian residents are at risk of prejudice, discrimination, and opaque decision-making processes due to the lack of clear safeguards in these areas, particularly as the use of AI in the public sector, law enforcement, and business sectors grows. Generally, Strengthening Ethiopia's capacity to safeguard individual liberty, dignity, and trust in the digital economy requires proactive technology adaption, institutional reform, and legislative improvement.

## 5.2 Recommendations

1. Enhance Institutional Independence: Establish a fully autonomous Data Protection Authority (DPA), separate from the Ethiopian Communication Authority, to ensure impartial enforcement, free from potential conflicts of interest, consistent with the supervisory authority model under art 51 GDPR.
2. Clarify Key Legal Definitions and Standards: Amend the PDPP to provide precise definitions for legitimate interest, public interest, and adequate safeguards in cross-border transfers. Issue interpretative guidelines modeled on the European Data Protection Board‘s recommendations to harmonies implementation.
3. Strengthen Enforcement Powers and Sanctions: Align penalty provisions with the deterrent standards of art 83 GDPR, enabling fines up to a proportion of global annual turnover for serious infringements. Expand the Ethiopian supervisory authority‘s investigative powers to include mandatory compliance audits, routine inspections, and whistleblower protections.
4. Integrate Emerging Technology Safeguards: Introduce explicit provisions governing AI, biometric data, and algorithmic decision-making, ensuring transparency, human oversight,

and accountability. Mandate Data Protection Impact Assessments (DPIAs) for high-risk processing, following art 35 GDPR standards.

5. Refine Cross-Border Data Transfer Mechanisms: Develop a formal adequacy assessment framework, in line with arts 45–46 GDPR, to evaluate whether third countries offer equivalent protection. Require binding corporate rules or standard contractual clauses for transfers to non-adequate jurisdictions.
6. Expand Public Awareness and Capacity-Building: Launch nationwide awareness campaigns targeting individuals, businesses, and government institutions to promote understanding of data subject rights and compliance obligations. Provide structured training for data protection officers, legal practitioners, and judicial authorities on PDPP enforcement.
7. Align with Regional and International Standards: Ratify and implement the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention) to enhance regional cooperation and policy harmonization. Establish a regular review mechanism to update the PDPP in response to technological developments and evolving global privacy norms.

# Bibliography


**Laws and Proclamation**

1. African Union, African Union Convention on Cyber Security and Personal Data Protection adopted 27 June 2014
2. Regulation (EU) 2016/679 (General Data Protection Regulation) [2016]
3. International Development Association Loan Agreement for Financing Second Ethiopia Resilient Landscapes and Livelihoods Project Ratification Proclamation No. 1285/2023
4. The federal democratic republic of Ethiopia constitution 1995
5. Personal data protection Proclamation No.1321/2024

**Books**

1. DLA Piper, Data Protection Laws of the World: Full Handbook, (2023).
2. European Public Service Union (EPSU), The General Data Protection Regulation (GDPR): An EPSU Briefing, (2019).
3. European Union Agency for Network and Information Security (ENISA), Privacy by Design in Big Data: An Overview of Privacy Enhancing Technologies in the Era of Big Data Analytics, (2015).
4. Ian Walden, Privacy and Data Protection in Chris Reed Edited Computer Law, Oxford University Press, (7th Ed. 2011).
5. Lee A. Bygrave, Data Protection Law: Approaching Its Rationale, Logic and Limits, Kluwer International Law, Information Law Series-10, (2002).

**Articles**

1. Anvesha Singh, Cross-Border Data Transfers: Legal Challenges and Solutions in the Globalized Digital Economy, IJIRL, Vol. 4 No. 1, P. 357, (2024).
2. Bart Van Der Sloot & Frederik Zuiderveen Borgesius, The EU General Data Protection Regulation: A New Global Standard for Information Privacy, Eur. Data Prot. L. Rev. Vol. 6 No. 1, (2020).
3. Berhan Taye & Roman Teshome, Privacy and Personal Data Protection in Ethiopia, CIPESA, (2018).

4. Damilola M. Adeniyi and Oluwakamiye T. Olorunfemi, Cross-Border Data Transfers: Compliance Challenges and Best Practices for Prevention of Data Breaches, IDDPP, National Data Protection Commission, (2025).
5. Graham Greenleaf, The New Data Protection Convention 108+ and its Importance for Asia, Presented at the Asian Privacy Scholars Network (APSN) Conference, (2024).
6. Immaculeta Chidera Onyekwe, AI and Data Privacy in the Internet of Things (IoT): A New Frontier in the Connected World, IJDPP, Nigeria Data Protection Commission, (2025).
7. John Babikian, Securing Rights: Legal Frameworks for Privacy and Data Protection in the Digital Era, Law Research Journal, Vol. 1 No. 2, (2023).
8. Juliane Kokott and Christoph Sobotta, The Distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR, IDPL, Vol. 3 No. 4, (2013).
9. Justin Bryant, Africa in the Information Age: Challenges, Opportunities, and Strategies for Data Protection and Digital Rights, Stan. Tech. L. Rev., Vol. 24, (2021).
10. Kinfe Micheal Yilma & Alebachew Birhanu, Safeguards of the Right to Privacy in Ethiopia: A Critique of Laws and Practices, JEL, Vol. 26, No. 1, P. 116-117, (2013).
11. Kinfe Yilma, Follies of Ethiopia‘s Data Protection Legislation, Global Privacy Law Review, Vol. 6, No. 2 P. 1-2, (2025).
12. Nadezhda Purtova, The Law of Everything: Broad Concept of Personal Data and the Future of EU Data Protection Law, Law, Innovation & Tech, Vol. 10 No. 1, (2018).
13. Nisha Tusharkumar Gajjar, Data Privacy and Protection in the Digital Age: Emerging Trends and Technologies, IJEASM, Vol. 5 No. 4, P. 2, (2024).
14. Oskar J. Gstrein and Anne Beaulieu, How to Protect Privacy in a Datafied Society? A Presentation of Multiple Legal and Conceptual Approaches, Philosophy and Technology, Vol. 35 No. 3, (2022).
15. Peter Erik Blume, Data Protection and Privacy: Basic Concepts in a Changing World, in Scandinavian Studies in Law, ICT Legal Issues, Vol. 56, (2010).
16. Peter Hustinx, EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation, SCRIPTed, Vol. 9 No. 1, (2012).
17. Ryan Calo, Artificial Intelligence Policy: A Primer and Roadmap, U.C.D L. Rev., Vol. 51 No. 2, (2018).

18. Valentin Rupp and Max Von Grafenstein, Clarifying ―Personal Data‖ and the Role of Anonymization in Data Protection Law: Including and Excluding Data from the Scope of the GDPR (More Clearly) Through Refining the Concept of Data Protection, Computer and Security Review, Vol. 52, (2024).
19. Waseem Zafer and Floris Huider, OECD Guidelines and International Law: Navigating Data Protection and Privacy Regulations, (2008).

**Policy Reports**

1. Chiara Del Giovane et. al., The Nature, Evolution and Potential Implications of Data Localization Measures, OECD Trade Policy Paper, (2023).
2. Dan Jerker B. Svantesson, Data Localization Trends and Challenges; Considerations for the Review of the Privacy Guidelines OECD Digital Economy Papers, P. 20, (2020).
3. European Data Protection Supervisor, Accountability on the Ground Part II: Data Protection Impact Assessments & Prior Consultation, (2019).
4. Institute of International Finance, Data Localization: Costs, Tradeoffs, and Impacts across the Economy, (2020).
5. OECD Going Digital Toolkit, Trade and Cross-Border Data Flows, (2021).
6. United Nations Conference on Trade and Development, Data Protection Regulations and International Data Flows: Implications for Trade and Development, United Nations, P. 12-13, (2016).

**Thesis**

1. Samuel Worku, The Right to Privacy in the Age of Surveillance: Personal Data Protection in Ethiopia, Master‘s Thesis, Addis Ababa University School of Law, P. 43, (2024).

**Newspaper Article**

1. Ashenafi Endale, Critics Fear Comms Authority Personal Data Dominion, Impartiality in Legislative Wrangle, The Reporter (2024), https://www.thereporterethiopia.com/38279/, (accessed 12 August 2025).