ADDIS ABABA UNIVERSITY

COLLEGE OF NATURAL AND COMPUTATIONAL SCIENCES

SCHOOL OF INFORMATION SCIENCE

DESIGNING A COMPREHENSIVE FRAMEWORK FOR PERSONAL DATA PROTECTION IN ETHIOPIAN COMMERCIAL BANKS IN ALIGNMENT WITH EU GDPR

By: Maereg Seyoum (GSE/4726/14)

Advisor: Dereje Teferi (Ph.D.)

December, 2024

Addis Ababa, Ethiopia

ADDIS ABABA UNIVERSITY

COLLEGE OF NATURAL AND COMPUTATIONAL SCIENCES

SCHOOL OF INFORMATION SCIENCE

DESIGNING A COMPREHENSIVE FRAMEWORK FOR PERSONAL DATA PROTECTION IN ETHIOPIAN COMMERCIAL BANKS IN ALIGNMENT WITH EU GDPR

A Thesis Submitted to School of Information Science of Addis Ababa University in Partial Fulfilment of the Requirements for the Degree of Master of Science in Information Systems

By: Maereg Seyoum

Advisor: Dereje Teferi (Ph.D.)

December, 2024

Addis Ababa, Ethiopia

ADDIS ABABA UNIVERSITY

COLLEGE OF NATURAL AND COMPUTATIONAL SCIENCES

SCHOOL OF INFORMATION SCIENCE

DESIGNING A COMPREHENSIVE FRAMEWORK FOR PERSONAL DATA PROTECTION IN ETHIOPIAN COMMERCIAL BANKS ALIGNMENT WITH EU GDPR

By: Maereg Seyoum

Name and Signature of Members of the Examining Board

Dereje Teferi (Ph.D.)	_____	_____
Advisor	Signature	Date
Ermias Abebe (Ph.D.)	_____	_____
Examiner	Signature	Date
Getachew Hailemariam (Ph.D.)	_____	_____
Examiner	Signature	Date

Declaration

This thesis has not been previously submitted for any degree and is not being concurrently submitted for any degree at any university. I hereby declare that the thesis is the result of my independent investigation, except where otherwise indicated. The research was conducted with the guidance and support of my research advisor, and all external sources have been appropriately acknowledged through explicit citations and references. A comprehensive list of references is appended to this thesis.

Signature: _____

Maereg Seyoum

This thesis has been submitted for examination with my approval as a university advisor.

Advisor's Signature: _____

Dereje Teferi (Ph.D.)

Acknowledgments

First and foremost, I wish to express my heartfelt gratitude and praise to Almighty God for His boundless blessings, wisdom, strength, guidance, and unwavering support, which granted me the opportunity and courage to successfully complete this research work.

I would like to express my deepest and most sincere gratitude to my research advisor, **Dr. Dereje Teferi,** for his invaluable guidance, support, and encouragement throughout this research journey. His expertise and mentorship have been instrumental in helping me understand the methodologies required to conduct rigorous research and present my findings with clarity and precision.

In addition to my advisor, I would like to extend my heartfelt gratitude to **Dr. Lemma Lessa** for generously sharing his extensive knowledge and experience during his class sessions. His unreserved commitment to teaching and mentorship has been a source of inspiration and has greatly enriched my understanding of the subject matter.

I extend my deepest gratitude **to Ato Tagel Mekonnen**, Director of Data Analytics and Database (and former Director of the Cyber Security Department) at Dashen Bank, and **Ato Eskatnaf Wolde**, Director of Cyber Security at Zemen Bank, for their unwavering support and invaluable contributions to this research. I also sincerely thank the staff, management, and employees of Commercial Bank of Ethiopia, Dashen Bank, Awash Bank, Zemen Bank, Wegagen Bank, and Hijira Bank for their active participation in responding to questionnaires, engaging in interviews, and contributing to the framework demonstration and expert validation sessions. This thesis would not have been possible without your generous insights, valuable inputs, and steadfast support, for which I am profoundly grateful.

No words can truly capture my gratitude to my beloved spouse**, Rozina Ali**, for her boundless love, unwavering support, countless sacrifices, and constant inspiration throughout my life. Her encouragement has been my greatest strength. I also extend my deepest thanks to my family and friends, whose encouragement and support motivated me to pursue and complete my master's degree.

Finally, I am profoundly grateful to my colleagues, classmates, and friends who have contributed to the completion of my research work. Their assistance, camaraderie, and encouragement have been invaluable throughout this journey.

Abstract

Data protection is a vital issue for commercial banks, especially since they manage large volumes of sensitive customer data. This research investigates the data protection practices of Ethiopian commercial banks, assesses their compliance with international standards like the EU General Data Protection Regulation (GDPR), and highlights deficiencies in their current methods. Utilizing a mixed-methods research approach, data was gathered through surveys, interviews, and validation sessions with stakeholders, including bank staff, management, and regulators.

The results indicate considerable shortcomings in data governance, compliance protocols, and risk management strategies, emphasizing the necessity for a customized framework to tackle these issues. Consequently, this study introduces a comprehensive Personal Data Protection Framework aimed at improving data governance, legal adherence, risk management, data minimization, and security protocols. This framework aligns with GDPR principles while being flexible enough to fit the specific regulatory and operational environment of Ethiopian commercial banks.

By adopting this framework, banks can enhance their data protection practices, build customer trust, and ensure compliance with international standards. The findings of this study go beyond academic contributions, providing actionable insights for banks, regulators, and policymakers to bolster data protection within the banking industry. The research concludes with suggestions for future research, including cross-industry analyses such as telecom and medicals institutions, the incorporation of emerging technologies; AI and ML, and long-term evaluations of the framework's effectiveness.

Key words: Personal Data, Data Protection, GDPR Compliance, Ethiopian Commercial Banks, GDPR Privacy Framework, Regulatory Compliance, Data Protection Framework, Emerging Technologies in Data Protection

Table of Contents

List of Tables

List of Figures

Acronyms

AES	Advanced Encryption Standard
DC	Data Center
DK	Design Knowledge
DLP	Data Loss Prevention
DPAs	Data protection authorities
DPO	Data Protection Officer
DSO	Data Security Officer
DS	Design Science
DSR	Design Science Research
EDMS	Electronic Document Management Systems
EU	European Union
EU GPPR	European Union General Data Protection Regulation
GDPR	General Data Protection Regulation
INSA	Information Network Security Administration
IoT	Internet of Things
IPS	Intrusion Prevention Systems
IRT	Incident Response Team
ISF	Information Security Framework
KYC	Know Your Customer
MFA	Multi-factor authentication
NDA	Non-disclosure agreement
NIST	National Institute of Standards and Technology
PII	Personally Identifiable Information
RBAC	Role-Based Access Controls
SDLC	Secure Software Development Life Cycles
SIEM	Security Information and Event Management
SPSS	Statistical Package for the Social Sciences
USB	Universal Serial Bus

Chapter One

Introduction

1.1 Background and Context

In today's digital age, personal data has emerged as a highly valuable asset, necessitating robust protection measures(Anant et al., 2020). Across industries, the banking sector stands as a custodian of vast amounts of sensitive information, entrusted with safeguarding the financial well-being and personal data of millions of customers. In this era, where data breaches and cyber threats loom large, the need for robust personal data protection mechanisms is more critical than ever witnessed a rapid transformation in its financial sector (Tayyba et al., 2025). The nation's commercial banks have expanded their reach and services, catering to a growing customer base, and in the process, they have become repositories of vast troves of personal information. In this interconnected world, safeguarding the confidentiality, integrity, and availability of personal data has become a matter of paramount importance at both the national and international levels (Benedicta Ehimuan et al., 2024).

Commercial banks hold a vast repository of sensitive customer data, encompassing personal identification information, bank account details, credit/debit card numbers, and biometric data (Zhang et al., 2023). Safeguarding this information is paramount and should be a core strategic priority for these institutions. Failure to adequately protect customer data can trigger a cascade of severe consequences, including financial losses, regulatory non-compliance and penalties, customer dissatisfaction and attrition following by significant reputational damage (Folorunso et al., 2024).

In order to protect those sensitive customer data, Commercial banks in Ethiopia shall need to adopt the best data protection framework and customize upon the applicable points (Kinfe Micheal Yilma and Halefom Hailu Abraha, 2015). Even there are several data protection frameworks that applicable for the personal data protection in a glob such as California Consumer Protection Act (CCPA), Japan’s Act on the Protection of Personal Information (APPI) and EU GDPR; because of the GDPR most widely recognized and robust data protection that set clear, high standards for the personal data protection. As the Ethiopian banks have vision to operate internationally, the alignment of Ethiopian commercial banks with the GDPR framework is not merely a matter of regulatory compliance; it is a proactive step toward

securing the personal data of customers, instilling trust, and fostering international cooperation. This alignment also provides a competitive advantage by enabling Ethiopian banks to participate seamlessly in the global economy.

The European Union's General Data Protection Regulation (GDPR), implemented in 2018, (Štarchoň & Pikulík, 2019) represents a pivotal moment in global data protection standards. While GDPR is primarily designed for European Union member states, its influence extends far beyond the EU's borders. It is a model for data protection and privacy that sets rigorous standards for the treatment of personal data, impacting organizations worldwide, including those outside of the EU.

The General Data Protection Regulation (GDPR) stands out as one of the most comprehensive data privacy laws in the world. Its key strengths lie in its ability to ensure individuals' fundamental rights to privacy while enforcing strict data handling and processing standards for organizations. By providing a clear legal framework, GDPR enhances transparency and accountability, ensuring that businesses are held responsible for the personal data they collect. Notably, its global reach means that any organization dealing with EU residents must comply, fostering global consistency in data protection practices. Additionally, the regulation empowers individuals with greater control over their data, including the right to access, correct, and delete their personal information, thus setting a high bar for data privacy globally. With its strict penalties for non-compliance, GDPR ensures that both individuals and businesses benefit from a more secure and trustworthy digital environment.

However, this endeavour is not without its challenges. Ethiopian commercial banks face a complex regulatory environment, limited resources, varying levels of awareness about GDPR principles, and a dynamic landscape of cyber threats. Addressing these challenges and aligning with GDPR is a multi-faceted process that requires comprehensive research and practical solutions.

This thesis, titled "Designing a Comprehensive Framework for Personal Data Protection in Ethiopian Commercial Banks: Alignment with EU GDPR" aims to address the fundamental problem by focusing on the development of a structured, comprehensive framework expressly designed to ensure personal data protection in Ethiopian commercial banks. This framework, meticulously aligned with the stringent requirements of the EU GDPR, aims not only to enhance compliance but also to fortify the security and privacy of personal data within the Ethiopian banking sector.

This study is not only significant for Ethiopian commercial banks and the financial sector but also for regulatory authorities and policymakers. It contributes to the development of effective data protection practices and the strengthening of data security and privacy in an era where the global exchange of personal information is the norm. The journey to align Ethiopian commercial banks with GDPR is a step towards enhancing data protection, preserving customer trust, and fostering the growth of the banking sector in a globalized world.

1.2 Problem Statement

Ethiopian commercial banks are entrusted with vast volumes of sensitive customer data, which has become a cornerstone of their operations (Md Abdul Ahad Maraj, 2024). However, the management, protection, and compliance of this personal data with international standards, for example the European Union's General Data Protection Regulation (EU GDPR), present a significant challenge (Tikkinen-Piri et al., 2018). The problem at hand encompasses several critical issues:

A key issue is aligning with these standards and stringent data protection regulations, given resource limitations and difficulties in adopting advanced technologies (Lessa & Gebrehawariat, 2023; Yabets, 2019). This is compounded by a lack of awareness and varying levels of understanding of GDPR principles among bank stakeholders (Bogale et al., 2019). Furthermore, Ethiopian banks are exposed to significant data security vulnerabilities due to the evolving landscape of cyber threats and the absence of comprehensive data protection measures, leading to substantial risks to the security and confidentiality of personal data (Asfaw, 2023).

The confluence of these challenges underscores the absence of a tailored and comprehensive framework for personal data protection in Ethiopian commercial banks that aligns seamlessly with the stringent regulations mandated by the EU GDPR. Without a dedicated and effective framework, these banks face substantial risks in terms of non-compliance, data breaches, reputational damage, and potential financial implications. This thesis endeavours to address are the lack of a structured, comprehensive framework specifically designed to ensure personal data protection within Ethiopian commercial banks, aligned cohesively with the stringent guidelines and requirements of the EU GDPR. This lack hinders not only the adherence to international standards but also the establishment of a robust data protection system essential for ensuring data security and privacy within the Ethiopian banking sector.

1.3 Objectives of the Study

The objective of this thesis is divided to general objective and Specific objectives.

1.4.1 General Objective

The General objective of the research is to develop a comprehensive and tailored framework for personal data protection, specifically designed to address the challenges faced by Ethiopian commercial banks and aligned with the principles of the EU GDPR.

1.4.2 Specific Objectives

The specific objectives of the study are:

1. **Conduct a Comprehensive Gap Analysis**: Evaluate the existing data protection practices in Ethiopian commercial banks through a gap analysis, identifying areas of compliance and non-compliance with local and international standards, including the EU GDPR.
2. **Customize GDPR Principles for Local Context:** Adapt and customize the GDPR principles to suit the local context of Ethiopian commercial banks, considering regulatory requirements, cultural nuances, and specific challenges faced by the banking industry in Ethiopia.

1.4 Research Questions

The research questions for this research is focuses on understanding of the challenges of the commercial bank on protecting their customer's personal data and explore the potential solution to tackle the issue:

RQ1. What are the existing data protection practices in Ethiopian commercial banks?

RQ2. What are the key components of a comprehensive data protection framework tailored to Ethiopian commercial banks?

RQ3. How can the designed framework be effectively implemented within the operational context of Ethiopian banks?

1.5 Significance of the Study

The significance of the study lies in its potential to contribute valuable insights, address critical challenges, and make a positive impact on various stakeholders. The out lines are:

1. ***Enhancing Data Security in Ethiopian Commercial Banks:***

The study aims to design a tailored data protection framework, contributing to the enhancement of data security practices in Ethiopian commercial banks. This is crucial for safeguarding sensitive customer information, mitigating the risk of data breaches, and fostering a secure banking environment.

2. ***Aligning with International Standards:***

By aligning with the EU GDPR, the study addresses the global nature of data protection. Ethiopian commercial banks, through compliance with international standards, can position themselves as trustworthy entities on a global scale, facilitating international collaboration and partnerships.

3. ***Promoting Regulatory Compliance:***

The study seeks to assist Ethiopian commercial banks in navigating complex regulatory landscapes, ensuring compliance with local data protection regulations and international standards. Compliance is essential for avoiding legal ramifications, financial penalties, and reputational damage.

4. ***Improving Customer Trust and Confidence:***

Addressing data protection challenges and implementing a robust framework can significantly impact customer trust and confidence. Strengthening data security measures reassures customers that their personal information is handled with care and integrity, thereby fostering long-term relationships.

5. ***Enabling Organizational Resilience:***

The study's focus on operational resilience equips Ethiopian commercial banks with strategies to mitigate the impact of potential data breaches. This contributes to the overall resilience of banking operations, ensuring continuity and minimizing disruptions.

6. ***Supporting Ethical Data Handling:***

Ethical considerations are integral to the study's framework. By promoting ethical data handling practices, the research emphasizes the importance of respecting privacy rights and conducting banking operations in an ethically responsible manner.

7. ***Providing a Framework for Future Research and Development:***

The study lays the groundwork for future research in the field of data protection in developing economies. It serves as a reference point for researchers, policymakers, and practitioners seeking to further refine data protection frameworks and practices.

1.6 Scope and Limitation

Defining the scope and limitations of thesis is crucial to provide clarity on the boundaries and focus of the research.[1] By clearly defining the scope and limitations, it provides transparency about the parameters of the research, allowing readers and stakeholders to understand the context within which the findings and recommendations are applicable.

1.6.1 Scope of the Study:

The study focuses on Ethiopian commercial banks, specifically examining the local context and challenges related to personal data protection. It centres on the European Union's General Data Protection Regulation (EU GDPR) as the primary regulatory framework, exploring the alignment of Ethiopian banks with its principles. The study covers a range of personal data types, including customer information and financial transactions, and investigates the existing technological infrastructure within these banks. Additionally, it proposes enhancements to ensure compliance with GDPR requirements. Operational processes concerning data handling, storage, and transmission within the banking environment are also integral to the scope of the research.

1.6.2 Limitations of the Study:

The study's findings and recommendations are specific to Ethiopian commercial banks and may not be directly applicable to other industries or regions. It considers the regulatory environment as it stands during the research period, acknowledging that changes in regulations post-research are outside its scope. Resource constraints, both financial and technological, may limit the implementation of proposed enhancements in certain banks. While the human factor in data protection is considered, the study does not delve into the psychology or behavioral aspects of employees and customers. Socio-political factors, such as changes in government policies or public perceptions, are also outside the study's scope. Additionally, the research

[1] https://researcher.life/blog/article/decoding-the-scope-and-delimitations-of-the-study-in-research/

does not conduct an exhaustive technology audit of each bank but focuses on proposing general technological improvements aligned with GDPR principles. Finally, the evaluation of the long-term effectiveness of the proposed framework is acknowledged as a complex task that may require further research beyond the study's current scope.

1.7 Thesis Structure

The organization of this thesis is structured to present the research in a logical and coherent manner, divided into six chapters. Chapter One introduces the research by outlining its objectives, scope, and significance. Chapter Two reviews pertinent literature, establishing the academic groundwork and pinpointing the gaps the study intends to fill. Chapter Three elaborates on the research methodology, discussing the research design, data collection methods, sampling techniques, data analysis procedures, framework development processes, and ethical considerations. Chapter Four focus on data collection and analysis, showcasing the gathered data, identifying trends, and deriving conclusions. Chapter Five expands on these insights to create a comprehensive personal data protection framework specifically designed for Ethiopian commercial banks, addressing their distinct challenges while conforming to international standards. Lastly, Chapter Six wraps up the study by summarizing the findings, providing actionable recommendations for stakeholders, and highlighting areas for future research, thereby ensuring the study's contribution to both academic and practical advancements in data protection.

Chapter Two

Literature Review

2.1 Overview of Data Protection

Data protection is paramount in today's digital age (Azamat, 2023), where the rapid advancement of technology and the internet has transformed the way we collect, store, and share information. Safeguarding the privacy, integrity, and confidentiality of personal and sensitive information is essential not only for individuals but also for organizations that handle vast amounts of data (Yadav et al., 2023). As data volumes continue to grow exponentially, driven by the proliferation of devices, social media, and online transactions, the need for robust data protection measures becomes increasingly critical (Gutwirth et al., 2011).

A data breach or loss can have severe financial, reputational, and legal consequences for organizations. Financially, the costs associated with a data breach can be staggering, including expenses related to remediation, legal fees, regulatory fines, and potential compensation to affected individuals (Rodrigues et al., 2024). Reputational damage can lead to a loss of customer trust, which is often difficult to rebuild, resulting in decreased sales and market share. Legally, organizations may face lawsuits from customers or regulatory bodies, further compounding the financial impact.

Organizations must prioritize data protection to ensure business continuity and maintain customer trust. This involves implementing comprehensive data protection strategies that include encryption, access controls, regular security audits, and employee training on data handling best practices(Excel G Chukwurah & Samuel Aderemi, 2024). Additionally, organizations should stay informed about the latest data protection regulations and compliance requirements, such as the European Union General Data Protection Regulation (EU GDPR) and Ethiopian Personal data protection regulation Proclamation No. 1321 /2024.

A regulatory framework like the General Data Protection Regulation (GDPR) achieves several critical objectives that are essential for safeguarding individual privacy in the digital age. First and foremost, it provides clear and comprehensive guidelines on the scope and nature of fundamental rights related to data privacy. This is particularly important as it emphasizes the sovereign role of the data subject—the individual whose personal data is being processed—in controlling their own personal information. By establishing these rights, the GDPR empowers

individuals to make informed decisions about how their data is collected, used, and shared, thereby enhancing their autonomy and agency in the digital landscape(Sion et al., 2021).

In addition to defining individual rights, the GDPR plays a crucial role in raising widespread awareness about the significant impact that large-scale, contemporary, software-driven data processing operations can have on individuals' rights and freedoms. In an era where data is often referred to as the new oil, the regulation highlights the potential risks and challenges associated with the misuse of personal data. It encourages organizations, policymakers, and the public to engage in discussions about data ethics, privacy concerns, and the implications of technology on society. This heightened awareness is vital for fostering a culture of respect for privacy and accountability among data handlers.

Finally, the GDPR creates a sense of urgency and imposes accountability on organizations by compelling them to proactively prioritize and respect these rights and principles. It establishes a framework that requires organizations to embed data protection into their operations and decision-making processes, often referred to as "privacy by design." This means that data protection considerations must be integrated into the development of new products, services, and technologies from the outset, rather than being an afterthought. By doing so, the GDPR ensures that organizations take their responsibilities seriously and are held accountable for their data processing activities, ultimately leading to a more trustworthy and secure digital environment for individuals.

In conclusion, as we navigate an increasingly data-driven world, the importance of data protection cannot be overstated. It is not merely a technical issue but a fundamental aspect of ethical business practices and customer relations. By investing in data protection, organizations can safeguard their assets, protect their customers, and ultimately ensure their long-term success in a competitive landscape.

2.2 Personal data protection frameworks

Data privacy frameworks are comprehensive and structured sets of principles, regulations, and guidelines that are meticulously designed to govern the collection, use, storage, and sharing of personal information. These frameworks play a crucial role in ensuring that individuals' privacy is effectively safeguarded in an increasingly digital world where personal data is frequently collected and processed (Benedicta Ehimuan et al., 2024).

At the core of these frameworks are guiding principles that govern how organizations should handle personal data. These principles provide a clear path towards compliance with diverse privacy regulations, including the GDPR in Europe, the CCPA in the United States, and other regional frameworks. By adhering to these guidelines, organizations can effectively uphold individual rights, such as the right to access, erase, and transfer their personal data.

Moreover, data privacy frameworks emphasize the importance of strengthening data security measures. This necessitates the implementation of robust technical and organizational safeguards to protect personal information from unauthorized access, breaches, alteration, and other security threats. By adhering to these standards, businesses can handle data responsibly, ensuring that they not only comply with legal requirements but also align with industry best practices that promote trust and transparency.

In addition to legal compliance, data protection frameworks offer significant benefits to businesses. They enable organizations to make informed decisions regarding customer privacy, which can enhance customer trust and loyalty. By demonstrating a commitment to protecting personal information, businesses can differentiate themselves in a competitive market.

Moreover, these frameworks assist organizations in maintaining compliance with relevant legal and regulatory requirements, thus mitigating the risk of legal penalties associated with non-compliance. Non-compliance can have severe consequences, including substantial financial losses, reputational damage, and erosion of customer trust. By proactively implementing data privacy frameworks, businesses can effectively mitigate these risks and cultivate a culture of accountability and responsible data handling practices.

2.2.1 EU General Data Protection Regulation (GDPR)

The European Union's General Data Protection Regulation (GDPR), enacted on May 25, 2018, regulates the processing and transfer of personal data of individuals residing within the European Union. This comprehensive privacy regulation applies to organizations across all sectors and of all sizes, replacing the previous Data Protection Directive 1995/46. The fundamental goals of the GDPR remain consistent with the Directive—establishing clear rules

for the protection of personal data and ensuring the lawful data movement within and outside the EU[2].

The General Data Protection Regulation (GDPR) is a far-reaching piece of legislation with a broad scope and expansive definitions, significantly impacting how organizations handle personal data. It encompasses any information that can be used to directly or indirectly identify a living individual, including names, email addresses, tax ID numbers, online identifiers, and other relevant data points. This broad definition of 'personal data' encompasses a wide range of information that can be used to directly or indirectly identify an individual, thereby encompassing a significant amount of data processed by organizations.

The stringent data protection standards established by the GDPR have served as a model for privacy regulations in other jurisdictions, such as the California Consumer Privacy Act (CCPA) in the United States (Illman & Temple, 2019), India's new Personal Data Protection Bill (Parliament of the Republic of India, 2018, (Govindarajan, V., Srivastava, A., & Enache, 2019) and Japan's update to the Act on the Protection of Personal Information (Kitayama, n.d.)

Furthermore, the GDPR defines 'processing' comprehensively to encompass a wide range of activities, including the collection, recording, storage, and transfer of personal data. This broad definition means that many organizations are likely to be subject to the GDPR, even if they do not explicitly collect or store personal data.

The GDPR's broad scope and definitions have led to some confusion and debate about its applicability. However, it is important to note that the GDPR is intended to protect individuals' privacy rights and to confirm that organizations are transparent about how they collect and use personal data.

An organization not established within the European Union (EU) may still be subject to the GDPR when processing the personal data of individuals residing in the EU or the European Economic Area (EEA), which includes Norway, Liechtenstein, and Iceland. This applies specifically when the company actively offers goods or services to individuals within the EU or when it monitors the behaviour of individuals within the EU. While simply having a website accessible within the EU generally does not trigger GDPR compliance, other evidence

[2] https://privacyshield.gov/ps/article?id=European-Union-Data-Privatization-and-Protection#:~:text=GDPR%20is%20a%20comprehensive%20privacy,for%20the%20movement%20of%20data.

demonstrating an intent to offer goods or services to individuals within the EU will be considered relevant.

Scope of EU GDPR

Its extensive scope covers personal data, which includes any information that can identify an individual either directly (such as names and addresses) or indirectly (like IP addresses, cookies, and location data). The regulation broadly defines processing to include nearly any action taken on personal data, such as collection, storage, sharing, and deletion. This ensures that all facets of personal data handling are governed by GDPR's stringent framework.

Importantly, the GDPR has extraterritorial applicability, meaning it extends its influence beyond the borders of the EU. It applies to organizations with a presence in the EU, such as offices or employees, as well as to companies outside the EU that provide goods or services to EU residents, whether for free or for a fee. Furthermore, organizations that track the behavior of EU residents through cookies or other tracking technologies must comply with GDPR requirements, even if they do not have a physical presence in the EU. This broad scope underscores GDPR's aim to protect data rights globally, solidifying its position as a leading standard for privacy legislation.

GDPR Key Principles:

Simply put, the data processing requirements enforced by the GDPR are rooted in Seven general principles for privacy(Štarchoň & Pikulík, 2019). Understanding those Seven principles of the GDPR will make it easier for you to understand the rules and regulations.

Article 5 of the General Data Protection Regulation (GDPR) outlines the crucial rules that form the foundation of the data protection system (Hustinx, n.d.). These fundamental principles are outlined at the outset of the GDPR and exert a significant influence on all other requirements and guidelines within the legislation. Consequently, ensuring compliance with these core data protection principles is the first crucial step for controllers to fulfill their obligations under the GDPR. An outline of the Data Protection Principles contained in Article 5 of the GDPR is provided below(Calder et al., n.d.):

Lawfulness, fairness, and transparency: The processing of personal data must be lawful, fair, and transparent. Individuals must be informed about the collection, use, consultation, or other processing of their personal data, as well as the extent to which this processing will occur.

Purpose Limitation: Personal data should only be collected for specified, explicit, and legitimate purposes. Further processing of data for purposes incompatible with the original collection purpose is generally prohibited, except in certain cases such as archiving for public interest, scientific, or historical research purposes, or for statistical purposes as outlined in Article 89(1) of the GDPR.

Data Minimisation: The processing of personal data must be adequate, relevant, and limited to what is necessary for the intended purposes. This necessitates minimizing the storage period of personal data to the absolute minimum required.

Accuracy: Controllers must ensure the accuracy and, where necessary, the up-to-datedness of personal data. Every reasonable step must be taken to ensure that inaccurate personal data, considering the purposes for which it is processed, is erased or rectified without delay.

Storage Limitation: Personal data should only be retained in a form that permits identification of the data subject for the duration necessary to fulfill the intended processing purposes. To ensure compliance with this principle, controllers must establish time limits for the erasure or periodic review of personal data.

Integrity and Confidentiality: Personal data must be processed in a manner that ensures appropriate security and confidentiality, including protection against unauthorized or unlawful access, use, alteration, disclosure, destruction, or accidental loss. This requires the implementation of appropriate technical and organizational measures.

Accountability: The controllers are responsible for ensuring compliance with all of the aforementioned Data Protection Principles and must be able to demonstrate this compliance.

Rights of Data Subjects

The GDPR empowers data subjects with seven key rights, enabling them to exert greater control over their personal data and ensuring transparency in its processing. An overview of these rights is provided below. (Hoofnagle et al., 2019):

The right to data portability empowers individuals to receive their personal data in a structured, commonly used, and machine-readable format, facilitating seamless data transfer between different service providers. This right is applicable only when the processing is based on

consent or contractual necessity. The right to rectification allows individuals to correct inaccurate data, while the right to restriction allows them to limit processing in certain situations, such as when processing is unlawful or data accuracy is disputed.

Furthermore, data subjects possess the right to object to the processing of their personal data, particularly when such processing is based on legitimate interests or public interest grounds. This right to object is absolute in the context of direct marketing. The "right to be forgotten" allows individuals to request the deletion of their data in cases of data irrelevance, unlawful processing, or withdrawn consent, with exceptions for situations like conflicts with freedom of expression. Lastly, the GDPR addresses profiling and automated decision-making through the right to resist profiling, which prohibits fully automated decisions with significant consequences unless justified by law, consent, or contractual necessity, and mandates safeguards like human intervention to protect the individual's interests. Collectively, these rights strengthen data protection and accountability in data processing practices.

Obligations for Data Controllers and Processors

To ensure GDPR compliance, data controllers and processors must adhere to nine key obligations (Hoofnagle et al., 2019). These include:

1. **Record-keeping:** Maintaining comprehensive records of processing activities, encompassing the types of data processed, the purposes for which it is processed, access controls, data retention periods, and implemented security measures. This creates a roadmap for regulators during investigations.
2. **Data Protection Policy:** Adopting a policy outlining the rationale for data collection, purposes, accuracy maintenance, access controls, etc.
3. **Transparency:** Providing data subjects with clear and readily accessible information about data processing practices, including prompt responses to data subject requests and clear explanations for any denials of such requests.
4. **Data Protection by Design and Default:** Incorporating privacy protections into the technical design and default settings of systems.
5. **Data Protection Officer (DPO):** Appointing a DPO for large-scale or sensitive data processing. The DPO oversees compliance, advises on GDPR requirements, cooperates with Data Protection Authorities, and acts as a contact point for data subjects and authorities.

6. **Data Protection Impact Assessments (DPIAs):** Conducting DPIAs for high-risk processing activities, such as automated decision-making with significant effects on individuals, large-scale sensitive data processing, and systematic monitoring of publicly accessible areas. Failure to conduct a DPIA when required is a violation itself.
7. **Organizational Safeguards:** Implementing organizational measures, such as access restrictions and logging, to ensure data security.
8. **Technical Safeguards:** Implementing appropriate technical security measures to protect against data loss, destruction, damage, and unauthorized access or processing. These measures should be proportionate to the risks involved.
9. **Personal Data Breach Notification:** Notifying the Data Protection Authority (and data subjects if high risk) of personal data breaches within 72 hours of discovery, unless the breach is unlikely to result in a risk to individuals. All breaches must be documented.

The GDPR emphasizes that controllers are primarily responsible for compliance, even for actions of processors. Processors have significant responsibilities as well, including contractual commitments on data use, security, breach notification, and data retention. The consequences of non-compliance are substantial, including significant fines, legal actions by individuals or representative organizations, and potential damage to reputation.

Penalties for non-compliance

GDPR fines must be effective, proportionate, and serve as a strong deterrent in each case. To determine the appropriate level of fines, authorities consider various factors, including the intentional nature of the infringement, the company's efforts to mitigate the damage, and their cooperation with authorities. These factors can significantly influence the final penalty amount.

For the most severe violations outlined in Article 83(5) of the GDPR, fines can reach up to €20 million or 4% of the company's global annual turnover in the preceding year, whichever is higher. Even for less severe violations listed in Article 83(4), fines can be substantial, reaching up to €10 million or 2% of the company's global annual turnover in the preceding year, whichever is higher (Wolff & Atallah, 2020).

2.2.2 The California consumer privacy act (CCPA)

The California Consumer Privacy Act (CCPA) is a significant data privacy legislation designed to strengthen consumer rights concerning personal information gathered by businesses. It was

signed into law on June 28, 2018, and took effect on January 1, 2020. The CCPA is recognized as one of the most extensive privacy laws in the United States. It is frequently likened to the EU's GDPR because of its emphasis on consumer empowerment and data transparency, although it includes specific provisions suited to the U.S. regulatory framework (Pardau, 2018).

The California Consumer Privacy Act (CCPA) is a landmark piece of legislation that aims to enhance privacy rights and consumer protection for residents of California. One of the key components of the CCPA is its broad definition of "personal information." This term encompasses a wide array of data types that can be used to identify an individual. Specifically, personal information includes, but is not limited to, the following categories:

1. **Names and Aliases**: This includes not only a person's full name but also any nicknames or pseudonyms they may use.

2. **Postal Addresses**: Any physical address where an individual resides or receives mail is considered personal information.

3. **IP Addresses**: An Internet Protocol (IP) address, a unique numerical label assigned to each device on a network using the Internet Protocol for communication, is considered a form of personal information under certain circumstances.

4. **Social Security Numbers**: This sensitive information, which is often used for identification and verification purposes, is protected under the CCPA.

5. **Biometric Information**: This includes data derived from physical or behavioural characteristics, such as fingerprints, facial recognition data, and voiceprints.

6. **Geolocation Data**: Information that can pinpoint an individual's location, often collected through mobile devices or GPS technology, falls under this category.

7. **Professional or Employment-Related Information**: This encompasses details about an individual's job history, professional qualifications, and employment status.

8. **Education Information**: Any data related to an individual's educational background, including schools attended, degrees earned, and academic performance, is also included.

The CCPA's applicability is extensive, as it covers personal information collected by businesses from consumers, irrespective of the format in which this information is gathered.

This means that whether the data is collected electronically through websites and apps, in paper form through physical documents, or through any other means, it is subject to the regulations set forth by the CCPA. This comprehensive approach aims to ensure that consumers have greater control over their personal information and how it is used by businesses.

Specific Rights of Consumers

The California Consumer Privacy Act (CCPA) is a landmark piece of legislation that significantly enhances consumer rights regarding personal information. Under the CCPA, consumers are granted several critical rights that empower them to take control of their personal data in an increasingly digital world(Pardau, 2018).

Firstly, consumers have the right to know what personal information a business collects about them. This includes not only the specific data points collected, such as names, addresses, and email addresses, but also the sources from which this information is obtained. Businesses are required to disclose how they use this information, whether for marketing, service improvement, or other purposes. This transparency is designed to help consumers make informed decisions about their interactions with businesses.

Secondly, consumers possess the right to request the deletion of their personal information. However, there are certain exceptions to this right. For instance, businesses may retain personal information if it is necessary for security purposes, such as preventing fraud or data breaches. Additionally, businesses may need to keep certain information to comply with legal obligations, such as tax or employment laws. This balance aims to protect both consumer privacy and the operational needs of businesses.

Another significant right granted by the CCPA is the ability for consumers to opt-out of the sale of their personal information. This means that consumers can instruct businesses not to sell their data to third parties, which is particularly important in an era where data monetization is prevalent. By exercising this right, consumers can limit the exposure of their personal information and reduce the risk of it being used in ways they do not consent to.

Scope of CCPA

The California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA) are significant pieces of legislation that aim to enhance consumer privacy rights and establish

a framework for businesses to handle personal information responsibly. These laws are notable for their broad extraterritorial reach, meaning they can apply to businesses regardless of their physical location, as long as they meet specific criteria related to their operations involving California residents (Byun, 2020).

To determine whether a business is subject to the CCPA and CPRA, it must satisfy the following conditions:

1. **Does Business in California**: This criterion encompasses a variety of activities that indicate a business's engagement with California residents. It includes:
    - Conducting transactions with individuals residing in California, which could involve selling goods or services.
    - Employing individuals who are California residents, thereby establishing a workforce presence in the state.
    - Paying taxes to the state of California, which signifies a financial connection to the state.
2. **Collects Personal Information and Meets Thresholds**: A business must collect personal information from California residents and meet at least one of the following thresholds to be subject to the CCPA and CPRA:
    - **Annual Gross Revenue**: The business's annual gross revenue must exceed $25 million. This threshold is designed to capture larger businesses that have significant financial resources and customer bases.
    - **Volume of Personal Information**: The business must buy, sell, receive, or share the personal information of more than 100,000 California consumers, households, or devices annually. This criterion focuses on the scale of data handling and the potential impact on consumer privacy.
    - **Revenue from Personal Information**: The business derives at least 50% of its annual revenue from selling or sharing the personal information of California consumers. This condition targets businesses that rely heavily on monetizing consumer data.

If a business meets any of these criteria, it is obligated to comply with the data privacy requirements set forth by the CCPA and CPRA. This includes implementing measures to

protect consumer data, providing transparency about data collection and usage practices, and allowing consumers to exercise their rights regarding their personal information, such as the right to access, delete, or opt-out of the sale of their data.

CCPA fines and penalties

The CCPA establishes specific penalties for businesses that fail to comply with its provisions (Bradley, 2024).

- **Civil Penalties**: Civil penalties under the CCPA can be significant, reaching up to $7,500 per intentional violation and $2,500 per unintentional violation if not rectified within 30 days. This poses a substantial financial risk, especially for companies handling large volumes of consumer data.
- **Consumer Lawsuits**: Furthermore, the CCPA empowers consumers to file lawsuits against businesses for certain data breaches. In the event of a data breach resulting from a failure to implement reasonable security measures, businesses may be held liable for damages, which can range from $100 to $750 per consumer per incident or actual damages incurred by the consumer, whichever is greater

2.2.3 Ethiopia's personal data protection proclamation

On April 4, 2024, Ethiopia's House of Peoples' Representatives passed the Personal Data Protection Proclamation No. 1321/2024 (PDP Proclamation), representing a crucial advancement in the protection of privacy rights within the nation. This extensive legislation establishes a strong regulatory framework for personal data protection, filling a significant void in Ethiopian law, where regulations were previously scattered across multiple legal documents.

The Proclamation is designed to safeguard individual privacy and foster a secure digital economy. It accomplishes this by providing clear definitions for essential terms such as "personal data," "biometric data" (including fingerprints and facial recognition), "sensitive personal data," and "generic data." These definitions enhance understanding, allowing both data subjects and data controllers/processors to grasp the extent of protection and their respective responsibilities(Haile, 2024).

By delineating the types of data that are protected and specifying acceptable uses, the law grants individuals increased control over their personal information while guiding organizations in ethical and compliant data management practices. This dual emphasis on individual rights and

organizational responsibility underscores Ethiopia's dedication to aligning with international data governance standards.

The Scope of Application

The Personal Data Protection Proclamation has a wide-ranging application concerning the management of personal information, which includes both automated and manual data processing within filing systems. It applies to data controllers and processors based in Ethiopia, regardless of the physical location of the data. Additionally, the Proclamation covers foreign entities that utilize equipment for data processing within Ethiopia (excluding transit operations), as long as they have a designated representative in the country.

The law is applicable to both private and public organizations, including federal and regional government agencies and city administrations that handle personal data.

Exemptions Certain activities are not covered by the Proclamation, such as:

- ✓ Personal or Household Activities: Processing done solely for personal use.
- ✓ Inter-Agency Information Sharing: Limited to government agencies that operate on a need-to-know basis.
- ✓ Specific Exemptions: Safeguarding national security, defense, or public safety.
- ✓ Historical, statistical, and scientific research purposes.
- ✓ Public interest objectives, including economic or financial state interests.
- ✓ Protection of judicial independence and proceedings.
- ✓ Data Transit: Data that originates outside of Ethiopia and merely passes through the country.
- ✓ This comprehensive framework ensures extensive coverage while allowing for flexibility in activities that necessitate exemptions, thereby balancing the protection of individual rights with national and operational requirements.

Individual Rights

The Personal Data Protection Proclamation grants individuals substantial control over their personal information. It outlines the following rights for data subjects:

Rights of Individuals:

- ✓ **Access**: Individuals have the right to view their personal data held by organizations.
- ✓ **Rectification**: They can request corrections for any inaccurate information.
- ✓ **Erasure**: Individuals can request the deletion of their data when it is no longer necessary.
- ✓ **Restriction**: They can limit the processing of their data.
- ✓ **Objection**: Data subjects can refuse the use of their data for targeted marketing or automated decision-making.

The Proclamation mandates that data controllers, which are organizations that manage personal data, must register with the Ethiopian Communication Authority (ECA) prior to processing any data. The ECA serves as the official regulatory body responsible for enforcing the Proclamation and ensuring adherence to its provisions. Data controllers are obligated to secure informed consent from individuals before handling their personal information. Additionally, they are required to implement robust security measures to protect the data and to promptly report any data breaches. The Proclamation also governs cross-border data transfers, allowing such transfers only if they comply with applicable data protection regulations and if adequate safeguards are established in the receiving country. The following outlines the specific safeguards or conditions necessary for cross-border data transfer:

The Proclamation assigns data controllers, organizations that handle personal data, the responsibility to register with the Ethiopian Communication Authority (ECA) before processing any data. The ECA is designated as the regulatory body to enforce the Proclamation and ensure compliance. Data controllers are required to obtain informed consent from individuals before processing their personal data. They must also implement strong security measures to protect this data and report any data breaches promptly. The Proclamation also regulates cross-border data transfers, allowing them only if they comply with relevant data protection regulations and appropriate safeguards are in place in the receiving jurisdiction.

The Proclamation outlines specific guidelines for data retention, emphasizing the importance of responsible data management practices. Data controllers, which include organizations and individuals who handle personal information, are required to store such data only for a "reasonable time necessary" to fulfil the intended purpose for which the data was collected. This means that once the purpose has been achieved, data controllers must take appropriate measures to delete or anonymize the data to protect individuals' privacy.

However, there are notable exceptions to this rule. For instance, if explicit consent is given by the individual whose data is being processed, data controllers may retain the information for a longer period. This consent must be informed, meaning that individuals should be fully aware of how their data will be used and for how long it will be retained. Additionally, data may be retained if it is required for historical research purposes, allowing researchers to access valuable information that can contribute to academic and scientific advancements.

To ensure transparency and accountability in the implementation of the Proclamation, the designated authority is mandated to report on its effectiveness. This reporting will keep the public informed about how well the legislation is being enforced and whether it is achieving its intended goals. Regular updates and assessments will help build trust between the public and the authorities responsible for data protection.

The ECA, as the designated supervisory body, will play a pivotal role in overseeing the implementation and enforcement of these regulations. This body is tasked with monitoring compliance among both individuals and organizations, ensuring that they adhere to the established guidelines for data retention. The ECA will also have the authority to investigate any breaches of the Proclamation and impose penalties where necessary, thereby reinforcing the importance of data protection and privacy rights. Through its efforts, the ECA aims to create a culture of compliance and respect for personal data, ultimately safeguarding individuals' rights in the digital age.

Penalties for Violations

To promote responsible data management and prevent violations, the law establishes penalties for non-compliance. Fines for specific offenses can range from 60,000 to 100,000 Birr, and more severe violations may lead to imprisonment. This highlights the necessity for organizations to prioritize data privacy and comply with the regulations.

2.2.4 EU GDPR Vs California Consumer Privacy Act (CCPA) Vs The Ethiopian Personal Data Protection Proclamation (EPDPP)

The EU General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and the Ethiopian Personal Data Protection Proclamation (EPDPP) all encompass core principles and goals focused on safeguarding personal data. Although they were developed

in distinct legal and cultural environments, these regulations display significant similarities, such as:

Similarities

In one or other those regulations have a common point that they share each other. Those similar points are discussing here below in detail.

- **Purpose**: The primary aim of data protection regulations is to safeguard individuals' personal data and privacy. These laws are designed to create a framework that governs how organizations collect, use, store, and share personal information. By establishing clear guidelines, these regulations help ensure that individuals' privacy is respected and that their data is handled responsibly.
- **Individual Rights**: Data protection laws grant individuals a variety of rights concerning their personal information. These rights typically include the ability to access their data, request corrections for any inaccuracies, and seek deletion of their data under specific circumstances. For instance, the General Data Protection Regulation (GDPR) includes a "right to be forgotten," allowing individuals to request the removal of their personal data when it is no longer necessary for the purposes for which it was collected. Similarly, the California Consumer Privacy Act (CCPA) provides a "right to delete," enabling consumers to request the deletion of their personal information held by businesses. The Ethiopian Personal Data Protection Proclamation (EPDPP) also includes comparable provisions to ensure individuals can exercise control over their personal data.
- **Transparency Requirements**: Transparency is a critical component of data protection regulations. Organizations are required to inform individuals about the data they collect, the purposes for which it is processed, and the rights individuals have regarding their data. This is typically achieved through privacy notices or policies that clearly outline how personal information will be handled. By promoting transparency, these regulations empower individuals to make informed decisions about their data and enhance trust between consumers and organizations.
- **Security Obligations**: To protect personal data from unauthorized access, loss, or misuse, data protection laws impose security obligations on organizations. These obligations mandate that organizations implement appropriate technical and organizational measures to safeguard personal information. This may include

encryption, access controls, regular security assessments, and employee training on data protection practices. By enforcing these security measures, regulations aim to minimize the risk of data breaches and ensure that individuals' personal information is adequately protected.

- **Penalties for Non-Compliance**: Failure to comply with data protection regulations can lead to significant consequences for organizations. Non-compliance may result in hefty fines, legal actions, and reputational damage. For example, under the GDPR, organizations can face fines of up to 4% of their annual global turnover or €20 million, whichever is higher. Similarly, the CCPA imposes penalties for violations, which can include fines for each instance of non-compliance. These penalties serve as a deterrent, encouraging organizations to adhere to data protection laws and prioritize the privacy of individuals.
- **Territorial Scope**: Data protection regulations often extend beyond the borders of the jurisdictions in which they were enacted. For instance, the GDPR applies to any entity that processes the personal data of EU residents, regardless of whether the entity is located within the EU. This extraterritorial application ensures that individuals' data is protected even when processed by organizations outside the EU. The CCPA similarly applies to businesses outside California if they meet certain criteria, such as processing the personal information of California residents. The EPDPP also has a territorial scope that encompasses personal data processing involving Ethiopian residents, ensuring that their data is protected regardless of where the processing occurs. This global approach to data protection reflects the increasing interconnectedness of the digital world and the need for comprehensive privacy safeguards.

Differences

Although the EU GDPR, CCPA, and Ethiopian Personal Data Protection Proclamation (EPDPP) have fundamental principles in common, their variations highlight the unique legal, cultural, and economic environments from which they originated. The distinctions are tabulated below.

Feature	EU GDPR	CCPA	Ethiopian Personal Data Protection Proclamation
Jurisdiction	Applies across the European Union and beyond.	Applies to businesses in California or targeting Californians.	Applies within Ethiopia and to entities processing Ethiopian residents' data.
Scope of Application	Broad: covers all entities processing personal data.	Applies to for-profit businesses meeting certain thresholds (e.g., revenue > $25M).	Covers both private and public entities, with broader applicability.
Legal Basis for Processing	Requires a legal basis (e.g., consent, contract, legitimate interest).	Focuses on consumer rights, does not require a specific legal basis.	Requires a legal basis (e.g., consent, contract, legitimate interest).
Consumer Rights	Extensive, including data portability and objection to processing.	Includes rights to know, delete, and opt-out of data sales.	Right to be Informed, Right of Access, Right to Rectification, Right to Erasure, Right to Object
Penalties	Fines up to €20 million or 4% of global revenue.	Fines up to $7,500 per intentional violation.	Fines for specific offenses can range from 60,000 to 100,000 Birr, and more severe violations may lead to imprisonment.
Data Protection Authority	Supervisory authorities in each EU member state.	No dedicated authority; enforced by the Attorney General.	Ethiopian Communication Authority (ECA)
Sensitive Data	Explicitly defines sensitive data with stricter rules.	Does not explicitly classify sensitive data but has protections for specific categories.	Similar to GDPR with defined sensitive data protections.
Data Breach Notification	Requires notification within 72 hours.	Requires notification without unreasonable delay.	Requires prompt notification, likely similar to GDPR.

Table 1 - EU GDPR Vs CCPA Vs Ethiopian PDPP

2.3 Data Protection in Banking

The term 'banking' encompasses a broad spectrum of financial institutions, ranging from small savings and loan organizations to large, internationally active commercial banks (Shelagh Heffernan, 2005). Some of the banks operating today have a long and established history, spanning generations. This enduring presence may contribute to customer trust, as it fosters a sense of stability and confidence in the bank's ability to safeguard their funds and personal information.

The rapid technological advancements of the past decade, characterized by a significant shift towards the online world, the emergence of data as a critical commodity, and the increasing integration of data processing into daily life, have rendered outdated a legislative framework for data protection that was established in an era when computers and information and communication technologies were still in their nascent stages (Giurgiu & Lallemang, n.d.).

While banks have maintained significant amounts of personal and financial information about their customers, advancements in technology have made this data increasingly accessible to authorized personnel within the institution (Md Abdul Ahad Maraj, 2024). The rapid advancement of financial technology in recent decades, encompassing innovations such as wire transfers, credit/debit cards, online banking, and mobile payments, has necessitated significant transformations within the banking sector. Banks must not only modernize their systems to accommodate these technological advancements but also implement robust security measures to protect sensitive customer information from cyber threats, including phishing and malware attacks.

As banking regulations evolve to address the complexities of modern financial systems, banks face increasing pressure to safeguard customer data from cyberattacks and unauthorized access. This article will explore the strategies employed by modern banks and financial institutions to fulfil this critical responsibility.

To effectively safeguard sensitive data, banks must adopt a comprehensive, multi-layered approach to security, encompassing both internal and external threats. This necessitates securing all aspects of banking operations, from customer-facing interfaces to internal processes, employee activities, vendor relationships, and underlying systems. The following sections will explore some of the key strategies employed by banks to achieve this level of security (Codina Sabau, 2022).

2.3.1 Authentication

Authentication is a critical security measure that mandates the verification of the identity of any individual initiating a transaction within the banking system. This applies across all channels, including online and mobile banking platforms, in-person interactions at bank branches, and transactions conducted via credit/debit cards at POS terminals and ATMs. Furthermore, robust authentication protocols are essential for bank employees accessing customer and bank data. While traditional authentication methods relied primarily on IDs and passwords or PINs, modern banks have increasingly adopted two-factor and multi-factor authentication, as well as biometric techniques, such as behavioral biometrics, to enhance security across various channels, including Interactive Voice Response (IVR) systems

2.3.2 Audit Trails

Banks have always maintained transaction records, providing statements and passbooks. Additionally, robust audit trails capture all customer interactions. Transaction data, including time and details, is recorded across all channels (in-branch, online, mobile). This data is backed up daily, archived, and never permanently deleted

2.3.3 Secure Infrastructure

A holistic approach to infrastructure security involves a combination of technological solutions, user education, and proactive management to create a resilient defense against a wide range of cyber threats. Regularly updating security measures and staying informed about the evolving threat landscape is crucial for maintaining a secure infrastructure. A secure infrastructure requires robust protection of database systems and servers, with strong access controls and encryption of production data.

A holistic approach to infrastructure security necessitates a multi-layered defense, encompassing technical, procedural, and organizational safeguards. This includes network security, access control, data encryption, endpoint security, patch management, disaster recovery, security training, vendor security assessments, and regulatory compliance.

Continuous monitoring, adaptation to evolving threats, and a combination of technological, educational, and proactive management measures are crucial for maintaining a secure and resilient infrastructure.

2.3.4 Secure Processes

To ensure robust security, banks have implemented a comprehensive framework that includes KYC updates, NDAs, and secure premises. DLP solutions are crucial for mitigating insider threats and ensuring compliance with regulations like the GDPR. Regular risk assessments and adherence to global and local regulations are essential for maintaining a strong security posture and safeguarding customer information.

2.3.5 Continuous Communication

Banks actively engage with customers through various channels, providing regular updates on system upgrades, new authentication procedures, and periodic account statements. To enhance security and customer awareness, banks offer flexible options for customers to set spending limits and alerts for unusual account activity. This proactive approach ensures customers are informed about potential threats and empowers them to manage their accounts securely and efficiently.

2.4 Motivation of the study

In the dynamic landscape of modern banking, the custodianship of personal data stands as an imperative cornerstone, shaping the trust, integrity, and operational credibility of financial institutions (Ml & Zahid, 2023). Ethiopian commercial banks, as key players in the nation's economic development, find themselves at the crossroads of technological advancement, global interconnectedness, and an evolving regulatory environment. Against this backdrop, the significance of personal data protection in Ethiopian commercial banks cannot be overstated.

1. ***Confidentiality and Trust:*** Banking relationships are built on a foundation of trust, and the confidentiality of personal data is paramount to maintaining this trust Customers entrust their sensitive information to banks, (Yousafzai et al., 2003) expecting that it will be safeguarded with the utmost care. The assurance of robust personal data protection mechanisms reinforces customer confidence, fostering a trusting relationship between banks and their customers.
2. ***Regulatory Compliance:*** In an era where data protection regulations are becoming increasingly stringent globally, aligning with international standards is not just a best practice but a necessity (*Implementing IT Governance - A Practical Guide to Global Best Practices in ... - Gad J. Selig - Google Books,* n.d.) Compliance with regulations, especially the European Union's General Data Protection Regulation (EU GDPR), not only ensures legal adherence but also facilitates smooth interactions in the global financial ecosystem and potentially enhances the country's reputation for data governance.

3. ***Risk Mitigation:*** The banking sector is an attractive target for cyber threats (Borghard, 2018) and malicious activities aimed at exploiting vulnerabilities in data protection. Robust personal data protection measures act as a formidable line of defense against cyber threats, mitigating the risk of data breaches, financial fraud, and reputational damage.
4. ***Customer Experience and Loyalty:*** Personalized banking services are increasingly dependent on the accurate and secure processing of customer data(Suh & Han, 2003). Effective data protection not only safeguards customer information but also enables banks to offer tailored services, contributing to an enhanced customer experience and fostering customer loyalty.
5. ***Global Competitiveness:*** In a globally connected financial landscape, the ability of Ethiopian commercial banks to compete on an international scale is contingent upon their adherence to global data protection standards. Aligning with EU GDPR, a benchmark in data protection, positions Ethiopian banks as credible and competitive entities in the international market.
6. ***Strategic Preparedness:*** Anticipating and addressing emerging threats to personal data is a strategic imperative (Varisco et al., 2019). As the digital landscape evolves, a proactive approach to data protection ensures that Ethiopian commercial banks are prepared to navigate new challenges and harness opportunities in an era of rapid technological change.

In conclusion, the significance of personal data protection in Ethiopian commercial banks extends far beyond compliance; it is a strategic imperative that encompasses trust, regulatory adherence, risk mitigation, customer experience, global competitiveness, and strategic preparedness. As Ethiopian banks tread the path of progress, the fortification of personal data protection emerges as not only a regulatory necessity but a linchpin for sustainable growth and resilience in an ever-evolving financial landscape.

2.5 Challenges in Data Protection

Data protection faces various challenges, reflecting the dynamic nature of technology, evolving regulatory landscapes, and the increasing sophistication of cyber threats. Here are some of the key challenges in data protection(Aly Bouke et al., n.d.):

2.5.1 Lack of Comprehensive Data Protection Laws

The absence of robust data protection laws can create significant challenges for the effective implementation of the Convention. This lack of legal clarity can lead to uncertainty among businesses and other organizations regarding their data privacy and protection obligations, hindering the Convention's overall effectiveness.

2.5.2 Balancing National Security and Data Privacy

The effective implementation of the Data Privacy Convention hinges on finding the appropriate balance between national security needs and the protection of individual privacy rights. Governments must ensure they have the necessary tools to safeguard national security while fulfilling their obligations under the Convention. This delicate balance is particularly crucial in the context of cross-border data transfers and cooperation between law enforcement and intelligence agencies, where the Convention mandates the establishment of appropriate safeguards to protect individual privacy rights.

2.5.3 Technical and Infrastructural Challenges

In addition to the legal and regulatory challenges there are several technical and infrastructural challenges, some of them are:

i. ***Technology Gap***: Nations with limited access to Information and Communication Technologies (ICT) may face significant challenges in developing and implementing robust data protection frameworks. Furthermore, the digital divide can exacerbate existing social, economic, and political inequalities. Individuals and communities with limited ICT access may be disproportionately vulnerable to data privacy violations, lacking the awareness, resources, and agency to effectively exercise their data protection rights.

ii. ***Cybersecurity Threats:*** Cybersecurity threats, such as data breaches and cyberattacks perpetrated by cybercriminals and state-sponsored actors, have a significant impact on the effective implementation of the Data Privacy Convention. These threats can lead to the unauthorized access, use, or disclosure of personal information, undermining data protection laws and eroding public trust in digital services.

iii. ***Emerging Technologies:*** While emerging technologies like artificial intelligence (AI), the Internet of Things (IoT), and big data analytics hold immense potential, they also present significant challenges to data privacy. AI systems can make decisions about individuals based on their data, raising concerns about fairness and transparency.

Furthermore, IoT devices collect a wide range of sensitive user data, significantly increasing the risk of privacy violations if not adequately protected.

2.5.4 Capacity Building and Awareness Challenges

Despite their critical importance, capacity-building and awareness-raising efforts face significant challenges in the effective implementation of data protection frameworks. These challenges include:

i. ***Resource Constraints for Data Protection Authorities:*** Data protection authorities (DPAs) are essential for ensuring compliance with the Data Privacy Convention. However, limited financial resources, insufficient staff, and inadequate training and expertise significantly constrain the ability of DPAs to effectively carry out their crucial responsibilities.

ii. ***Limited Public Understanding of Data Privacy Rights:*** The successful implementation of the Data Privacy Convention hinges on robust public awareness of data privacy rights. However, many individuals remain unaware of their rights and the importance of protecting their personal information. This lack of awareness can have serious consequences, including underreporting of privacy violations and a weakened public demand for stronger data protection measures.

iii. ***Capacity Building in Data Privacy:*** Effective implementation of the Data Privacy Convention hinges on robust capacity-building initiatives. This requires comprehensive training programs for government officials, legal professionals, law enforcement officers, IT specialists, and other relevant stakeholders on data protection principles, best practices, and the specific requirements of the Convention.

2.6 Related Researches

In conducting this research, the researcher explored various studies related to personal data protection in the banking sector. Several relevant studies were identified, providing valuable insights into different regulatory frameworks and security challenges in banking data protection.

One such study is "Information Security Frameworks for Assisting GDPR Compliance in the Banking Industry" by João Serrado, Ruben Filipe Pereira, Miguel Mira da Silva, and Isaías Scalabrin Bianchi, published on September 19, 2020. This research examines how information security frameworks (ISFs) support banks in complying with the General Data Protection

Regulation (GDPR). Using a design science research approach and semi-structured interviews, the study identifies best practices that align ISFs with GDPR requirements(Serrado et al., 2020). It emphasizes the necessity for industry-specific adaptations in the banking sector, as GDPR provides broad guidelines but lacks detailed implementation strategies for financial institutions. A key finding is that many banks struggle with integrating ISFs into GDPR compliance due to a lack of clarity regarding framework compatibility. Furthermore, the study highlights the shortage of professionals with expertise in both banking regulations and data protection, making compliance more challenging. One of the most significant contributions of this research is the development of an artifact that maps ISFs to GDPR compliance requirements, offering banks a structured approach to align security practices with regulatory mandates. This study bridges the gap between cybersecurity best practices and legal data protection obligations, making it a crucial reference for financial institutions striving to enhance their compliance strategies.

Another relevant study is "Personal Data Security in South Africa's Financial Services Market: The Protection of Personal Information Act 4 of 2013 and the European Union General Data Protection Regulation Compared" by T.V. Warikandwa, published on May 21, 2021(Warikandwa, 2021). This research critically examines the effectiveness of South Africa's Protection of Personal Information Act (POPIA) in safeguarding personal data within the financial sector and compares it with GDPR. The study highlights the growing risks of cybercrime, particularly due to increased digitization and cross-border data flows. While GDPR sets a stringent global standard for data protection, POPIA attempts to align with it but faces limitations, especially in enforcement and extraterritorial applicability. A key concern raised in the study is that South African banks may struggle to meet the data protection standards necessary for seamless global financial interactions. The lack of full harmonization between POPIA and GDPR puts financial institutions at risk of being classified as non-compliant, potentially leading to restrictions on international data transfers. Additionally, many banks prioritize cost reduction over cybersecurity investments, exposing sensitive personal data to security breaches. To address these issues, the study recommends strengthening South Africa's regulatory framework by enforcing stricter compliance monitoring, introducing mandatory data protection impact assessments, and integrating "privacy by design" principles into banking systems. It also emphasizes the importance of collaboration between financial regulators, law enforcement, and cybersecurity experts, as well as increased investment in cybersecurity training and the appointment of dedicated data protection officers in banks.

The third related study is "Protection of Personal Data and Privacy in the Banking Sector in Kosovo and Its Impact on Consumer Protection" by Fitim Gashi and Bedri Peci, published in 2016(Gashi, 2016). This research discusses the evolving legal framework for personal data protection in Kosovo's banking industry and its alignment with European Union regulations such as GDPR. While Kosovo has established the National Agency for Protection of Personal Data, enforcement remains a major challenge. The study reveals that banks process vast amounts of consumer data daily, yet deficiencies in security measures and regulatory compliance expose consumers to risks of data misuse and privacy violations. It also finds that financial institutions often collect more personal data than necessary, increasing the potential for breaches of data protection principles. A critical issue highlighted in the study is the lack of consumer awareness regarding data privacy rights, coupled with inadequate transparency from banks on data processing practices. Additionally, banks frequently use customer data for direct marketing without obtaining clear, informed consent. The research further notes physical privacy concerns in banking branches, where customers discussing financial matters can be overheard, compromising confidentiality. To address these issues, the researcher recommend stricter enforcement of data protection laws in Kosovo, improved alignment with GDPR, and the implementation of "privacy by design" measures in banking operations. The study also stresses the need for greater consumer education on data privacy rights, enhanced cybersecurity strategies, and clearer consent mechanisms to ensure that customer data is handled appropriately.

These related studies collectively provide a comprehensive understanding of personal data protection challenges and regulatory efforts in different financial markets. While GDPR serves as a global benchmark, its implementation varies significantly across regions, highlighting the need for tailored security frameworks, stricter enforcement mechanisms, and improved consumer awareness to enhance data protection in the banking sector.

Chapter Three

Research Methodology

3.1 Introduction

The research methodology serves as the roadmap guiding into Design a comprehensive framework for personal data protection in Ethiopian commercial banks. This chapter delves into the specific methods employed to answer the research questions. Here, the researcher will unveil the strategic approach adopted, the data collection techniques utilized, and the data analysis methods chosen to illuminate the research inquiry.

This chapter is structured to provide a transparent and replicable framework for the research process. The researcher begins by outlining the chosen research approach; mixed methods quantitative and qualitative research approach, and research design justifying its suitability for the research question at hand. Subsequently, after sampling techniques, the data collection methods will be meticulously explained, detailing the instruments or techniques used to gather the data (surveys, interviews, document analysis). The researcher will then delve into the data analysis methods, outlining the specific techniques employed to extract meaning, identify patterns, and draw conclusions from the collected data.

Furthermore, this chapter will address any ethical considerations encountered during the research process. The writer of this paper will discuss the measures taken to ensure data privacy, confidentiality, and informed consent from participants. Finally, the limitations of the chosen methodology and potential areas for future research will be acknowledged, providing a comprehensive perspective on the research endeavour.

3.2 Research Approach

The two paradigm that characterize the research in Information System are behavioural science and design science (Hevner et al., 2004). The behavioural science paradigm is cantered on formulating and evaluating theories that seek to clarify or forecast human or organizational behaviour. On the other hand, the design-science paradigm is focused on expanding the boundaries of human and organizational potential by developing new, innovative solutions and systems. While behavioral science aims to comprehend and predict actions, design science is dedicated to creating practical tools and frameworks that improve performance and tackle real-world issues. Since the objective of this research paper is to design the comprehensive personal

data protection for the commercial banks the researcher selects the design science research approach. Design Science Research (DSR) combines practical relevance and scientific rigor in Information Systems (IS) research. It achieves practical relevance by focusing on the creation of useful artefacts, while maintaining scientific rigor through the formulation and testing of design theories. This dual focus ensures that the research not only addresses real-world challenges but also contributes to the theoretical foundation of the field.(Gutwirth et al., 2011)

The Design Science Research (DSR) approach offers two key perspectives: design artefacts and design theories. The Design Science Research Methodology (DSRM) produces a variety of research outputs, including constructs, models, frameworks, architectures, design principles, methods, instantiations, and design theories. These outputs contribute both to the practical development of solutions and to the theoretical advancement of the field (Baskerville et al., 2018). Design science plays a crucial role in bridging gaps by delivering valuable outputs through design, analysis, reflection, and abstraction. The Design Science Research Methodology (DSRM) contributes new knowledge to the domain by addressing four key dimensions or quadrants: invention, improvement, exaptation, and routine design. These categories encompass the creation of novel solutions (invention), the enhancement of existing systems (improvement), the adaptation of solutions from other domains (exaptation), and the development of standard, repeatable designs (routine design). Each dimension contributes uniquely to advancing both practical applications and theoretical insights (Baskerville et al., 2018).

So as, since there is no developed framework for personal data protection tailored to commercial banks in Ethiopia, this research is categorized as the invention.

The research design provides a crucial framework for a study. The selection of the research approach is a pivotal decision, as it determines how data will be collected. However, it's important to remember that the research design process involves a complex interplay of interrelated decisions.

The Design Science Research (DSR) paradigm originates from the fields of engineering and the sciences of the artificial (Simon 1996). Fundamentally, the Design Science Research (DSR) paradigm is a problem-solving approach. DSR seeks to advance human knowledge by developing innovative solutions to real-world problems, leading to the creation of innovative artifacts and the generation of valuable design knowledge (DK). (Hevner, March, Park, & Ram 2004). A key objective of Design Science Research (DSR) is to extend the boundaries of human

and organizational capabilities through the design and development of innovative artefacts, including constructs, models, methods, and instantiations. (Hevner et al. 2004, Gregor & Hevner 2013). Design Science Research (DSR) focuses on generating design knowledge (DK) – knowledge of how things can and should be constructed or arranged by human agency to achieve desired goals. The following presents a structured plan for conducting DSR research:

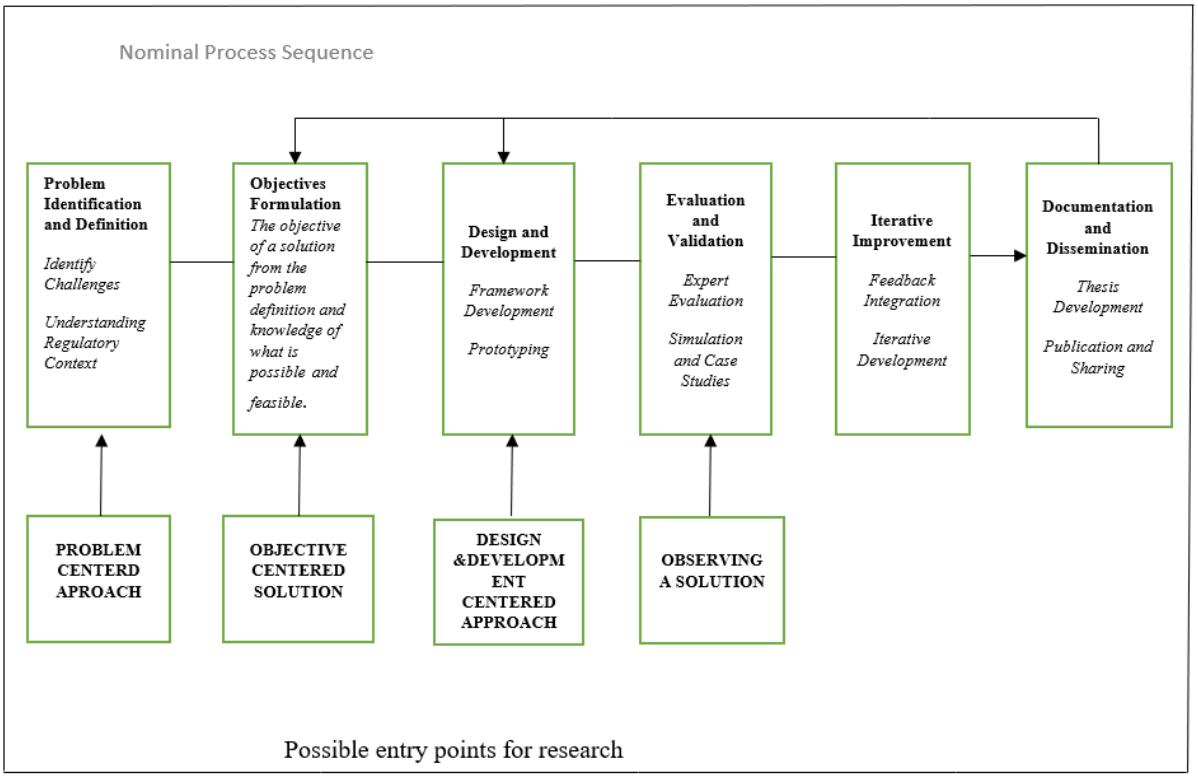

Figure 1- DSR methodology

3.2.1 Problem Identification and Definition

This step is critical for defining the problem and effectively justifying the value of the proposed solution. By substantiating the value, it effectively motivates both the researcher and the research audience to engage with and accept the research findings. This process also provides valuable insights into the researcher's comprehensive understanding of the problem and the rationale underpinning their chosen approach (Uunanen, 2006). Therefor the researched do:

- **Identify Challenges**: Determine the specific challenges faced by Ethiopian commercial banks in aligning with EU GDPR for personal data protection.
- **Understanding Regulatory Context**: Assess the regulatory framework and GDPR requirements for data protection.

3.2.2 Objectives Formulation:

This section focuses on establishing the objective of the solution by thoroughly examining the problem definition and carefully considering the feasibility and practicality of potential solutions. The main goal of this research is to create a comprehensive framework specifically designed for the Ethiopian banking sector, ensuring complete alignment with the principles and requirements of the EU General Data Protection Regulation (GDPR). This framework aims to tackle the distinct challenges that Ethiopian banks encounter in data protection, promoting compliance with international standards and improving their data governance practices.

3.2.3 Design and Development

This study focuses on developing a thorough data protection framework aimed at improving the privacy and security of personal information within the Ethiopian banking industry. The initiative starts with creating a conceptual design that aligns with the fundamental principles of the EU General Data Protection Regulation (GDPR), recognized as a global benchmark for data protection. However, given the distinct challenges and regulatory environment in Ethiopia, this framework will be specifically tailored to address the needs and limitations of the Ethiopian banking sector. By customizing the design to local circumstances, the research seeks to connect international best practices with the practical challenges encountered by Ethiopian banks. Following the conceptual design phase, the intended prototype development was hindered by factors such as resource limitations and lack of management approval for bank testing. Consequently, the researcher presented the draft framework to bank management and technical officers for critique. This procedure undergoes thorough assessment to ensure it not only meets the highest data protection standards but also effectively tackles the specific security and privacy issues faced by Ethiopian banks. The research will examine how well the framework integrates with current banking systems and operations, providing a solution that is both feasible and scalable. Ultimately, the objective is to establish a strong foundation for data protection in Ethiopia's banking sector, promoting trust and adherence to international standards.

3.2.4 Evaluation and Validation

The research will involve a comprehensive approach to gathering expert evaluations from a diverse group of data protection professionals, regulators, and industry specialists. This multifaceted evaluation process is designed to thoroughly assess the suitability and robustness of the developed framework. The insights garnered from these expert opinions will be

invaluable, providing critical perspectives on the framework's effectiveness, its alignment with current industry standards, and its potential to meet the evolving challenges in data protection.

Due to resource and time constraints, and the challenge of securing management approval, the researcher faced limitations in performing prototype testing within Ethiopian commercial banks. To mitigate this, the developed framework was presented to bank management teams to gather their feedback. This feedback was then used to refine the framework, ensuring it aligns with GDPR principles while also being tailored to the specific context of Ethiopian commercial banks. This approach allowed the researcher to compensate for the lack of direct prototype testing in a practical setting by incorporating expert insights and contextual considerations.

Furthermore, the research will focus on determining whether the framework adequately addresses the specific data protection needs of Ethiopian banks, which may differ from those in other regions due to unique regulatory, cultural, and operational contexts. The outcomes of this research are expected to contribute significantly to the field of data protection, offering insights that could lead to enhanced practices and policies within the banking sector in Ethiopia. Ultimately, the goal is to ensure that the developed framework not only meets theoretical standards but also proves to be a practical tool for safeguarding sensitive data in the banking industry.

3.2.5 Iterative Improvement:

The research will incorporate comprehensive feedback from expert evaluations and detailed case studies to meticulously refine and enhance the design and functionality of the proposed framework. By systematically integrating this feedback, the framework will undergo continuous improvement, effectively addressing any identified shortcomings and better aligning with the specific needs and requirements of Ethiopian banks.

An iterative development approach will be employed throughout this process, allowing for necessary adjustments to be made at various stages. This approach is crucial to ensure that the framework not only aligns effectively with the stringent requirements of the General Data Protection Regulation (GDPR) but also adapts to the unique challenges and contextual factors present in the Ethiopian banking environment.

This iterative process is designed to be dynamic and responsive, ensuring that the framework remains both practical and compliant with international data protection standards. By engaging

with stakeholders and incorporating their insights, the framework will evolve to meet the changing landscape of data protection and banking practices in Ethiopia, ultimately fostering a secure and efficient banking system that prioritizes customer privacy and data security.

3.2.6 Documentation and Dissemination:

The research will culminate in the development of a structured thesis, which will serve as a comprehensive documentation of the entire design process, findings, and improvements made throughout the study. This thesis will not only outline the methodologies employed but will also delve into the rationale behind each decision made during the research. It will provide a detailed account of the framework's evolution, highlighting the various stages of development, the challenges encountered, and the solutions implemented to overcome these obstacles.

In addition to documenting the design process, the thesis will include a thorough analysis of the practical applications of the developed framework. This will involve case studies or examples that illustrate how the framework can be applied in real-world scenarios, particularly within the banking sector. The implications of these applications will be discussed, emphasizing their significance in enhancing data protection measures and ensuring compliance with regulatory standards.

Following the completion of the thesis, the outcomes, insights, and the final developed framework will be disseminated through various academic journals and relevant conferences. This dissemination process is crucial for sharing the research findings with the broader academic community and industry professionals. By presenting the research at conferences and publishing in journals, the aim is to contribute to the ongoing discourse on data protection in the banking sector, fostering collaboration and dialogue among researchers, practitioners, and policymakers.

This approach ensures a systematic and iterative process for the development of a data protection framework tailored specifically for Ethiopian commercial banks, aligned meticulously with the stringent standards of the EU GDPR.

3.3 Sampling Techniques

Sample survey techniques were developed as a practical alternative to complete population censuses, which are often impractical, prohibitively costly, or time-consuming. These

techniques utilize scientific knowledge about the population to draw accurate inferences from a representative sample. (Weber & Duarte, 2022). There are different sampling methods that a researcher can use to collect and analyse the data. Mainly sampling techniques are divided in to two main categories; Probability Sampling and Non-Probability Sampling. Under Probability Sampling: simple random, stratified random, cluster Sampling, systematic sampling and multi stage sampling are categorized. Also under non-probability sampling methods there are quota sampling, snowball Sampling, judgement sampling and convenience sampling are there (Taherdoost et al., 2016).

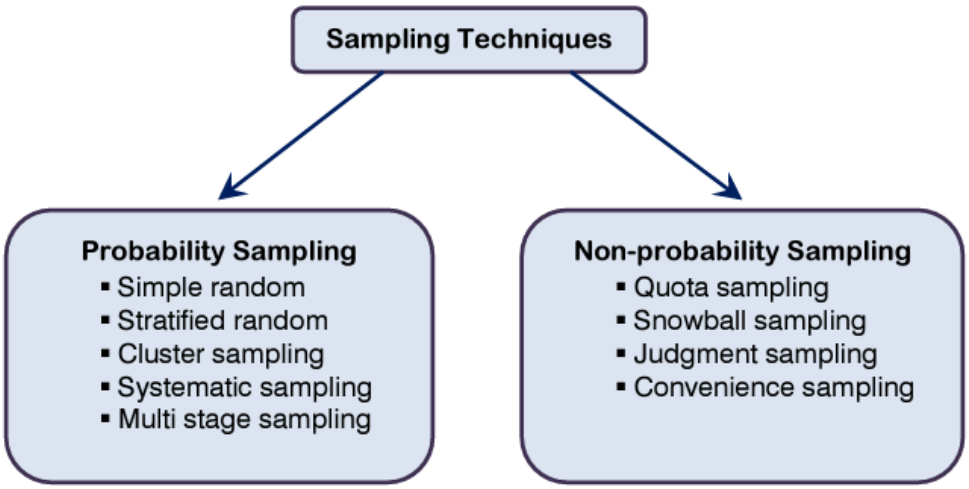

Figure 2- Sampling Techniques

The objective of this thesis is to create a thorough framework for the protection of personal data that can be applied to commercial banks in Ethiopia. To accomplish this, the author identified that Purposive Sampling as the most appropriate sampling technique. The research utilized purposive sampling to achieve a stratified representation of the banking sector. This method facilitated the division of the population into distinct subgroups—large, medium, and small banks—based on customer base. By selecting representative banks from each stratum, the study aimed to capture the nuances and variations within the sector. Specifically, the large bank stratum included the Commercial Bank of Ethiopia, Dashen Bank SC, and Awash Bank SC, chosen for their prominent positions in the market. For the medium-sized banks, Zemen Bank SC and Wogagen Bank SC are included, while Hijira Bank SC is chosen to represent the small banks in the sample. This stratification guarantees that the sample accurately reflects the various segments within the Ethiopian banking industry.

3.4 Data Collection Methods

For the thesis on "Designing a Comprehensive Framework for Personal Data Protection in Ethiopian Commercial Banks: Alignment in EU GDPR," data collection should be systematic and focused on design, development, and validation. Here are data collection methods that the researcher use.

3.4.1 Literature Review:

The research will commence with a comprehensive examination of the current literature concerning personal data protection, compliance with GDPR, and various data protection frameworks. It will involve analyzing studies, reports, and articles pertinent to data security and GDPR. This literature review will aim to pinpoint best practices, challenges, and trends in the global banking sector, with a particular emphasis on how banks are adopting data protection strategies and adhering to GDPR regulations. By integrating this information, the study will establish a robust theoretical basis for creating a customized data protection framework for the banking sector in Ethiopia.

3.4.2 Surveys

The study conducted survey among a group of bank employees to evaluate their understanding of GDPR principles, their experiences with data protection practices, and their views on the potential advantages of the suggested data protection framework. This survey aims to measure the level of comprehension among bank personnel regarding GDPR compliance, pinpoint any knowledge deficiencies, and collect feedback on how the proposed framework could enhance data protection strategies within their organizations. The findings will offer valuable insights into employee perceptions and their preparedness for the rollout of the new framework.

3.4.3 Interviews

The study involves carrying out structured interviews with key figures in Ethiopian commercial banks. These interviews delve into their views on existing data protection practices, their knowledge of GDPR, the obstacles they encounter in implementing data protection strategies, and their aspirations for an optimal data protection framework. By collecting insights from these varied stakeholders, the research seeks to identify the practical needs, gaps, and opportunities for improving data protection in the Ethiopian banking industry.

3.4.4 Content Analysis

The study examines various contexts related to personal data protection within Ethiopia's financial sector. Key among these is the directive issued by the National Bank of Ethiopia, which outlines regulatory requirements for safeguarding personal data in the banking industry. Additionally, the internal policies and procedures adopted by commercial banks to ensure the protection of customer data are reviewed to assess their alignment with national standards and best practices.

Furthermore, the study considers the Critical Mass Cyber Security Requirement Standard, a framework published by the Ethiopian Information Network Security Administration (INSA). This document provides detailed cybersecurity requirements that support the protection of sensitive information, including personal data, across critical infrastructure sectors. Collectively, these contexts form the foundation of Ethiopia's approach to personal data protection in the financial sector and highlight the interplay between regulatory mandates, institutional policies, and national cybersecurity strategies.

3.5 Data Analysis Procedures

Data analysis is the systematic process of collecting and examining statistical information to derive meaningful conclusions (Creswell, J. W. ,2014). This process transforms raw data, such as customer reviews and feedback, into actionable insights that enable managers to make informed decisions and develop effective business strategies and tactics.

The data analysis procedures that the researcher follows are starting from collecting the data using the above-mentioned techniques (Literature Review, Interviews, Surveys and Content Analysis. Then those data that collected cleaned using different data cleaning techniques that check and correct the duplication data, errors and outliers. Those cleaned data are evaluated carefully then create a visualize to reach to conclusion.

3.6 Ethical Considerations

Ethical considerations in research provide a set of guiding principles for researchers. These essential principles include voluntary participation, informed consent, anonymity, confidentiality, assessment of potential harm, and responsible communication of research findings (Gutwirth et al., 2011). In this study, the researcher followed the following basic points while conducting the research:

- The researcher will utilize a recommendation letter from the university as part of the application process
- Voluntary participation: the participants of the research are voluntarily participated.
- Prior to agreeing or declining to participate, individuals must be fully informed about the study's purpose, potential benefits, associated risks, and funding sources.
- No personally identifiable data is collected.
- All research materials utilized in this study are appropriately acknowledged and cited.
- It is important to emphasize that the data collected for this research is strictly for academic purposes.
- The research protocol is designed to minimize all potential risks to participants, including physical, social, and psychological harm, to the greatest extent possible
- The researcher ensure that the work is free of plagiarism or research misconduct, and you accurately represent your results.

Chapter Four

Data Collection and Analysis

4.1 Introduction

The aim of this chapter is to detail the methodology used in gathering and analyzing the data necessary to answer the research questions posed in the study. This section sets the foundation for understanding the processes undertaken to explore the current personal data protection practices within Ethiopian commercial banks. By elaborating on the data collection techniques, survey design, sampling strategies, and analytical methods employed, this chapter serves as a guide for how the study addresses key aspects of personal data protection and its alignment with international standards, particularly the European Union's General Data Protection Regulation (GDPR).

In the context of this research, the primary objective is to assess how commercial banks in Ethiopia handle personal data and to determine the level of compliance with recognized global data protection frameworks. The GDPR, widely considered a benchmark for stringent data protection practices, provides a valuable lens through which to evaluate the current policies and operational procedures in Ethiopian banks. Understanding how well these banks align with such international standards is essential for identifying gaps, proposing improvements, and ensuring customer data is securely managed.

To ensure that comprehensive and reliable insights are obtained, the study adopts a mixed-method approach. This approach combines both **quantitative** and **qualitative** techniques, allowing for a more robust analysis of data protection practices. The quantitative data, collected through surveys, enable a broad understanding of practices across multiple institutions. On the other hand, the qualitative data, gathered through in-depth interviews, provide detailed insights into the challenges, strategic priorities, and contextual factors affecting the implementation of data protection frameworks in Ethiopian banks.

The methodology used in this study is guided by several key considerations:

1. **Relevance to the Research Objectives**: The data collection and analysis methods were chosen to directly address the research questions, ensuring that the data gathered would

be relevant and sufficient to understand the current landscape of data protection in Ethiopian commercial banks.

2. **Rigor and Reliability**: Careful attention was paid to designing the research instruments (e.g., surveys and interview guides) to ensure the accuracy and reliability of the data. The survey instrument was tailored to capture essential elements of data protection, such as access controls, encryption methods, data breach responses, and compliance with legal standards. Interviews provided an additional layer of depth, allowing respondents to share their experiences and perspectives in a nuanced manner.
3. **Comprehensive Coverage of Data Protection Practices**: The study sought to cover a wide range of data protection measures, from technical aspects (such as data encryption and access management) to organizational practices (such as employee training, incident response, and compliance monitoring). By employing both quantitative and qualitative methods, the research provides a well-rounded view of data protection measures at different levels within the banking sector.
4. **Contextual Relevance**: While GDPR is the focal international standard used for comparison, the research also takes into account local challenges and regulatory frameworks in Ethiopia. The study explores how Ethiopian banks are attempting to balance international compliance with local realities, such as resource constraints, infrastructure limitations, and evolving regulatory requirements.

In summary, this chapter provides a comprehensive account of how the research was structured to generate meaningful insights into the state of personal data protection in Ethiopian commercial banks. The methods employed ensure that the study is both thorough and aligned with the research questions, ultimately contributing valuable findings to the ongoing discussions around data protection and privacy in the financial sector.

4.2 Quantitative and Qualitative Data Analysis and Findings

4.2.1 Quantitative Data Analysis

A total of fifty (50) professionals from various Ethiopian commercial banks participated in the survey. Respondents were selected based on their roles in data security-related domains, with the following distribution: Data Management (6 respondents), IT Security (23 respondents), IT Audit (13 respondents), and IT Risk Management (6 respondents). The questionnaire was administered via Google Forms to ensure convenience and accessibility for respondents. The data was then analyzed using the Statistical Package for the Social Sciences (SPSS), a widely

recognized statistical analysis tool. SPSS facilitated detailed exploration of trends, relationships, and patterns within the data, ensuring the findings are both robust and reliable.

Results of Quantitative Data Analysis

Demographic Data

The demographic data of the respondent of the research is shown as below.

I. Job area of the respondent

1. Which department do you work in?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Database Management and Data Analytics	5	10.0	10.0	10.0
	IT Audit	13	26.0	26.0	36.0
	IT/IT Security Department	29	58.0	58.0	94.0
	Risk Management	3	6.0	6.0	100.0
	Total	50	100.0	100.0	

Table 2: Demographic Data

II. Working Experience of the respondent

How many years of experience do you have in your current role?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1–3 years	14	28.0	28.0	28.0
	4–6 years	13	26.0	26.0	54.0
	7–10 years	2	4.0	4.0	58.0
	Less than 1 year	10	20.0	20.0	78.0
	More than 10 years	11	22.0	22.0	100.0
	Total	50	100.0	100.0	

Table 3: Working Experience

Topic 1: Current Practices in Data Protection

To evaluate current practices in data protection, the researcher posed Six targeted questions addressing key aspects of how banks protect their customers' personal data. The findings are summarized as follows:

I. Presence of a Dedicated Data Protection Officer (DPO)

Does your bank currently have a designated Data Protection Officer (DPO)?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	I don't know	13	26.0	26.0	26.0
	No	30	60.0	60.0	86.0
	Yes	7	14.0	14.0	100.0
	Total	50	100.0	100.0	

Table 4: Assigning DPO

Interpretation:

The lack of dedicated DPOs in most banks highlights a significant gap in compliance with global best practices for personal data protection.

III. Effectiveness of Customer Data Protection Mechanisms

The current data protection measures implemented by our bank are robust and effective in safeguarding customer information.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	1	2.0	2.0	2.0
	2	20	40.0	40.0	42.0
	3	15	30.0	30.0	72.0
	4	10	20.0	20.0	92.0
	5	4	8.0	8.0	100.0
	Total	50	100.0	100.0	

Table 5: Effectiveness of Customer Data Protection Mechanisms

- **28%** of respondents believe their bank has effective mechanisms in place to protect customer data.
- However, **72%** disagreed, indicating that the mechanisms in place are insufficient.

Interpretation:

While a majority view the mechanisms as effective, a sizable portion of respondents remains unconvinced, pointing to potential areas for improvement.

IV. Comprehensiveness and Effectiveness of Security Measures

The security measures implemented by our bank to protect customer data are comprehensive and highly effective.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	1	2.0	2.0	2.0
	2	18	36.0	36.0	38.0
	3	18	36.0	36.0	74.0
	4	7	14.0	14.0	88.0
	5	6	12.0	12.0	100.0
	Total	50	100.0	100.0	

Table 6: Comprehensiveness and Effectiveness of Security Measures

- **26%** of respondents agreed that their bank employs comprehensive and effective security measures.
- Conversely, **74%** felt the measures were neither comprehensive nor efficient enough to meet expected standards.

Interpretation:

Although most respondents acknowledge the effectiveness of security measures, a notable minority perceives gaps in comprehensiveness and efficiency.

IV. Consistency in Conducting Security Audits

The bank consistently conducts security audits to ensure the highest standards of data protection are maintained.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	2	13	26.0	26.0	26.0
	3	20	40.0	40.0	66.0
	4	11	22.0	22.0	88.0
	5	6	12.0	12.0	100.0
	Total	50	100.0	100.0	

Table 7: Consistency in Conducting Security Audits

- **34%** of respondents stated that their bank consistently conducts security audits to maintain high standards of data protection.
- However, **66%** disagreed, suggesting inconsistency in audit practices.

Interpretation:

Regular security audits are vital for identifying and addressing vulnerabilities. However, inconsistency in this practice can significantly undermine the effectiveness of overall data protection efforts.

V. Effectiveness of Employee Training on Data Protection

The training provided to employees of our bank on data protection practices is highly effective in equipping them with the necessary skills and knowledge to safeguard sensitive information.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	2	15	30.0	30.0	30.0
	3	23	46.0	46.0	76.0
	4	9	18.0	18.0	94.0
	5	3	6.0	6.0	100.0
	Total	50	100.0	100.0	

Table 8: Effectiveness of Employee Training on Data Protection

- Only **24%** of respondents rated employee training on data protection as highly effective.
- A significant portion of respondents (**76%)** expressed dissatisfaction with the training program, indicating that it failed to effectively equip them with the necessary skills and knowledge. This suggests a critical gap between the intended learning outcomes and the actual training experience.

Interpretation:

The findings highlight a critical need to enhance the effectiveness of training programs to build a robust culture of data protection within banks.

VI. Managing Third-Party Vendors with Access to Customer Data

Our bank effectively manages third-party vendors who have access to customer data, ensuring compliance with stringent data protection standards.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	1	2.0	2.0	2.0
	2	17	34.0	34.0	36.0
	3	15	30.0	30.0	66.0
	4	14	28.0	28.0	94.0
	5	3	6.0	6.0	100.0
	Total	50	100.0	100.0	

Table 9: Managing Third-Party Vendors

- **34%** of respondents believed their bank has an effective strategy to manage third-party vendors with access to customer data.
- The remaining **66%** disagreed, indicating a divide in perceptions.

Interpretation:

Managing third-party risks is a critical component of data protection. A 34-64 split in perceptions underscores the need for banks to review and strengthen vendor management policies.

Summary

The analysis reveals mixed perceptions of data protection practices within Ethiopian banks. While some areas, such as security measures and audit practices, demonstrate positive trends like the absence of DPOs, employee training, and vendor management, indicate significant gaps that require attention. These findings serve as a foundation for identifying areas where banks can improve their compliance with data protection standards and enhance overall customer data security.

Topic 2: Key Components of a Data Protection Framework

The second section of the questionnaire focused on evaluating the key components that should be included in a customer data protection framework. Five major areas were assessed, capturing the perspectives and recommendations of IT staff to inform the development of an effective framework. The results are summarized as follows:

I. Regular Data Encryption

Regular data encryption is vital for protecting customer data, as it plays a key role in ensuring confidentiality and preventing unauthorized access to sensitive information.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	2	2	4.0	4.0	4.0
	3	2	4.0	4.0	8.0
	4	14	28.0	28.0	36.0
	5	32	64.0	64.0	100.0
	Total	50	100.0	100.0	

Table 10: Regular Data Encryption

- **92%** of respondents agreed that regular data encryption is vital for protecting customer data. They highlighted its importance in maintaining confidentiality and preventing unauthorized access to sensitive information.
- **8%** of respondents disagreed, suggesting alternative priorities or approaches.

Interpretation:

Encryption is overwhelmingly recognized as a cornerstone of data protection, underscoring its role in safeguarding sensitive data.

II. Having a Dedicated Data Protection Officer (DPO)

Having a dedicated Data Protection Officer (DPO) at our bank is essential for ensuring effective data protection, as it establishes accountability and fosters a culture of compliance with data privacy regulations.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	2	1	2.0	2.0	2.0
	3	7	14.0	14.0	16.0
	4	12	24.0	24.0	40.0
	5	30	60.0	60.0	100.0
	Total	50	100.0	100.0	

Table 11: Having a Dedicated Data Protection Officer (DPO)

- **82%** of participants believed that assigning a dedicated Data Protection Officer (DPO) is essential for effective data protection. Respondents noted that a DPO enhances accountability and fosters a culture of compliance with data privacy regulations.
- **18%** disagreed, indicating that some may view a DPO as less critical or believe existing roles can fulfill the responsibilities.

Interpretation:

While most agree on the necessity of a DPO, the dissent highlights the need to clarify the DPO's value in ensuring compliance and leadership in data protection efforts.

III. Access Control and User Authentication

Access control measures, such as user authentication, are critical components of our bank's data protection framework, as they safeguard sensitive information by ensuring that only authorized personnel can access it.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	3	1	2.0	2.0	2.0
	4	13	26.0	26.0	28.0
	5	36	72.0	72.0	100.0
	Total	50	100.0	100.0	

Table 12: Access Control and User Authentication

- **98%** of respondents agreed that access control measures, such as user authentication, are critical for a bank's data protection framework. These measures are designed to rigorously restrict access to sensitive information to only authorized personnel.
- **2%** disagreed, suggesting alternative approaches or a perceived adequacy of existing practices.

Interpretation:

The near-unanimous agreement highlights the universal importance of robust access control and authentication mechanisms in securing customer data.

IV. Regular Staff Training

Regular staff training is crucial for ensuring compliance with data protection policies, as it empowers employees with the knowledge and skills necessary to uphold privacy standards and effectively protect sensitive information.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	2	1	2.0	2.0	2.0
	3	2	4.0	4.0	6.0
	4	9	18.0	18.0	24.0
	5	38	76.0	76.0	100.0
	Total	50	100.0	100.0	

Table 13: Regular Staff Training

- **94%** of respondents agreed that regular staff training is crucial for ensuring compliance with data protection policies. They emphasized the role of training in empowering employees with the knowledge and skills necessary to uphold privacy standards and protect sensitive data effectively.

- **6%** disagreed, possibly reflecting doubts about the effectiveness or implementation of current training programs.

Interpretation:

This finding underscores the need for consistent and well-structured training programs to cultivate a culture of data protection awareness and capability among employees.

V. Regular Monitoring and Audits

Regular monitoring and audits are highly significant for maintaining data protection standards, as they provide ongoing assessments of our security measures and ensure compliance with established protocols.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	3	1	2.0	2.0	2.0
	4	16	32.0	32.0	34.0
	5	33	66.0	66.0	100.0
	Total	50	100.0	100.0	

Table 14: Regular Monitoring and Audits

- **98%** of respondents agreed that regular monitoring and audits are essential for maintaining data protection standards. These practices were seen as crucial for ongoing assessments of security measures and ensuring compliance with established protocols.
- **2%** disagreed, which might stem from a perception that existing monitoring measures are sufficient or concerns about resource allocation.

Interpretation:

The strong agreement reflects the critical role of audits and monitoring in sustaining data protection efforts and ensuring adherence to standards over time.

Summary

The analysis of this topic reveals broad consensus among IT staff on the key components of a robust data protection framework. Regular data encryption, staff training, access control, monitoring, and the presence of a dedicated DPO emerged as the most significant elements. These insights provide valuable guidance for designing a comprehensive data protection framework tailored to the banking sector. However, areas of disagreement highlight the need for further discussion and clarification to address concerns and align perspectives.

Topic 3: Implementation of the Framework

The third section of the study focuses on evaluating the readiness and capability of banks to implement a personal data protection framework aligned with international standards, particularly the EU-GDPR. Five key aspects related to implementation were assessed, and the findings are summarized below:

I. Adaptability and Readiness to Implement a Comprehensive Data Protection Framework

Our bank is highly adaptable and ready to implement a comprehensive data protection framework, enabling us to respond effectively to evolving regulatory requirements and industry best practices.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	2	1	2.0	2.0	2.0
	3	11	22.0	22.0	24.0
	4	23	46.0	46.0	70.0
	5	15	30.0	30.0	100.0
	Total	50	100.0	100.0	

Table 15: Adaptability and Readiness

- **76%** of respondents stated that their bank is highly adaptable and ready to implement a comprehensive data protection framework, enabling the institution to respond effectively to evolving regulatory requirements and industry best practices.
- **24%** disagreed, indicating that their bank is not yet prepared to adopt such a framework.

Interpretation:

The high adaptability rate demonstrates promising readiness among most banks to adopt advanced data protection frameworks, although some institutions may require additional preparation or support.

II. Management Commitment

Our bank's management is fully committed to implementing robust data protection practices, prioritizing the safeguarding of sensitive information and fostering a culture of privacy throughout the organization.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	2	2	4.0	4.0	4.0
	3	8	16.0	16.0	20.0
	4	26	52.0	52.0	72.0
	5	14	28.0	28.0	100.0

	Total	50	100.0	100.0	

Table 16: Management Commitment

- **80%** of respondents agreed that their bank's management is fully committed to implementing robust data protection practices. They noted that management prioritizes safeguarding sensitive information and fostering a culture of privacy within the organization.
- **20%** felt that their bank's management lacks sufficient commitment to implementing the framework, citing various reasons for this lack of prioritization.

Interpretation:

Strong management commitment is critical to successful framework implementation. While the majority agree on this point, the notable minority indicates potential barriers that need to be addressed at the leadership level.

III. Employees' Adherence to Data Protection Protocols

Our bank's employees are highly likely to adhere to data protection protocols when equipped with comprehensive training and the necessary resources, ensuring a strong commitment to safeguarding sensitive information.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	2	4	8.0	8.0	8.0
	3	8	16.0	16.0	24.0
	4	23	46.0	46.0	70.0
	5	15	30.0	30.0	100.0
	Total	50	100.0	100.0	

Table 17: Employees' Adherence

- **76%** of respondents believed that employees are likely to adhere to data protection protocols when provided with comprehensive training and adequate resources, ensuring effective safeguarding of sensitive data.
- **24%** disagreed, emphasizing the need for stricter rules, enhanced training, and additional resources to ensure adherence.

Interpretation:

The findings highlight the importance of employee training and resources in building a robust data protection culture. The minority response signals that gaps in employee compliance could undermine implementation efforts.

IV. Role of Regulatory Guidelines from Authorities

Regulatory guidelines from authorities, such as the National Bank of Ethiopia, play a crucial role in effectively supporting the implementation of data protection measures, providing a robust framework for compliance and best practices

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	2	2	4.0	4.0	4.0
	3	3	6.0	6.0	10.0
	4	15	30.0	30.0	40.0
	5	30	60.0	60.0	100.0
	Total	50	100.0	100.0	

Table 18: Role of Regulatory Guidelines from Authorities

- **90%** of respondents agreed that regulatory guidelines from authorities, such as the National Bank of Ethiopia, are crucial for supporting the implementation of data protection measures. These guidelines provide a robust framework for compliance and best practices.
- **10%** disagreed, indicating skepticism about the role or adequacy of regulatory guidance in facilitating effective implementation.

Interpretation:

The overwhelming agreement underscores the importance of a strong regulatory framework in guiding banks toward effective data protection practices. Addressing concerns from the minority could further enhance regulatory impact.

V. Preparation and Commitment to Aligning with International Data Protection Standards

Our bank is fully prepared and committed to aligning with international data protection standards, such as the GDPR, demonstrating a proactive approach to safeguarding customer information and ensuring compliance with global best practices

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	1	2.0	2.0	2.0
	2	1	2.0	2.0	4.0
	3	15	30.0	30.0	34.0
	4	20	40.0	40.0	74.0
	5	13	26.0	26.0	100.0
	Total	50	100.0	100.0	

Table 19: Preparation and Commitment to Aligning with International Data Protection Standards

- **66%** of respondents indicated that their bank is prepared and committed to aligning with international data protection standards, such as the GDPR, showcasing a proactive approach to safeguarding customer information and ensuring compliance with global best practices.
- **34%** disagreed, suggesting that significant work remains to fully align banks with international standards.

Interpretation:
While most banks demonstrate commitment to international alignment, the sizable minority reflects areas where additional focus is needed, particularly in aligning policies, resources, and practices with global standards.

Summary

The findings highlight overall readiness and enthusiasm among banks to implement a comprehensive data protection framework aligned with the EU-GDPR. Strong adaptability, management commitment, and reliance on regulatory guidelines are promising indicators. However, gaps in employee adherence, varying levels of management commitment, and challenges in meeting international standards point to areas where further efforts are required to ensure seamless and effective implementation.

Open-Ended Question Analysis

The researcher conducted open-ended questions to gather in-depth insights from participants on key aspects of personal data protection. The responses provided valuable qualitative data, summarized as follows:

I. Data Breach Incidents

When asked about the response to data breaches or incidents, most participants described a consistent approach based on the bank's incident response procedures. Common steps included:

- Containment of the breach to minimize impact.
- Eradication of the threat to restore system integrity.
- Investigation to determine the cause and scope of the breach.

- Reporting the incident to regulatory offices, such as those designated for monitoring compliance.

KeyInsight:
A structured incident response protocol is widely adopted, but the responses suggest that reporting to regulatory bodies is a critical area requiring proper execution and accountability.

II. Additional Recommendations for Implementing the Framework

Participants suggested several key areas of focus for the successful implementation of a comprehensive data protection framework:

- **Data Classification and Encryption:** Categorizing and protecting data based on its sensitivity.
- **Monitoring and Risk Assessment:** Proactively identifying and mitigating vulnerabilities.
- **Policy Development:** Establishing and enforcing data protection policies.
- **Employee Training and Awareness:** Regular and comprehensive training programs to equip staff with knowledge on data protection practices.
- **Compliance:** Aligning with both local regulations and international standards, such as the GDPR.

KeyInsight:
Participants emphasized a multi-faceted approach to implementation, highlighting technical, procedural, and educational components as critical to the framework's success.

III. Roles and Responsibilities of the Regulatory Body

Most participants agreed on the crucial role of the National Bank of Ethiopia in personal data protection. Specific responsibilities included:

- **Creating and Enforcing Regulations:** Developing clear and enforceable data protection guidelines.
- **Monitoring and Auditing:** Regularly reviewing banks' data protection practices to ensure compliance.

KeyInsight:

Participants stressed that a strong regulatory presence is essential for driving compliance and maintaining a high standard of data protection across the banking sector.

IV. Required Resources for Implementing the Framework

Participants identified critical resources needed for implementing a robust data protection framework:

- **Financial Resources:** Adequate budgeting to acquire and implement advanced security tools like Data Loss Prevention (DLP) systems, database activity monitoring tools, and fraud management systems.
- **Technological Resources:** Deployment of advanced tools and systems to secure data at rest and in motion.
- **Human Resources:** Emphasis on the human aspect, with mandatory training for employees on:
    - Data protection regulations.
    - Types of attacks and potential threats.
    - Consequences of data breaches.

KeyInsight:
Participants highlighted that robust financial support, cutting-edge technologies, and a well-trained workforce are foundational for successful implementation.

Summary

The qualitative responses revealed a comprehensive understanding of data protection requirements among participants. They provided clear recommendations on improving incident response, implementing frameworks, defining regulatory roles, and allocating necessary resources. These insights underline the significance of co-operation between banks, regulatory bodies, and bank's staffs to achieve a secure and effective data protection environment.

4.2.2 Qualitative Data Analysis

As discusses in Chapter Three, the research also employed a qualitative approach to collect and analyze the bank's current personal data protection mechanisms. Through interviews with the researcher conducted interviews with key figures from the banking sector: Director of Cyber Security at Dashen Bank, the Director of Cyber Security at Zemen Bank, and the Senior

Manager of Cyber Audit at Commercial Bank of Ethiopia, as well as the Director of Bank Inspection at the National Bank of Ethiopia., the study aimed to identify gaps, recommend improvements, and assess the bank's readiness to adopt a comprehensive data protection framework. Thirteen interview categories, each with one or two questions, were used to guide the data collection process.

I. Data Protection Officer (DPO)

Under the EU GDPR, one of the key requirements is the appointment of a Data Protection Officer (DPO) within organizations that handle significant volumes of personal data. Given that banks routinely collect and process extensive personal data from their customers, the role of the DPO becomes particularly critical.

- On the importance of the Data Protection Officer: the experts emphasize that "*The urgent need for a Data Protection Officer (DPO) at the bank cannot be overstated. With the bank's extensive handling of sensitive customer information, a DPO is essential to safeguard personal data and ensure regulatory compliance. It is imperative that the bank addresses the factors hindering the appointment of a DPO and takes immediate steps to fill this critical role."*
- On challenges acquire the DPO: the expert emphasized that "…*The bank has proactively developed and approved a data protection policy, even before the country's personal data protection regulation was enacted. While the bank has initiatives personal data protection, these are still in the early stages of implementation. The appointment of a Data Protection Officer (DPO) is one of the key tasks the bank plans to undertake in the coming years...*"
- Regarding the primary responsibilities of a Data Protection Officer within your bank: *"…The DPO will be responsible for overseeing the implementation of the data protection policy, ensuring its ongoing relevance by updating it to reflect current and future regulatory requirements. Additionally, the DPO will play a crucial role in enhancing employee awareness through capacity-building initiatives. The DPO will also be responsible for monitoring and ensuring compliance with both international and national data protection regulations*"

Extracted information from the interview's transcription	**Codes (subthemes) that were taken out of the data transcription**	**Main Theme**

The urgent need for a Data Protection Officer (DPO) at the bank cannot be overstated. With the bank's extensive handling of sensitive customer information, a DPO is essential to safeguard personal data and ensure regulatory compliance. It is imperative that the bank addresses the factors hindering the appointment of a DPO and takes immediate steps to fill this critical role.	DPO is essential to safeguard personal data and ensure regulatory compliance.	**Use of DPO**
The bank has proactively developed and approved a data protection policy, even before the country's personal data protection regulation was enacted. While the bank has initiatives on personal data protection, these are still in the early stages of implementation. The appointment of a Data Protection Officer (DPO) is one of the key tasks the bank plans to undertake in the coming years...	personal data protection…., is still in the early stages of implementation	
The DPO will be responsible for overseeing the implementation of the data protection policy, ensuring its ongoing relevance by updating it to reflect current and future regulatory requirements. Additionally, the DPO will play a crucial role in enhancing employee awareness through capacity-building initiatives. The DPO will also be responsible for monitoring and ensuring compliance with both international and national data protection regulations	Enforcing and update policy, monitoring regulation and capacity building,	

Table 20: DPO requirement

II. *Effectiveness of Customer Data Protection Mechanisms*

It is evident that banks are taking steps to protect critical data, including customers' personal information. However, based on my observations, there is a need to enhance these protections

further to align with both international and national compliance requirements, such as the EU GDPR.

- Regarding significant weakness: "…*the bank has developed clear and concise policies that address personal data protection and general information security. Furthermore, there are several complementary guidelines that reinforce these policies. Nevertheless, the bank faces challenges in effectively communicating these policies to end-users, raising employee awareness about data protection, and integrating data protection considerations into business requirements…"*

- Essential point to improve the effectiveness: "*…to strengthen its data protection posture, the bank should undertake comprehensive employee training to enhance understanding of data protection policies. Strict enforcement of these policies, including disciplinary measures for violations, is crucial. The bank should also invest in advanced security technologies, such as Data Loss Prevention (DLP), email security gateways, and anti-fraud systems. Furthermore, regular reviews of user access privileges should be conducted to ensure that they remain appropriate and necessary for business operations..."*

Extracted information from the interview's transcription	**Codes (subthemes) that were taken out of the data transcription**	**Main Theme**
The bank has developed clear and concise policies that address personal data protection and general information security. Furthermore, there are several complementary guidelines that reinforce these policies. Nevertheless, the bank faces challenges in effectively communicating these policies to end-users, raising employee awareness about data protection, and integrating data protection considerations into business requirements.	in effectively communicating these policies to end-users and considerations into business requirements	**Effectiveness of Customer Data Protection**

To strengthen its data protection posture, the bank should undertake comprehensive employee training to enhance understanding of data protection policies. Strict enforcement of these policies, including disciplinary measures for violations, is crucial. The bank should also invest in advanced security technologies, such as Data Loss Prevention (DLP), email security gateways, and anti-fraud systems. Furthermore, regular reviews of user access privileges should be conducted to ensure that they remain appropriate and necessary for business operations	comprehensive employee training, enforcement of these policies, disciplinary measures for violations, invest in advanced security technologies and reviews of user access privileges	

Table 21: Effectiveness of Customer Data Protection Mechanisms

I. Security Audits

Given that the bank complies with standards such as PCI DSS, ISO 27001, SWIFT, and other internal and external compliance audits, it is clear that personal data protection is already a critical checkpoint in these frameworks. However, to fully implement GDPR and meet the expectations of working with international financial organizations like Mastercard—especially given that European citizens are among the bank's customers—it is essential to align more closely with GDPR requirements.

- Additional Steps to comply on GDPR: "…*The bank has adopted and is compliant with PCI DSS for safeguarding cardholder data and ISO 27001:2022 for overall information security. While these standards include measures to protect PII, the bank can further enhance its data protection efforts by extending its ISO 27001 compliance to encompass personal data protection, specifically by implementing ISO/IEC 27001 and ISO/IEC 27002 standards."*

Extracted information from the interview's transcription	**Codes (subthemes) that were taken out of the data transcription**	**Main Theme**

The bank has adopted and is compliant with PCI DSS for safeguarding cardholder data and ISO 27001:2022 for overall information security. While these standards include measures to protect PII, the bank can further enhance its data protection efforts by extending its ISO 27001 compliance to encompass personal data protection, specifically by implementing ISO/IEC 27001 and ISO/IEC 27002 standards.	Enhance its data protection efforts by extending its ISO 27001 by ISO/IEC 27001 and ISO/IEC 27002	**Enhance the personal data protection.**

Table 22: Security Audit

II. Employee Training and Awareness

The general cyber security awareness training is conducted through various methods, including face-to-face sessions lasting half a day, as well as digital formats like email campaigns and desktop background reminders. However, based on the responses from the questionnaire, a significant number of participants indicated that the training is not effective when it comes to addressing personal data protection specifically.

Reason on ineffective of training: "…*although management briefings and employee portal announcements have been implemented to raise awareness about personal data protection, these initiatives have not been adequate. The training content has not sufficiently covered the nuances of personal data protection, and the delivery method, relying solely on text-based materials without engaging visuals like infographics and real-world scenarios, has limited its effectiveness. Additionally, the brevity of the training sessions has hindered comprehensive knowledge transfer…*"

Suggestion to better equip employees with GDPR-compliant data protection knowledge and practices: *"…To cultivate a robust data protection culture, the bank should revamp its training approach by incorporating engaging elements like infographics, short videos, role-specific training sessions, and interactive workshops. Utilizing a Learning Management System (LMS) to deliver training and implementing quizzes and exams can facilitate effective knowledge transfer and skill development. Moreover, integrating the results of these assessments into*

employee performance evaluations will incentivize active participation and continuous learning…"

Extracted information from the interview's transcription	Codes (subthemes) that were taken out of the data transcription	Main Theme
Although management briefings and employee portal announcements have been implemented to raise awareness about personal data protection, these initiatives have not been adequate. The training content has not sufficiently covered the nuances of personal data protection, and the delivery method, relying solely on text-based materials without engaging visuals like infographics and real-world scenarios, has limited its effectiveness. Additionally, the shortness of the training sessions has hindered comprehensive knowledge transfer.	The training content has not sufficiently; delivery method, relying solely on text-based, the shortness of the training.	**Awareness creation ineffective and recommendation to be more efficient**
To cultivate a robust data protection culture, the bank should revamp its training approach by incorporating engaging elements like infographics, short videos, role-specific training sessions, and interactive workshops. Utilizing a Learning Management System (LMS) to deliver training and implementing quizzes and exams can facilitate effective knowledge transfer and skill development. Moreover, integrating the results of these assessments into employee performance evaluations will incentivize active participation and continuous learning	incorporating infographics, short videos, role-specific training sessions, and interactive workshops, utilizing a Learning Management System (LMS) to deliver training and implementing quizzes and exams	

Table 23: Employee Training and Awareness

III. Third-Party Vendor Management

The bank collaborates with third-party vendors on various applications and systems, which requires stringent oversight to ensure compliance with data protection standards.

- Third-party vendor's adherence to data protection standards: *"...the bank considers adherence to industry standards, such as PCI DSS, as a plus for selection criterion when partnering with third-party vendors. Given that most vendors are located in Africa or the Middle East, compliance with EU GDPR is not currently a primary consideration…"*
- Improve the current vendor management practices*: "…in the future, as the bank and the country advance in their understanding and implementation of data protection regulations, adherence to EU GDPR will be a crucial consideration when selecting third-party vendors…"*

Extracted information from the interview's transcription	**Codes (subthemes) that were taken out of the data transcription**	**Main Theme**
The bank considers adherence to industry standards, such as PCI DSS, as a plus for selection criterion when partnering with third-party vendors. Given that most vendors are located in Africa or the Middle East, compliance with EU GDPR is not currently a primary consideration.	EU GDPR is not currently a primary consideration for vendor selection.	**Adherence of third party vendors on GDPR regulations**
In the future, as the bank and the country advance in their understanding and implementation of data protection regulations, adherence to EU GDPR will be a crucial consideration when selecting third-party vendors	In future EU GDPR will be a crucial consideration when selecting third-party vendors	

Table 24: Third Party Vendor Management

IV. Regulatory Guidelines and Support

The regulatory oversight and support provided by the National Bank of Ethiopia are essential for commercial banks in Ethiopia to implement robust personal data protection measures that safeguard customer information and comply with relevant regulations.

- Provides adequate guidance and monitoring from NBE: "… *Although the NBE has issued directives named "Financial consumer protection directive FCP/01/2020" emphasizing the importance of protecting customer data, specific and detailed guidelines are yet to be provided by the regulatory body*…."

- Oversight from regulatory bodies like the NBE: "…*the regulatory body is expected to issue clear, comprehensive guidelines on data protection and conduct audits to ensure compliance by banks..."*

Extracted information from the interview's transcription	**Codes (subthemes) that were taken out of the data transcription**	**Main Theme**
Although the NBE has issued directives emphasizing the importance of protecting customer data, specific and detailed guidelines are yet to be provided by the regulatory body	Specific and detailed guidelines are yet to be provided by the regulatory body	**Regulatory body guide and support**
The regulatory body is expected to issue clear, comprehensive guidelines on data protection and conduct audits to ensure compliance by banks	clear, comprehensive guidelines on data protection is expected	

Table 25: Regulatory Guidelines and Support

V. Data Breach Preparedness

The bank has an established incident response plan designed to address potential cyber incidents. However, in the context of data breaches, it is crucial to ensure that the plan is both comprehensive and effective.

- need improvement in current I&R: "*...the bank has established an incident response plan outlining procedures for reporting and responding to incidents. However, the bank's incident response capabilities could be further enhanced through regular simulations involving senior management to test the plan's effectiveness in real-world scenarios*."
- recommend incorporating to strengthen the I&R: "*...to ensure the effectiveness of the incident response plan, it is crucial to update the contact and escalation matrix regularly to reflect changes in personnel. Additionally, the bank should*

conduct regular exercises to test the plan's implementation and identify areas for improvement…"

Extracted information from the interview's transcription	Codes (subthemes) that were taken out of the data transcription	Main Theme
The bank has established an incident response plan outlining procedures for reporting and responding to incidents. However, the bank's incident response capabilities could be further enhanced through regular simulations involving senior management to test the plan's effectiveness in real-world scenarios	Regular simulations involving senior management to test the plan's	**I&R plan weakness and enhancement**
To ensure the effectiveness of the incident response plan, it is crucial to update the contact and escalation matrix regularly to reflect changes in personnel. Additionally, the bank should conduct regular exercises to test the plan's implementation and identify areas for improvement	update the contact and escalation matrix regularly and conduct regular exercises to test the plan's	

Table 26: Data Breach Readiness

VI. Budget and Resource Allocation

Implementing and maintaining compliance with comprehensive regulations like the GDPR requires substantial financial investment. Without adequate allocation of resources, achieving full compliance becomes a significant challenge for the bank.

- budgetary constraints and you prioritize resource allocation: *"…the bank's management has shown a willingness to allocate budget for IT security initiatives. However, securing budget approval often depends on middle management's ability to articulate the business value and necessity of specific systems…"*

Extracted information from the interview's transcription	Codes (subthemes) that were taken out of the data transcription	Main Theme

The bank's management has shown a willingness to allocate budget for IT security initiatives. However, securing budget approval often depends on middle management's ability to articulate the business value and necessity of specific systems	Management is willing for budget if the system has business value	**Budget allocation**

Table 27: Budjet and Resource Allocation

VII. Alignment with International Standards

Based on my observations of the bank's personal data protection practices, there are certain areas where the bank may fall short of complying with regulations. For example, the bank currently collects sensitive personal data such as customers' mother's name, monthly and annual income, source of income, and, in some cases, biometric data as part of the digital On-Boarding system. This collection of data may not align with the principle of purpose limitation, which limits the use of personal data to only the specific purposes for which it was collected.

- challenges on data protection framework with international standards: "…*the bank's data collection practices are focused on essential information required for banking services. Sensitive personal information, such as religious beliefs, political affiliations, or sexual orientation, is not collected. The central regulatory body mandates the collection of certain basic information, including mother's name, income source, and income value. While biometric data is not routinely collected, it is permissible under banking laws for customers who lack valid identification documents.*"

Extracted information from the interview's transcription	**Codes (subthemes) that were taken out of the data transcription**	**Main Theme**
The bank's data collection practices are focused on essential information required for banking services. Sensitive personal information, such as religious beliefs, political affiliations, or sexual orientation, is not collected. The central regulatory body mandates the collection of certain basic	Data collection focused on essential information required for banking services and sensitive personal information, is not collected	**Sensitive data collection.**

information, including mother's name, income source, and income value. While biometric data is not routinely collected, it is permissible under banking laws for customers who lack valid identification documents."		

Table 28: Alignment with International Standards

VIII. Policy Development and Implementation

Personal data protection policy is one of the mandatory for implementation and the protection and meet international standard.

- Crafting Data protection policy: "*...the bank currently has two distinct policies: an information security policy and a personal data protection policy. While the personal data protection policy has been endorsed and approved by the CEO and board of directors, a holistic framework that integrates both policies and provides clear procedures and guidelines for data protection practices is not developed yet…"*

Extracted information from the interview's transcription	Codes (subthemes) that were taken out of the data transcription	Main Theme
The bank currently has two distinct policies: an information security policy and a personal data protection policy. While the personal data protection policy has been endorsed and approved by the CEO and board of directors, a holistic framework that integrates both policies and provides clear procedures and guidelines for data protection practices is not developed yet	Policy is crafted but there is no clear guide line and procedure.	**Data protection policy, procedure and guideline**

Table 29: Policy Development and Implementation

IX. Employee Adherence to Protocols

Employees of the bank are expected to adhere to the policies and protocols that have been published and disseminated by the bank. However, it is evident that some employees do not fully comply with these data protection policies. As we know, if customer personal data is

breached, it can have disastrous consequences for the bank, including loss of reputation and trust.

- Employees adherence to policy and create stronger culture of compliance: "*...raising employee awareness of data protection policies and the potential consequences of non-compliance is crucial. The bank should implement strict monitoring procedures to detect policy violations and take appropriate administrative actions against offenders. Sharing information about these incidents across the organization can serve as a deterrent and reinforce the importance of adhering to data protection policies…"*

Extracted information from the interview's transcription	**Codes (subthemes) that were taken out of the data transcription**	**Main Theme**
Raising employee awareness of data protection policies and the potential consequences of non-compliance is crucial. The bank should implement strict monitoring procedures to detect policy violations and take appropriate administrative actions against offenders. Sharing information about these incidents across the organization can serve as a deterrent and reinforce the importance of adhering to data protection policies	Raising employee awareness and implement strict monitoring procedure	**Policy awareness and monitoring**

Table 30: Employee adherence to Protocol

X. Data Encryption and Access Controls

The bank employs various encryption methods and access controls to protect sensitive data stored in different databases (data at rest), as well as SSL encryption to safeguard data in transit (data in motion).

Improvements on data encryption: *"… while the bank is currently encrypting cardholder data, personal data encryption is still pending. To mature our data protection practices, we need to align business requirements with regulations, policies, and international standards…"*

Extracted information from the interview's transcription	Codes (subthemes) that were taken out of the data transcription	Main Theme
While the bank is currently encrypting cardholder data, personal data encryption is still pending. To mature our data protection practices, we need to align business requirements with regulations, policies, and international standards	personal data encryption is still pending	**Personal data encryption.**

Table 31: Data Encryption and Access Control

During an interview with the Director of Consumer Protection and Education at the National Bank of Ethiopia, the researcher gathered valuable insights into the regulatory landscape pertaining to consumer protection.

XI. Current regulation related to personal data protection

As the regulatory authority for commercial banks in Ethiopia, the National Bank of Ethiopia (NBE) plays a crucial role in issuing directives that align with the evolving regulatory landscape. Given the increasing importance of data protection, the NBE is expected to develop a dedicated personal data protection regulation. During an interview with the Director of Consumer Protection and Education at the NBE, it was revealed that "…..*while the NBE previously issued a consumer protection regulation that included some general data protection principles, a dedicated and comprehensive personal data protection regulation is still forthcoming….. the NBE is currently planning to either update existing directives or issue a separate, dedicated directive specifically addressing personal data protection….*"

XII. Challenges of the bank on personal data protection

Instances of personal data loss within the banking sector indicate significant challenges in effectively protecting customer data. During an interview, the Director of at NBE acknowledged these challenges, "……*inadequate implementation of data protection measures, including insufficient deployment of data loss prevention tools, weak email security, and inadequate data encryption are the major challenges of the bank. Also deficiencies in administrative controls, such as the lack of comprehensive data protection policies and procedures, ineffective access controls, and inadequate measures to address internal threats are the main challenges….."*

XIII. National Bank of Ethiopian monitoring and Evaluation

As the regulatory authority, the National Bank of Ethiopia (NBE) is responsible for overseeing the compliance of commercial banks with relevant regulations. The NBE has the authority to impose penalties on banks that fail to comply with data protection regulations. During discussions with the Director of Consumer Protection and Education at the NBE, it was emphasized that in cases of non-compliance, "*....the NBE would not only impose financial penalties but also actively support customers in pursuing legal recourse…. if a customer initiates legal action against a bank for data protection violations, the NBE would support the customer's claims in court….*"

XIV. Recommendation for the banks to address the compliance issue

To enhance data protection compliance, the researcher engaged with the Director of Information Security to gather their insights and recommendations. He says *"....to enhance data protection, banks must amend their data protection processes and governance frameworks. This includes appointing a dedicated Data Protection Officer (DPO), implementing robust technological safeguards such as DLP, IPS/IDS, and data monitoring tools, and conducting comprehensive employee training on data protection. Crucially, strong management support is essential for successful implementation. Without active engagement from bank management, achieving the desired level of data protection will be challenging. Furthermore, proactive monitoring and support from the regulatory body, such as the NBE, are crucial to ensure ongoing compliance and continuous improvement in data protection practices….*"

Extracted information from the interview's transcription	Codes (subthemes) that were taken out of the data transcription	Main Theme
While the NBE previously issued a consumer protection regulation that included some general data protection principles, a dedicated and comprehensive personal data protection regulation is still	There is no personal data protection regulation alone, it is incorporated to the consumer protection.	**No personal data protection.**

forthcoming. The NBE is currently planning to either update existing directives or issue a separate, dedicated directive specifically addressing personal data protection.		
Inadequate implementation of data protection measures, including insufficient deployment of data loss prevention tools, weak email security, and inadequate data encryption are the major challenges of the bank. Also deficiencies in administrative controls, such as the lack of comprehensive data protection policies and procedures, ineffective access controls, and inadequate measures to address internal threats are the main challenges	Inadequate implementation technologies are one of the personal data protection challenge to the bank	**Technology inadequacy**
The NBE would not only impose financial penalties but also actively support customers in pursuing legal recourse, if a customer initiates legal action against a bank for data protection violations, the NBE would support the customer's claims in court	NBE mandate on violation of regulations	**Only financial penalty is taken**
To their data protection processes and governance frameworks. This includes appointing a dedicated Data Protection Officer (DPO), implementing robust technological safeguards such as DLP, IPS/IDS, and data monitoring tools, and conducting comprehensive employee training on data protection. Crucially, strong management support is essential for successful implementation. Without active engagement from bank management, achieving the desired level of data protection will be challenging. Furthermore, proactive monitoring and support from the	Implementation of latest technology, assign DPO, training and NBE follow up is cruitial for protecting personal data,	**Recommendations**

regulatory body, such as the NBE, are crucial to ensure ongoing compliance and continuous improvement in data protection practices		

Table 32: NBE Regulator Response

4.3 Content Analysis

The researcher conducted a thorough examination of the various directives and regulations issued by the regulatory body; the National Bank of Ethiopia, which plays a crucial role in overseeing the operations of financial institutions within the country. In the course of this investigation, it became evident that there is a notable lack of specific regulations or directives that mandate commercial banks to actively protect the personal data of their customers. This gap in regulatory guidance is significant, as it raises concerns about the safeguards in place for bank's customer privacy and data security in the banking sector.

The only pertinent document that was identified during the research is the "Financial Consumer Protection Directive No. FCP/01/2020." This directive briefly references the importance of data protection in its section 4.4, where it stipulates that banks have an obligation to safeguard customer data. In addition to this documents, the researcher found there are few points on Critical Mass Cyber Security Requirement Standard Version 2.0 which is developed by INSA regarding the personal data protection on section 6.36. this indicates that those documents are somewhat vague and does not provide comprehensive guidelines or robust measures to ensure that commercial banks implement effective data protection practices.

Furthermore, the researcher delved into the policies that commercial banks have established regarding personal data protection. The findings revealed a concerning trend: the majority of these banks do not possess dedicated, standalone data protection policies. Instead, they tend to operate under broader information security policies that often do not go into sufficient detail to adequately address the nuances of personal data protection. Typically, these general security policies include only a single clause concerning the protection of personally identifiable information (PII), indicating a minimalist approach to a critical issue. This raises important questions about the efficacy of current measures being taken by commercial banks to ensure

the privacy and protection of their customers' personal data in an increasingly data-driven environment.

4.4 Discussion Section

The findings from this study provide critical insights into the current state of personal data protection practices within Ethiopian commercial banks and their alignment with international frameworks, particularly the EU GDPR. By employing both quantitative and qualitative methods, the study highlights strengths, weaknesses, and actionable recommendations for improving data protection in the banking sector.

I. Alignment with International Standards

The study reveals that while Ethiopian banks have initiated steps to protect personal data, there are significant gaps in aligning with international standards such as the GDPR. For example, the lack of a dedicated Data Protection Officer (DPO) in most banks underscores a key deficiency in meeting GDPR requirements. The findings indicate that only 13.6% of banks have a DPO, which hinders efforts to implement a comprehensive data protection framework. Furthermore, personal data encryption remains underutilized despite being a cornerstone of GDPR compliance. These gaps suggest a need for greater commitment to adopting international best practices.

II. Employee Training and Awareness

The analysis highlights employee training as a critical area requiring improvement. While some training initiatives are in place, 66% of respondents believe these efforts are insufficient for equipping employees with the necessary skills to uphold data protection standards. The qualitative findings further emphasize the inadequacy of current training formats, which rely heavily on text-based materials and lack engaging, role-specific content. Effective training programs that incorporate interactive workshops, infographics, and real-world scenarios are essential for fostering a culture of data protection awareness.

III. Regulatory Oversight and Support

The role of the National Bank of Ethiopia (NBE) in guiding and monitoring data protection practices emerged as a recurring theme in the study. Although the NBE has issued directives emphasizing customer data protection, the absence of detailed and specific guidelines limits

banks' ability to achieve robust compliance. Clear, comprehensive regulatory frameworks, including periodic audits, are necessary to support banks in aligning with both local and international standards.

IV. Challenges in Vendor Management

The study reveals a 36-64 split in perceptions of the effectiveness of vendor management strategies. This inconsistency highlights a critical area of vulnerability; as third-party vendors often handle sensitive customer data. Currently, adherence to GDPR is not a primary consideration when selecting vendors, reflecting a gap that must be addressed as Ethiopia advances its understanding of data protection regulations.

V. Resource Allocation and Budgeting

Implementing GDPR-compliant frameworks requires significant financial and technological investments. While bank management demonstrates a willingness to allocate resources for IT security, budget approvals often depend on the perceived business value of specific initiatives. This dependency underscores the importance of effectively communicating the strategic and financial benefits of robust data protection measures.

VI. Readiness for GDPR Framework Implementation

Despite existing gaps, the study identifies promising indicators of readiness among Ethiopian banks to adopt GDPR-aligned frameworks. A majority of respondents (82.8%) believe their institutions are adaptable and capable of implementing comprehensive data protection measures. However, inconsistencies in management commitment and employee adherence to protocols pose potential barriers to seamless implementation.

Key Implications

1. **Strategic Leadership:** Establishing a dedicated DPO in every bank is essential for driving accountability and ensuring compliance with evolving data protection standards.
2. **Policy Integration:** Banks should unify existing policies into a comprehensive framework that clearly outlines procedures and aligns with international standards.
3. **Enhanced Training Programs:** Revamping training approaches with engaging content and role-specific focus can improve employee compliance and awareness.

4. **Strengthened Regulatory Frameworks:** Detailed guidelines and consistent regulatory oversight are crucial for fostering a secure and compliant data protection environment.
5. **Resource Optimization:** Demonstrating the business value of data protection initiatives can secure the financial and technological resources needed for implementation.

4.5 Conclusion

The results of this study remind us that Ethiopian banks have made commendable progress in certain areas, particularly in data protection. However, they still face significant challenges in achieving full compliance with GDPR and other international standards. To bridge these gaps, a multifaceted approach is necessary. Leadership within the banking sector must prioritize data protection as a core strategic goal, ensuring that it receives the attention it deserves. Comprehensive training programs should be implemented to enhance staff awareness and expertise in handling data securely and in line with global regulations. Furthermore, fostering partnerships with regulatory bodies can provide valuable guidance and ensure alignment with both local and international compliance requirements. Lastly, substantial investment in advanced technological resources and infrastructure is essential to develop a robust data protection framework. By addressing these areas, Ethiopian banks can not only safeguard customer information more effectively but also enhance their credibility and competitiveness on a global scale.

Chapter Five

Framework Design and Development

5.1Overview of the Designed Framework

While in Ethiopia the adoption of personal data protection is regulation is on early stage, it is observing that it not matures enough as equivalent to the EU GDPR, commercial banks can take a proactive approach by implementing a framework aligned with GDPR principles. This forward-thinking strategy offers several advantages. Firstly, it demonstrates the bank's commitment to protecting customer data privacy, which can be a significant differentiator in a competitive financial services market. Secondly, a GDPR-aligned framework ensures the bank is prepared for potential for adoption and implementation of data protection regulations in Ethiopia. By having a GDPR-based framework in place, commercial banks can avoid scrambling to comply with new regulations and ensure a smooth transition. Finally, implementing strong data protection practices fosters trust with customers. Data breaches and privacy scandals can erode customer confidence in financial institutions. By prioritizing data security and transparency, banks can build stronger relationships with their customers and position themselves as leaders in responsible data stewardship.

5.2 Framework Development

Direct implementation of the EU GDPR presents significant challenges for Ethiopian commercial banks due to various factors. One key obstacle is the prevalence of unstructured data within banks, which is not easily searchable or organized. This makes it difficult to comply with GDPR's comprehensive data protection requirements, particularly those related to data subject rights and data breaches.

Another challenge arises from potential conflicts between the GDPR's "right to be forgotten" and local regulatory requirements, such as anti-money laundering and fraud prevention laws. Ethiopian banks are obligated to retain certain data for compliance purposes, which may clash with the GDPR's data erasure provisions.

Furthermore, the complexity of the banking ecosystem, involving numerous third-party vendors, poses challenges in ensuring GDPR compliance. Many of these vendors, particularly

those based in Africa and the Middle East, may not have the necessary infrastructure or expertise to meet GDPR standards.

Given these challenges, a direct, full-scale implementation of the EU GDPR is not feasible for Ethiopian commercial banks. To address this, the researcher has developed a tailored framework that aligns with the key principles of the GDPR while considering the specific context of Ethiopian commercial banks. This framework focuses on practical and achievable data protection measures that can be implemented with minimal resources.

Key Considerations of the developed framework are:

- **Data Minimization:** Collect and retain only the necessary personal data.
- **Data Security:** Implement robust security measures to protect personal data from unauthorized access, use, disclosure, alteration, or destruction.
- **Data Subject Rights:** Respect data subject rights, such as the right to access, rectify, and correct personal data, to the extent permitted by local laws.
- **Data Breach Notification:** Establish procedures for detecting, investigating, and reporting data breaches.
- **Employee Training:** Train employees on data protection principles and practices.
- **Regular Review and Updates:** Continuously review and update data protection policies and procedures to adapt to evolving regulatory requirements.

By focusing on these core principles and implementing the proposed framework, the researcher believes that Ethiopian commercial banks can significantly enhance their data protection practices and mitigate risks, even without a full-scale EU GDPR implementation. This tailored approach ensures a practical and effective solution for the specific needs of the Ethiopian banking sector.

5.3 Framework Components

The framework for personal data protection is a comprehensive and multifaceted system that encompasses a cohesive set of interrelated components, all meticulously designed to uphold regulatory compliance, safeguard sensitive personal information, and enhance overall data governance practices within organizations. These components are not merely standalone elements; rather, they are crafted to integrate seamlessly into the daily operations of the

commercial banks in Ethiopia, ensuring that data protection is interlaced into the very fabric of its processes and culture.

One of the key aspects of this framework is its alignment with internationally recognized standards, such as the European Union's General Data Protection Regulation (EU GDPR). This alignment is crucial, as it not only helps the bank meet legal obligations but also positions them as responsible stewards of personal data in a global context. By adhering to such standards, the banks can demonstrate their commitment to protecting individual privacy rights and fostering a culture of accountability.

The framework addresses both organizational and operational requirements, ensuring a holistic approach to managing data responsibly. This includes establishing clear policies and procedures for data handling, implementing robust security measures to protect against unauthorized access, and conducting regular audits to assess compliance and identify areas for improvement. By fostering transparency in data practices, organizations can build trust with their stakeholders, including customers, employees, and regulatory bodies.

Moreover, the framework is designed to mitigate risks associated with data breaches and non-compliance. This involves not only proactive measures, such as risk assessments and incident response plans, but also a commitment to continuous improvement. Organizations are encouraged to stay informed about emerging threats and evolving regulatory landscapes, allowing them to adapt their practices accordingly.

This strategic alignment with global best practices not only enhances organizational accountability but also contributes to operational efficiency. By streamlining data governance processes and ensuring that all employees are trained in data protection principles, organizations can reduce the likelihood of errors and improve their overall responsiveness to data-related challenges.

Ultimately, the implementation of a robust personal data protection framework fosters trust among stakeholders. When individuals feel confident that their personal information is being handled with care and respect, they are more likely to engage with the organization, whether as customers, employees, or partners. This trust is invaluable in today's data-driven world, where the responsible management of personal data is paramount to sustaining long-term relationships and achieving business success.

The developed personal data protection framework is presented on diagram below. Also each component of the framework is described in detail.

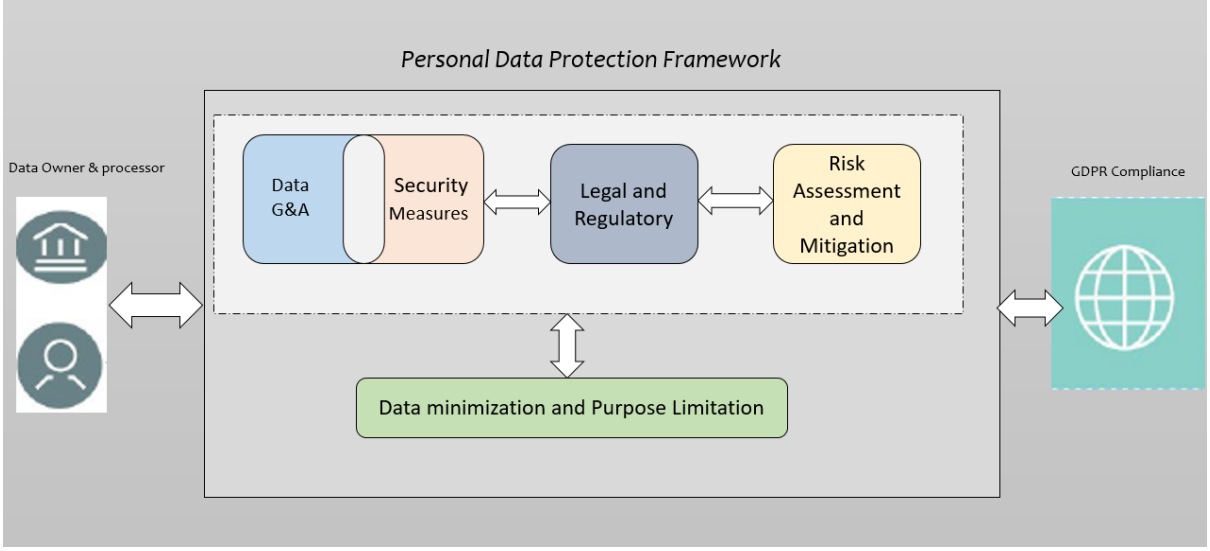

Figure 3: Personal Data Protection Framework HLD

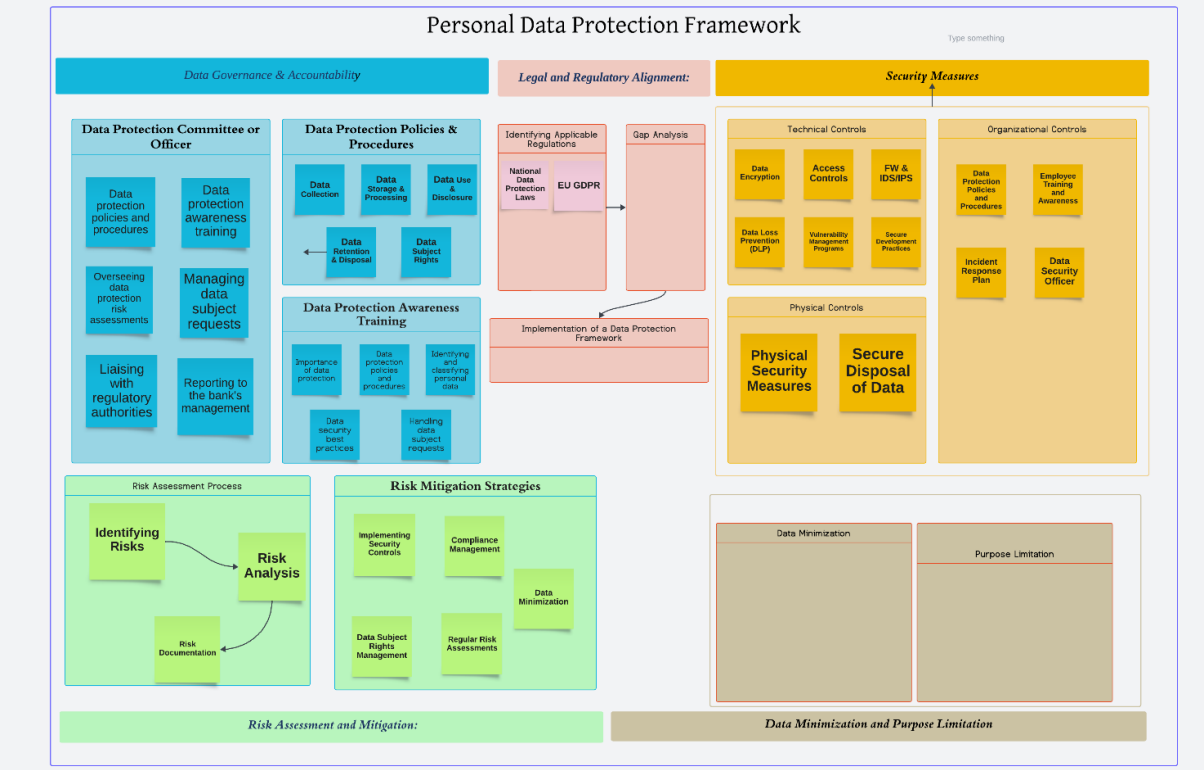

Figure 4: Personal Data Protection Framework Detailed

5.3.1 Data Governance & Accountability

Data Governance & Accountability is the foundation of a robust personal data protection framework, especially for commercial banks that handle vast amounts of sensitive customer

information. It establishes a clear structure with well-defined roles, responsibilities, and processes to ensure that customer data is collected, stored, used, and disposed of in a manner that complies with data protection regulations and respects individual privacy rights. This alignment with the principles of the EU GDPR helps ensure that the bank is prepared for potential regulatory changes and demonstrates its commitment to responsible data stewardship, which can be a significant competitive differentiator in the financial services industry.

Core Elements of Data Governance:

- **Data Protection Committee or Officer:**

A dedicated data protection committee or officer is crucial for overseeing data protection compliance within the bank. This group, often referred to as a data privacy committee, is responsible for developing and implementing a comprehensive data protection program that aligns with regulatory requirements and best practices. The committee should be composed of individuals with diverse expertise, including legal, compliance, information security, and business operations. This ensures a well-rounded perspective on data protection considerations across various aspects of the bank's activities. The data protection committee or officer should have a strong understanding of relevant data protection regulations, such as the EU GDPR, Ethiopian Personal data protection regulation, data security best practices, and the bank's specific data processing policies and guidelines. They are responsible for staying abreast of regulatory changes and industry developments in data privacy to ensure the bank's practices remain compliant and effective.

Key functions of the data protection committee or officer typically include:

- Developing and implementing data protection policies and procedures.
- Conducting data protection awareness training and education programs for employees.
- Overseeing data protection risk assessments and audits.
- Managing data subject requests (e.g., access, rectification, etc).
- Liaising with regulatory authorities on data protection matters.
- Reporting to the bank's management on data protection compliance issues.

- **Data Protection Policies & Procedures:**

  Comprehensive policies and procedures must govern every aspect of personal data handling to ensure that customer information is managed responsibly and securely throughout its lifecycle. These policies should clearly define the purposes and methods of data collection, establish secure practices for storing personal data, and specify the lawful and intended uses of such data during processing. They must also outline the conditions under which customer data may be disclosed to third parties, set clear timeframes for data retention, and detail secure disposal procedures once data is no longer required. Furthermore, they should provide transparent and efficient processes for addressing customer rights, including requests for data access, rectification, restriction, and portability. To be effective, these policies must be clear, concise, regularly updated, and easily accessible to all bank employees.

- **Data Protection Awareness Training:**

  Regular training programs shall conducted for all bank employees to ensure they fully understand their roles and responsibilities in handling personal data in accordance with established policies and regulations. These training sessions cover critical topics such as the importance of data protection, the bank's specific data protection policies and procedures, techniques for identifying and classifying personal data, and best practices for maintaining data security—including password hygiene and phishing awareness. Additionally, employees are trained on how to properly handle data subject requests, ensuring that customer rights are respected and fulfilled in a timely and compliant manner.

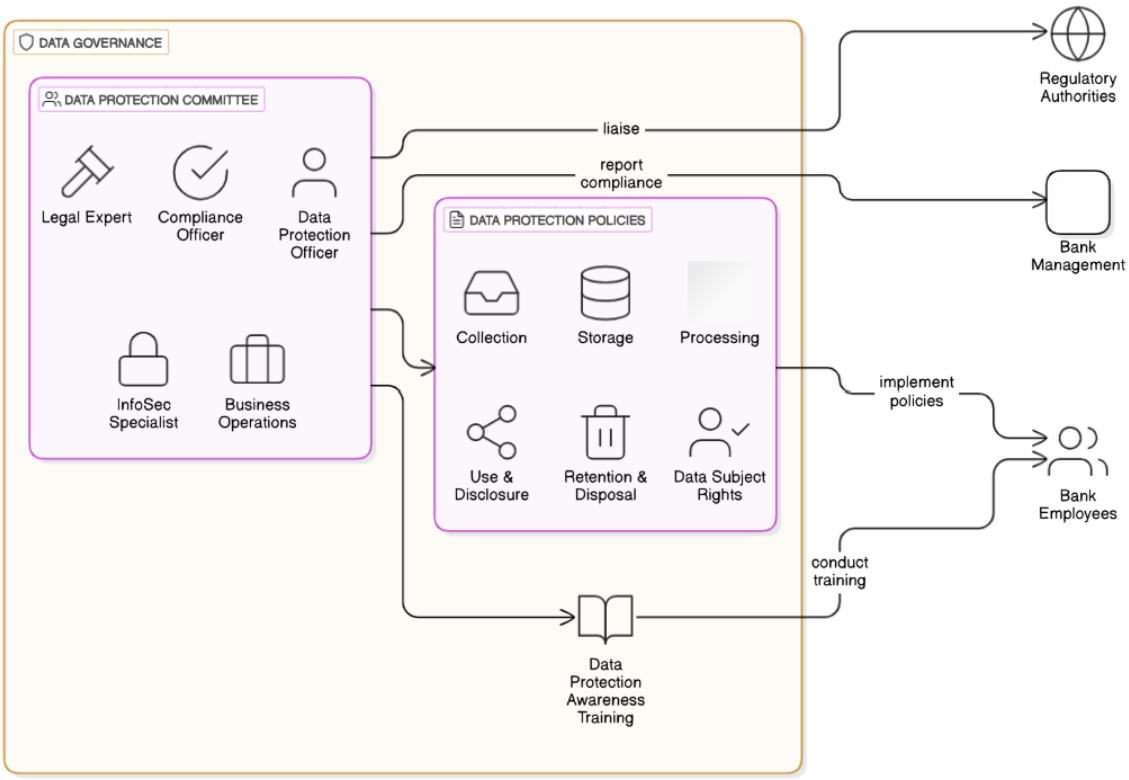

Figure 5: Data Governance and Accountability

5.3.2 Legal and Regulatory Alignment:

In the realm of personal data protection for commercial banks, legal and regulatory alignment refers to the strategic approach of ensuring a bank's data handling practices comply with a complex and ever-evolving landscape of data privacy regulations. This alignment is crucial for several reasons. First, it minimizes the risk of regulatory non-compliance, which can result in hefty fines, penalties, and reputational damage. Regulatory bodies around the world are increasingly enforcing data protection laws, and the financial sector is often a prime target for enforcement actions due to the vast amount of sensitive customer data it collects and processes. By aligning with relevant regulations, banks can demonstrate their commitment to responsible data stewardship and avoid the severe consequences of non-compliance.

To ensure effective data protection, banks must begin by identifying the legal and regulatory requirements that apply to their operations. This includes strict adherence to national data protection laws and a proactive approach to meeting future obligations set by the National Bank of Ethiopia and other regulatory authorities. Additionally, while the EU General Data Protection Regulation (GDPR) may not be directly enforceable, it remains a globally recognized benchmark. Aligning with GDPR principles not only reinforces a strong

commitment to data privacy but also provides a solid foundation for meeting domestic compliance standards.

Once the applicable regulations are identified, the bank should carry out a thorough gap analysis to assess how its current data protection practices align with legal and regulatory requirements. This analysis is essential for identifying compliance gaps and areas requiring improvement. Based on the results, the bank can determine whether its existing practices meet regulatory expectations or if there is a need to implement or revise its data protection framework. Such a framework should establish clear, well-documented policies, procedures, and control measures to ensure sustained regulatory compliance and to enhance the bank's overall data governance and risk management capabilities.

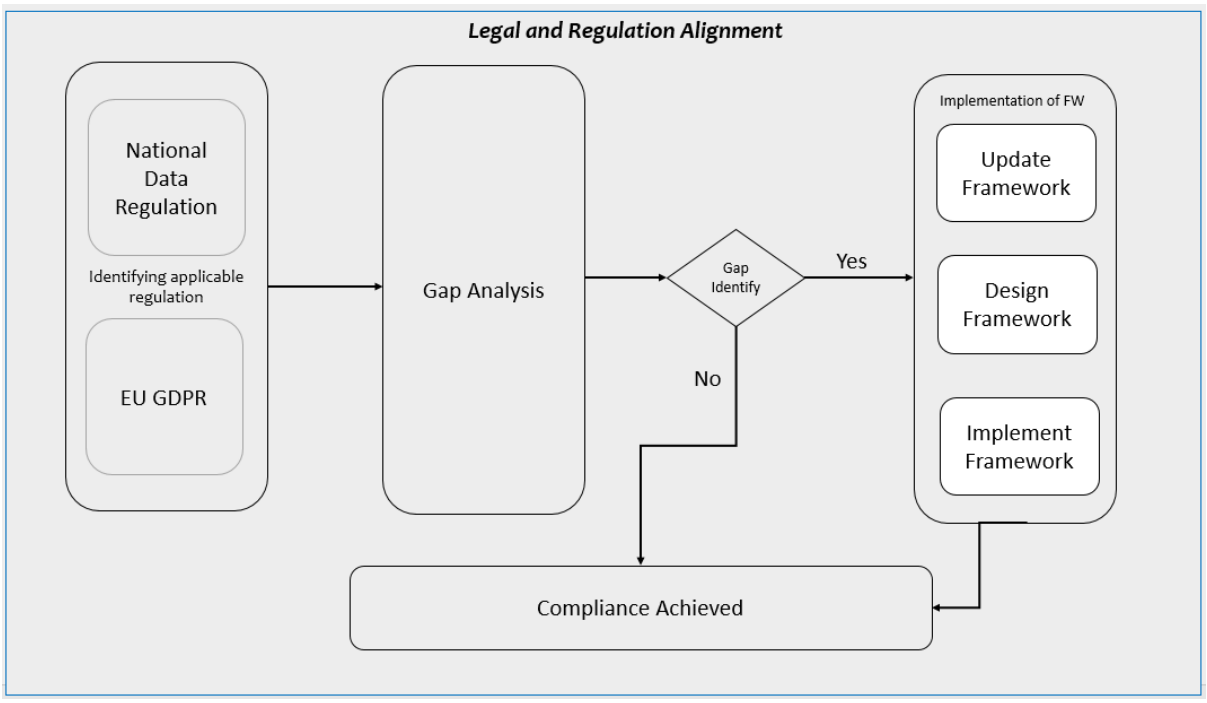

Figure 6: Legal and Regulatory Alignment

5.3.3 Risk Assessment and Mitigation:

In the realm of personal data protection for commercial banks, risk assessment and mitigation are fundamental pillars of a secure and compliant data protection framework. Personal data breaches, unauthorized access, and non-compliance with regulations can inflict a cascade of negative consequences for banks. These can include financial penalties that can reach millions

of Birr/dollars under regulations like the EU GDPR. Reputational damage can be severe, eroding customer trust and leading to a decline in new business. Perhaps most critically, data breaches can expose sensitive customer information, such as financial data, placing customers at risk of identity theft and fraud. By proactively identifying and mitigating these risks, banks can safeguard customer data, ensure compliance with regulations, and operate with confidence in the digital age.

Risk Assessment Process:

The risk assessment process begins with the identification of potential risks associated with personal data processing within the bank. These risks typically fall into four categories: security risks, such as data breaches, unauthorized access, and cyberattacks that threaten the confidentiality, integrity, and availability of data; compliance risks, stemming from non-adherence to data protection regulations, which can result in fines, legal penalties, and reputational harm; operational risks, including human error, system inefficiencies, or lack of training that may lead to data mishandling; and business risks, such as loss of customer trust, brand damage, and client attrition due to privacy concerns. Recognizing these risks is the first step toward effective data protection and governance.

Following identification, each risk is analyzed in terms of its likelihood and potential impact, enabling the bank to prioritize risks and allocate resources efficiently. This analysis takes into account factors such as the sensitivity and value of personal data, the vulnerability of IT systems, the probability of threats materializing, and the severity of consequences resulting from incidents like data breaches or regulatory violations.

All identified risks, along with their likelihood, impact, and assigned priority levels, are formally documented. This risk register becomes a foundational reference for designing and implementing targeted mitigation strategies that safeguard personal data and ensure regulatory compliance.

Risk Mitigation Strategies:

Following the risk assessment, the bank must implement a comprehensive set of security controls designed to protect personal data from unauthorized access, misuse, or loss. These controls span technical, organizational, and physical domains. Technical measures include

encryption of data at rest and in transit, strong access controls such as multi-factor authentication, firewalls, intrusion detection systems, and data loss prevention (DLP) tools. Organizational controls involve establishing robust data protection policies and procedures, conducting regular employee training on security best practices, maintaining incident response and vulnerability management programs. Physical controls are also critical and may include secure storage areas, restricted physical access to sensitive data locations, and environmental safeguards.

In addition to these controls, banks must adopt a holistic compliance management program that aligns with applicable data protection regulations. This includes creating clear policies and procedures, developing breach response plans, and maintaining continuous staff awareness and training. Data minimization controls is one of the basic controls with its core principles such as collecting only what is necessary and retaining it for the shortest time needed. Equally important is data subject rights management, which ensures that the bank can efficiently handle requests for access, rectification, erasure, restriction, or data portability. To maintain effectiveness, the bank should conduct regular risk assessments to identify emerging threats and continuously refine its mitigation strategies, thereby reinforcing a proactive approach to data security and compliance.

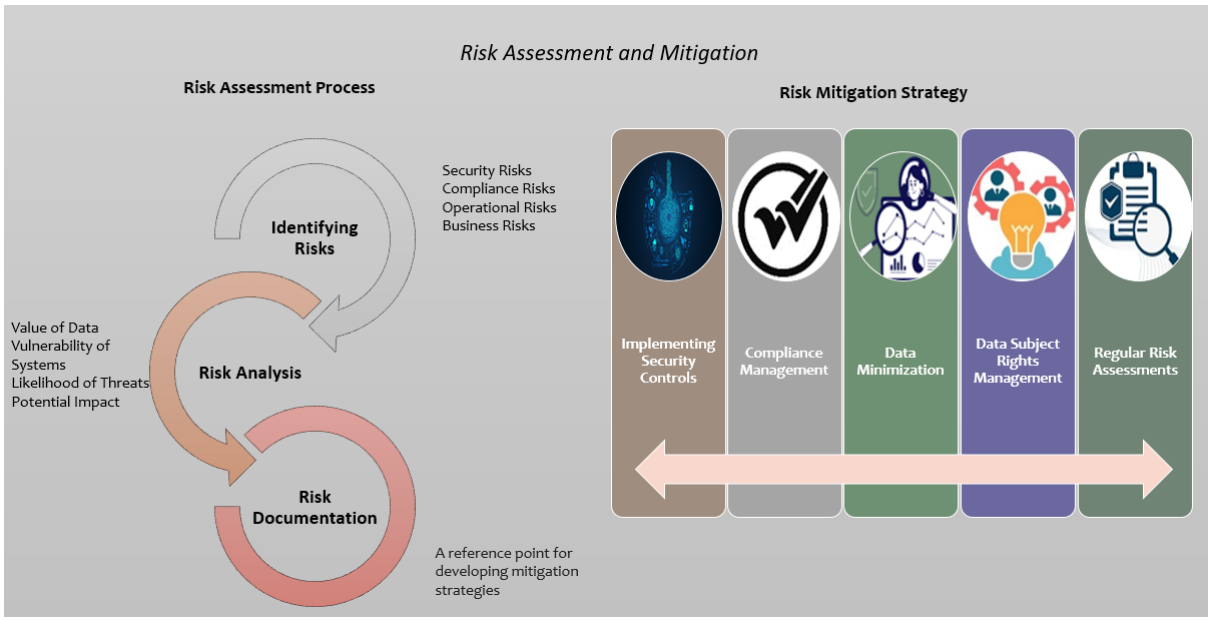

Figure 7: Risk Assessment and Mitigation

5.3.4 Data Minimization and Purpose Limitation:

Data minimization and purpose limitation are two fundamental principles protected personal data protection, that are crucial for responsible personal data handling, particularly within commercial banks. These principles work in tandem to ensure that banks collect, use, and retain only the personal data necessary for specific and legitimate purposes. Data minimization focuses on the quantity of data collected, while purpose limitation emphasizes the reason for collecting the data. By adhering to both principles, banks can demonstrate respect for customer privacy, reduce the risks associated with data collection and storage, and ensure compliance with data protection regulations.

Data Minimization:

Data minimization refers to the practice of collecting, using, and retaining only the minimum amount of personal data that is **adequate, relevant, and limited** to achieve the specific purposes for which it is processed. This means banks should avoid collecting excessive or irrelevant personal data from customers.

Data minimization offers several key benefits for banks. By reducing the amount of data collected, it significantly lowers the risk of data breaches and unauthorized access, as there is less sensitive information to manage, making security controls easier to implement. It also supports enhanced compliance with regulations, particularly the GDPR's data minimization principle, showcasing the bank's commitment to responsible data stewardship. Moreover, minimizing data simplifies data handling processes, reduces storage requirements, and improves operational efficiency. Perhaps most importantly, it strengthens customer trust, as clients value organizations that collect only the necessary data, fostering greater confidence in the bank's commitment to safeguarding their privacy.

Implementation Strategies:

To ensure effective personal data protection, it is essential to create a comprehensive inventory of all personal data collected and classify it based on sensitivity and purpose. Clearly defining the specific purposes for which customer data is collected, such as gathering contact information for account management, helps avoid unnecessary data collection. It is important to collect only the information that is needed during customer interactions, such as through

application forms or online banking processes. Regular reviews of the collected data should be conducted periodically to ensure it remains relevant and necessary for its intended purposes. Additionally, establishing clear data retention policies is critical, outlining how long different types of data will be retained, ensuring that data is not kept longer than necessary.

Purpose Limitation:

Purpose limitation dictates that personal data can only be collected and processed for **specified, explicit, and legitimate purposes** communicated to the data subject (customer) at the time of collection. Once collected, the data can only be further processed in a manner compatible with those original purposes.

Some benefits of purpose limitation include enhanced **transparency and control**, as customers gain a clear understanding of how their data is being used and have more control over their personal information. It also ensures **compliance** with the GDPR's purpose limitation principle, demonstrating transparency in data processing practices. Additionally, purpose limitation helps **reduce the risk of misuse**, as it limits the potential for data to be used for unauthorized purposes, thereby safeguarding customer privacy and trust.

Implementation Strategies:

Develop clear and concise privacy notices to explain the specific purposes for which personal data is collected and how it will be used, obtain informed consent from customers for specific data processing activities (e.g., marketing campaigns), and establish clear procedures to handle data subject access requests, ensuring that data is used for the originally communicated purposes.

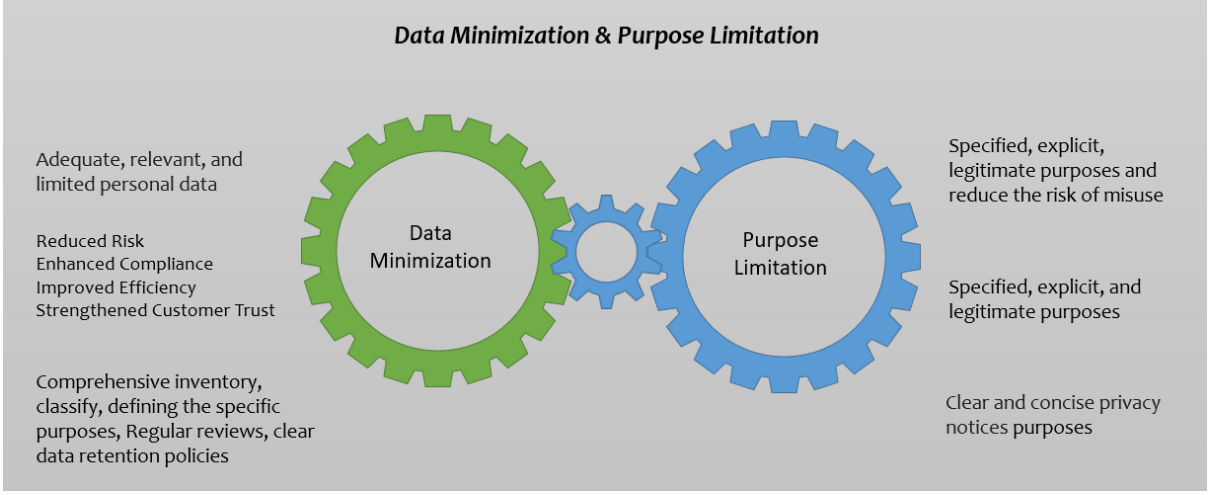

Figure 8: Data Minimization and Purpose Limitation

5.3.5 Security Measures

The ever-growing digital landscape presents both opportunities and challenges for commercial banks.(Emmanuel Magnus-Eweka, 2023). On the one hand, technology empowers banks to deliver a wider range of financial services to customers in a more efficient, convenient, and accessible manner. Online and mobile banking platforms enable customers to manage their finances from anywhere, anytime, and innovative financial products and services are constantly emerging. However, this digital transformation also introduces new vulnerabilities in personal data security. As banks collect and store increasing amounts of sensitive customer information, such as account details, financial transactions, and personal identification data, cybercriminals are constantly devising new methods to exploit weaknesses in security systems and steal this valuable data. To safeguard customer information, ensure compliance with data protection regulations (like the EU GDPR or Ethiopian personal data protection regulations), and maintain trust in the financial sector, commercial banks require robust security measures.

Technical Controls:

- **Data Encryption:** Encrypting personal data at rest (stored on servers) and in transit (during transmission) renders it unreadable to unauthorized individuals even if intercepted. Encryption technologies like AES-256 are industry standards.
- **Access Controls:** Implementing a layered approach to access control ensures that only authorized personnel have access to personal data based on their roles and responsibilities. This might involve using strong passwords, multi-factor authentication (MFA) with additional

verification steps, and role-based access controls (RBAC) that restrict access to specific data sets.

- **Firewalls and Intrusion Detection/Prevention Systems (IDS/IPS):** Firewalls act as gateways that filter incoming and outgoing network traffic, blocking unauthorized access attempts. IDS/IPS systems continuously monitor network activity for suspicious behaviour that might indicate a security breach attempt.
- **Data Loss Prevention (DLP):** DLP solutions can be deployed to monitor and prevent the unauthorized exfiltration of sensitive data from the bank's network. DLP can identify and block attempts to transfer data via email, USB drives, or other channels.
- **Vulnerability Management Programs:** Regularly scanning systems and applications for vulnerabilities and patching them promptly is crucial to address potential security weaknesses that attackers can exploit.
- **Secure Development Practices:** Implementing secure coding practices and secure software development lifecycles (SDLC) helps minimize vulnerabilities introduced during the software development process.
- **Security Information and Event Management:** By collecting event log data from various sources, it identifies activity that deviated from the normal in real-time and gives visibility for the organization what going on their network. This tool is a very curtail device on the organization to meet a compliance requirement as DGPR.

Organizational Controls:

- **Data Protection Policies and Procedures:** Comprehensive data protection policies and procedures should clearly outline the bank's approach to handling personal data. These policies should address data collection, storage, use, disclosure, retention, and disposal.
- **Employee Training and Awareness:** Regular training programs are essential for educating employees on data security best practices. Training should cover topics like password hygiene, phishing awareness, data breach response procedures, and recognizing suspicious activity.
- **Incident Response Plan:** A well-defined incident response plan outlines the steps to be taken in case of a data breach or security incident. This plan should include procedures for identifying, containing, investigating, and recovering from a breach, as well as notifying regulatory authorities and affected data subjects as required by regulations.

- **Data Security Officer:** Appointing a data security officer (DSO) can be beneficial. The DSO is responsible for overseeing the bank's data security program, implementing controls, and ensuring compliance with regulations.

Physical Controls:

- **Physical Security Measures:** Implementing physical security measures to protect data centers and other locations where personal data is stored is critical. These measures might include access control systems, security cameras, and environmental controls (e.g., proper temperature and humidity) to safeguard physical infrastructure.
- **Secure Disposal of Data:** When personal data reaches the end of its retention period, it should be disposed of securely. This might involve using secure data wiping software for electronic data or shredding physical documents to ensure they cannot be reconstructed.

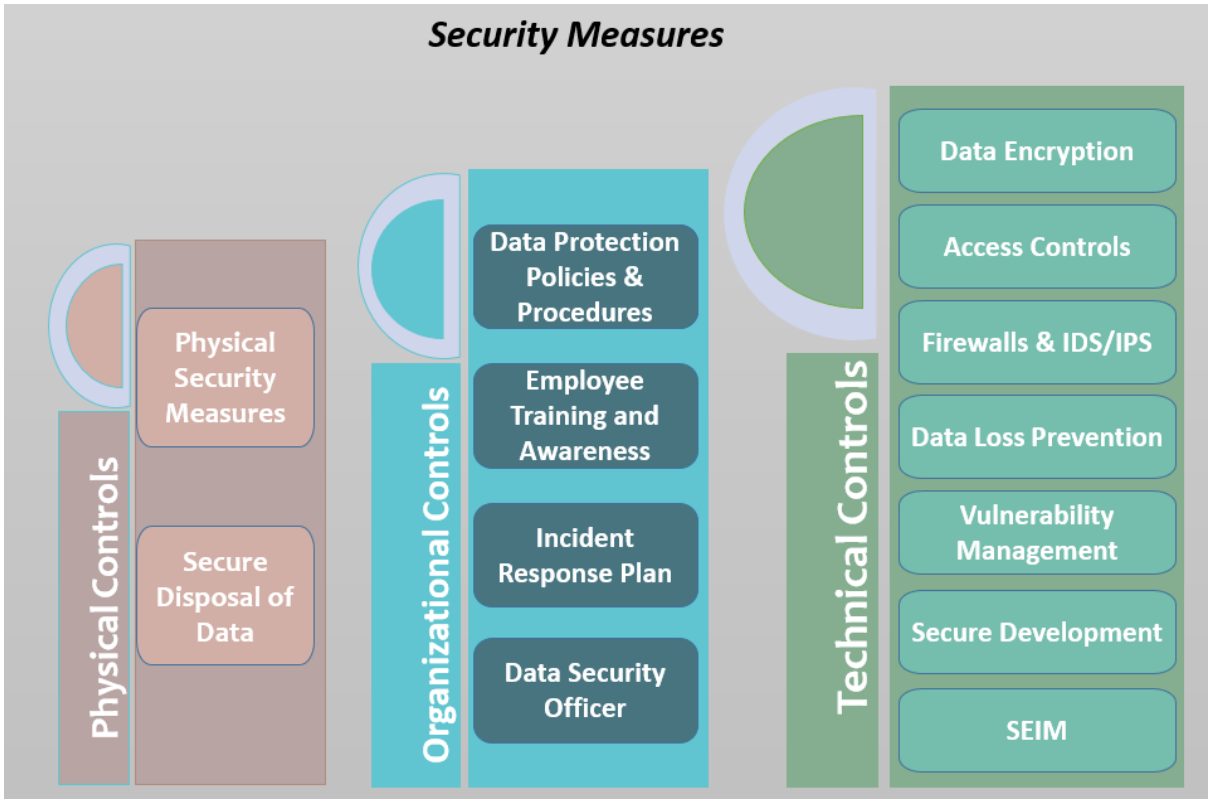

Figure 9: Security Measures

5.4 Training and Awareness Programs

In the realm of personal data protection for commercial banks, effective training and awareness programs are crucial for ensuring all employees understand their roles and responsibilities in handling customer data securely and compliantly. With the ever-increasing volume of sensitive

customer information collected and stored by banks, human error remains a significant risk factor for data breaches. According to (Baker et al., 2010) human error is a contributing factor in over 80% of data breaches. By equipping employees with the knowledge and skills necessary to safeguard data, well-designed training programs can significantly reduce the risk of human error and create a culture of data security awareness within the bank.

Training programs should be carefully tailored to meet the specific needs and responsibilities of various employee groups within the bank. While all employees should receive foundational data protection training, those handling sensitive data regularly require more specialized instruction. General awareness training should be mandatory for all staff, regardless of their role, to provide a basic understanding of data protection principles, the bank's policies, and best practices for handling personal data securely. This foundational training ensures a strong organizational commitment to safeguarding data at all levels.

For high-risk employees, such as customer service representatives, loan officers, and IT personnel, more in-depth training is crucial. These employees often access or process sensitive customer data, and therefore need comprehensive instruction on data protection regulations (such as the EU GDPR or Ethiopian data protection laws), advanced data security protocols, and specific procedures for managing data subject rights, including requests for access, rectification, erasure, and portability. This targeted training ensures that high-risk employees are fully equipped to handle personal data responsibly and in compliance with regulatory requirements.

An effective data protection training program in the banking sector must comprehensively address the responsibilities and risks associated with handling personal data. The content should begin by emphasizing the importance of data protection, ensuring employees understand both regulatory obligations and the bank’s commitment to safeguarding customer privacy. It should then introduce the core principles of data protection, such as data minimization, purpose limitation, and lawful processing. Employees must be well-versed in the bank's specific data protection policies and procedures, covering the entire data lifecycle—from collection and storage to use, disclosure, retention, and secure disposal. Training should also focus on identifying and classifying personal data by sensitivity levels, which is essential for applying appropriate security measures. Furthermore, practical instruction on data security best practices, including password hygiene, phishing awareness, data encryption, and secure data disposal, is vital. Staff who interact with customers should receive specialized training on

handling data subject requests (e.g., access, rectification, erasure, portability), and all employees must be equipped to recognize and report data breaches promptly, following established protocols.

To maximize engagement and retention, the program should employ diverse training delivery methods tailored to various learning styles. E-learning modules offer flexibility and accessibility for self-paced learning, while in-person sessions foster interaction and deeper understanding through discussion and Q&A. Scenario-based training helps employees apply their knowledge to realistic situations, reinforcing their ability to respond appropriately in real-life contexts. Finally, given the constantly evolving regulatory landscape and emerging cyber threats, regular updates and refresher courses are essential to keep employees' knowledge current and ensure continuous compliance and vigilance.

5.5 Pilot Implementation and Stakeholder Feedback

Implementing a pilot initiative for a comprehensive personal data protection framework in commercial banks presents several challenges that must be strategically managed. Resource limitations are a primary obstacle, as securing adequate funding and allocating dedicated personnel to support the pilot can be difficult amidst competing priorities. Organizational challenges also play a significant role, particularly in obtaining executive-level approvals and overcoming internal resistance to change, both of which can delay or hinder implementation. These barriers highlight the need for strong leadership, cross-functional collaboration, and a phased implementation strategy to ensure the pilot’s success.

To tackle these challenges, the research began by collecting feedback from experts. The draft framework was presented to Information Security Department Directors from different commercial banks.

The initial draft of the personal data protection framework was meticulously crafted and subsequently shared with the Information Security Department Directors and Senior Managers from a diverse array of commercial banks. This collaborative effort aimed to gather expert feedback that would be instrumental in refining the framework to better serve the needs of the banking sector.

The feedback received was both insightful and constructive, highlighting several critical areas that required attention and enhancement. One of the primary concerns raised was the need for

Enhanced Integration. Stakeholders emphasized the importance of ensuring that all components of the framework work seamlessly together. This integration is vital for creating a cohesive approach to personal data protection, where policies, procedures, and technologies are aligned to support the overarching goals of data security and compliance.

Another significant point of feedback revolved around Clarity on Redundancies. Experts pointed out the necessity of explicitly addressing and eliminating any redundant elements within the framework. This includes aspects such as policy development processes, the appointment of data protection officers, awareness training programs, and data governance initiatives. By streamlining these elements, the framework can become more efficient and easier to implement, ultimately leading to better data protection outcomes.

Additionally, the feedback underscored the importance of establishing a Unique Value Proposition for the framework. Stakeholders expressed the need for a clear articulation of the unique aspects of this framework, particularly in how it differentiates itself from other existing frameworks in the market. This clarity will not only help in promoting the framework but also in ensuring that its distinct benefits are recognized and leveraged by the banks.

In response to this valuable feedback, the framework underwent a thorough revision process. The researcher, drawing on the insights provided, made significant adjustments to address these key areas of concern. The revised framework is now poised to offer a more integrated, streamlined, and distinctive approach to personal data protection.

The researcher firmly believes that the refined framework will significantly enhance the effectiveness of personal data protection practices within Ethiopian commercial banks. By providing a robust and comprehensive guide for implementation and continuous improvement, the framework aims to empower banks to better safeguard personal data, comply with regulatory requirements, and build trust with their customers. This proactive approach to data protection is essential in today's digital landscape, where the risks associated with data breaches and privacy violations are ever-increasing.

5.6 Ethical Considerations

The framework places a strong emphasis on the ethical handling of personal data. It underscores the importance of respecting privacy rights, promoting transparency, and fostering an ethical culture within the commercial banks.

The designed framework is tailored to the unique context of Ethiopian commercial banks, addressing local challenges while aligning with global best practices as mandated by the EU GDPR. It aims to create a resilient and compliant data protection infrastructure, instilling trust and confidence in the banking sector.

5.7 Conclusion

This framework offers a thorough and adaptable strategy specifically designed for Ethiopian commercial banks, enabling them to effectively protect personal data. By implementing this framework, banks can ensure that they are in alignment with international standards, which is crucial in today's globalized financial environment. This alignment not only helps in meeting regulatory requirements but also plays a significant role in enhancing customer trust, as clients are increasingly concerned about the security of their personal information.

The framework acts as a detailed blueprint that addresses the unique challenges faced by banks operating in Ethiopia. These challenges may include varying levels of technological infrastructure, differing regulatory landscapes, and the need for tailored solutions that resonate with local cultural and economic contexts. By focusing on these local challenges, the framework encourages banks to adopt practices that are not only compliant with global standards but also relevant to the Ethiopian market.

Furthermore, the framework promotes the adoption of best practices in data protection, which can lead to improved operational efficiency and risk management. By fostering a culture of compliance and accountability, Ethiopian commercial banks can enhance their reputation and build stronger relationships with their customers. Ultimately, this comprehensive approach not only safeguards personal data but also contributes to the overall stability and integrity of the banking sector in Ethiopia.

Chapter Six

Conclusion and Recommendation

6.1 Introduction

This chapter presents a comprehensive summary of the research findings on personal data protection practices within Ethiopian commercial banks. It directly links these findings to the initial research objectives and distils key insights into actionable recommendations for enhancing data protection within the banking sector.

Drawing inspiration from globally recognized frameworks such as the EU GDPR, the research emphasizes the importance of aligning personal data protection practices with international best practices. This approach aims to not only enhance customer trust and confidence but also ensure compliance with evolving global standards.

Furthermore, the chapter identifies key areas for future research, encouraging further exploration and investigation by fellow researchers to expand upon the findings of this study and contribute to the ongoing evolution of data protection practices within the Ethiopian banking industry.

6.2 Result and conclusion

The purpose of this research is to design a comprehensive personal data protection framework for commercial banks in Ethiopia, aligned with the internationally recognized EU GDPR (General Data Protection Regulation). This study uses GDPR as a baseline model, adapting its principles to meet the specific needs and operational realities of Ethiopian banks. The primary goal of this research is to enhance the current personal data protection practices in Ethiopian banks, elevating them to meet the high expectations of customers who increasingly value privacy and data security. By doing so, the framework aims to build customer trust, improve organizational accountability, and position banks for seamless compliance with international standards. Furthermore, the proposed framework is intended to support Ethiopian banks in achieving global data protection compliance, fostering their competitiveness in an interconnected and regulated financial ecosystem. This study underscores the importance of aligning local practices with global standards to ensure robust data protection, mitigate risks, and drive sustainable growth in the digital economy.

The researcher performed a thorough examination of various literature to pinpoint existing research gaps in the field of personal data protection practises on commercial banks in Ethiopia. This examination also laid the groundwork for developing the theoretical and conceptual frameworks that support the study. To adopt a comprehensive and organized methodology, a Design Science Research Methodology (DSRM) was utilized to meticulously design, develop, and assess the proposed framework.

Both quantitative and qualitative research techniques were employed to gather data from pertinent departments within commercial banks in Ethiopia. The data collection involved surveys and interviews, to obtain insights from stakeholders actively involved in data management and protection practices. The gathered data was then systematically analyzed to evaluate the current state of data protection in Ethiopian banks, uncovering gaps, challenges, and areas that need enhancement.

In light of these findings, the researcher introduced a detailed framework aimed at addressing the identified deficiencies. This framework integrates global best practices, especially the EU GDPR, and tailors them to the specific needs and operational contexts of the Ethiopian banking sector. This iterative and evidence-driven approach guarantees the framework's relevance, applicability, and effectiveness in improving personal data protection practices.

The proposed framework was created through ongoing development and assessment activities. It was also shared with subject matter experts, such as directors of Information Security Departments from different commercial banks. The framework was enhanced based on the feedback provided by these experts. The framework composes of five different interdependent components that allow the bank to have a comprehensive framework to protect their customer personal data.

The study's results are systematically organized by addressing the established research questions (RQs), ensuring that the findings align directly with the research objectives.

RQ1. What are the existing data protection practices in Ethiopian commercial banks?

Based on the research findings, Ethiopian commercial banks are making concerted efforts to protect customer data by integrating personal data protection with measures specifically designed for securing critical financial data. These efforts emphasize the principles of

confidentiality and integrity, which are fundamental to maintaining customer trust. However, it is concerning that many banks operate under the assumption that safeguarding financial information inherently ensures the protection of personal data. This misconception neglects the specific requirements for personal data protection as defined by comprehensive frameworks like the EU General Data Protection Regulation (GDPR). A thorough evaluation of the current practices against GDPR revealed significant gaps that need to be addressed for the banks to comply fully with both international and local regulations, as well as to meet the growing customer expectations for data privacy.

One major finding from the research is the notable absence of a dedicated Data Protection Officer (DPO) in most banks. The GDPR mandates the appointment of a DPO to oversee personal data protection, emphasizing its critical importance in ensuring compliance and fostering a culture of data protection within organizations. The lack of this essential role reflects the nascent stage of data protection awareness and prioritization within Ethiopian banks, indicating a need for greater investment in this area. Additionally, the research identified several weaknesses in security measures currently in place. For instance, many banks have not implemented robust encryption mechanisms to protect data at rest, which leaves sensitive information vulnerable to unauthorized access and potential breaches. Similarly, data transmitted through various applications often lacks SSL/TLS encryption, exposing it to potential breaches during transit and increasing the risk of data interception by malicious actors.

Employee awareness and training were also found to be insufficient across the board. While some banks do provide cybersecurity training, these programs primarily focus on general threats and mitigation techniques, rather than emphasizing the critical importance of personal data protection. As a result, employees often lack a clear understanding of their roles and responsibilities in safeguarding personal data, which can lead to inadvertent mishandling of sensitive information. Another critical gap identified is the absence of a standalone personal data protection policy in most banks. Instead, personal data protection is often treated as a subsection within broader information security policies, which diminishes its emphasis and priority, leading to a lack of dedicated resources and attention to this vital area.

Audit and compliance practices were evaluated, revealing that while some banks are working towards compliance with standards like PCI DSS (Payment Card Industry Data Security Standard) and ISO/IEC 27001 (an international standard for information security

management), none of the banks evaluated were fully compliant with GDPR. The absence of regular audits specifically targeting personal data protection practices exacerbates these shortcomings, as it prevents banks from identifying and addressing vulnerabilities in their data handling processes. Furthermore, third-party management emerged as a significant risk area. Many banks lack adequate oversight and controls for external service providers, leaving personal data exposed to vulnerabilities through insufficiently regulated external entities. This lack of oversight can lead to potential data breaches and compromises in data integrity, further undermining customer trust.

In conclusion, while Ethiopian banks have made notable progress in securing financial data, their current practices for personal data protection require substantial improvements to meet GDPR standards and align with customer expectations. Addressing these gaps through the establishment of dedicated roles, targeted policies, enhanced security measures, and robust training programs will enable banks to achieve compliance and strengthen trust in their data handling practices. Regular audits and improved third-party management are also essential for sustaining these efforts and ensuring continuous alignment with international standards. By prioritizing personal data protection, Ethiopian banks can not only enhance their compliance posture but also foster a culture of accountability and transparency that is crucial in today's data-driven landscape.

RQ2. What are the key components of a comprehensive data protection framework tailored to Ethiopian commercial banks?

During the research conducted, the researcher found that there are major points need to implement the personal data protection on the commercial banks. One of the critical components for protecting personal data within a bank is the assignment of a Data Protection Officer (DPO). The DPO plays a central role in developing and implementing data protection policies, procedures, and guidelines that are essential for maintaining the integrity and confidentiality of customer information. They ensure these policies are enforced across the organization and regularly evaluate employee adherence to them through audits and assessments. Furthermore, the DPO conducts awareness training programs to educate employees about data protection principles and best practices, emphasizing the importance of safeguarding personal data in their daily operations. They also oversee data protection risks, manage data subject requests regarding their personal data, liaise with regulatory authorities,

and report compliance issues to the bank's management, ensuring that the organization remains aligned with legal and regulatory requirements.

Another essential measure for personal data protection is the establishment of independent and comprehensive policies and procedures. These policies should clearly define how the bank collects, stores, uses, and retains customer data, outlining the specific processes involved in each stage of data handling. To ensure transparency and accountability, these policies must be effectively communicated to all stakeholders within the organization, including employees, management, and customers. Regular reviews and updates of these policies are necessary to adapt to changing regulations and emerging threats in the data protection landscape.

Awareness and training programs tailored to personal data protection are equally vital. Employees interacting with customer data should undergo targeted training sessions delivered through various methods such as face-to-face workshops, learning management systems (LMS), brochures, and other mechanisms. These training sessions should cover topics such as data privacy laws, the importance of data security, and the specific responsibilities of employees in protecting personal data. For data processors specifically, dedicated training that focuses on handling personal data securely is crucial to minimize risks, ensuring that they understand the technical and organizational measures in place to protect sensitive information.

The bank must also implement robust security measures that encompass both technical and organizational controls. Technical controls should include data encryption for data at rest and in motion, ensuring that sensitive information is protected from unauthorized access. Role-based access control (RBAC) with the principle of least privilege should be enforced, allowing employees access only to the data necessary for their job functions. Firewalls with intrusion prevention and detection systems (IPS/IDS) should be deployed to monitor and protect the network from potential threats. Data loss prevention (DLP) tools are essential for identifying and preventing the unauthorized transfer of sensitive information. Vulnerability management processes should be in place to regularly assess and address security weaknesses. Secure development practices must be adopted to ensure that any software or applications developed by the bank are designed with security in mind. Additionally, Security Information and Event Management (SIEM) systems should be utilized to provide real-time analysis of security alerts generated by hardware and applications.

Alongside technical measures, organizational and physical controls are imperative. Physical security measures, such as safeguarding data centers and backup libraries, should be in place to protect sensitive locations from unauthorized access and environmental threats. This includes implementing access controls, surveillance systems, and secure entry points. Additionally, secure disposal methods must be applied when personal data is removed from physical or digital storage, ensuring that data is irretrievable and cannot be reconstructed.

By implementing these measures holistically, banks can significantly strengthen their data protection frameworks, ensuring compliance with regulations and safeguarding customer trust. This comprehensive approach not only protects personal data but also enhances the bank's reputation and fosters a culture of security awareness among employees.

RQ3. How can the designed framework be effectively implemented within the operational context of Ethiopian banks?

The research revealed that the successful implementation of the proposed data protection framework largely depends on the readiness and willingness of banks to adopt it. This readiness is not merely a matter of having the right tools or technologies in place; it encompasses a broader cultural shift within the organization that prioritizes data protection as a core value. Encouragingly, most banks demonstrated a high adaptability rate, showing a strong inclination toward adopting advanced data protection frameworks. This adaptability is indicative of a proactive approach to risk management and a recognition of the importance of safeguarding customer information in an increasingly digital world.

This readiness is particularly supported by their prior experience with international compliance standards, such as PCI DSS (Payment Card Industry Data Security Standard) and ISO certifications (International Organization for Standardization), which position them well to transition into personal data protection compliance. These standards have equipped banks with a foundational understanding of compliance requirements and best practices, making the shift to personal data protection less daunting. The familiarity with these frameworks allows banks to leverage existing processes and systems, thereby streamlining the implementation of new data protection measures.

A critical factor identified for successful implementation is strong management commitment. The role of leadership cannot be overstated; it is essential for driving the cultural change

necessary for effective data protection. While the majority of respondents agreed on its importance, a minority highlighted potential leadership barriers that need to be addressed, such as resistance to change and competing priorities. These leadership challenges underscore the need for targeted engagement and advocacy at the executive level to secure the necessary buy-in. Without the active support of top management, initiatives may falter due to lack of resources, insufficient prioritization, or inadequate communication of the importance of data protection across the organization.

Additionally, the research emphasized the pivotal role of employee training and resource allocation in fostering a robust data protection culture. Adequate training ensures that employees are equipped with the knowledge and skills to handle personal data responsibly, aligning their practices with both the framework and regulatory requirements. Training programs should be comprehensive and ongoing, incorporating the latest developments in data protection laws and technologies. Furthermore, resource allocation is critical; organizations must invest in the necessary tools, technologies, and personnel to support data protection initiatives effectively.

Another significant finding was the influence of a strong regulatory framework in guiding banks toward effective data protection practices. Regulations not only set clear compliance benchmarks but also create a supportive environment for the adoption of structured frameworks. The presence of comprehensive and enforceable regulations can accelerate the transition and sustain long-term compliance efforts. Regulatory bodies play a crucial role in establishing guidelines that help banks navigate the complexities of data protection, ensuring that they remain accountable and transparent in their practices.

In conclusion, the combination of bank readiness, leadership commitment, employee training, regulatory support, and previous international compliance experience creates a strong foundation for the successful adoption of the personal data protection framework. Addressing gaps at the leadership and resource levels will further enhance implementation efforts, ensuring alignment with global standards and the expectations of customers and regulators. By fostering a culture of data protection and prioritizing compliance, banks can not only protect sensitive information but also build trust with their customers, ultimately contributing to their long-term success in a competitive landscape.

6.3 Contributions of the Study

This research offers several important contributions to the domain of data protection within the banking industry:

- **Creation of a Customized Framework**: A specialized framework has been developed to tackle the unique data protection issues encountered by Ethiopian commercial banks. This framework presents practical and implementable guidelines that banks can utilize to enhance their data protection measures, ensuring they are more capable of effectively managing sensitive personal and financial data.
- **Connecting Local and Global Standards**: By aligning the proposed framework with the principles of the EU GDPR, the study helps to bridge the divide between current local practices and internationally accepted standards. This alignment not only fosters compliance with global data protection regulations but also boosts the international competitiveness of Ethiopian commercial banks, enabling them to participate more effectively in global banking services.
- **Offering Practical Recommendations:** The study provides actionable suggestions for key stakeholders, including banks, regulators, and policymakers. These recommendations address essential areas such as establishing strong governance frameworks, implementing advanced technological solutions, and improving regulatory oversight. By focusing on these aspects, the research outlines a pathway for developing a secure, efficient, and compliant data protection environment within the banking sector.

6.4 Implications for Practice

The results of this research provide practical and actionable recommendations for Ethiopian commercial banks, allowing them to bolster their data protection practices and align with global standards:

- **Improved Data Governance:** The adoption of the suggested framework will greatly enhance governance structures by defining clear roles and responsibilities, ensuring accountability, and improving oversight of data protection efforts. This organized approach will foster a culture of accountability and transparency in the management of sensitive customer information.

- **Effective Risk Mitigation:** By implementing advanced technical solutions such as robust encryption, role-based access controls, data loss prevention (DLP), intrusion detection systems (IDS), and intrusion prevention systems (IPS), banks can significantly lower the risk of data breaches and unauthorized access. These proactive strategies will protect customer data and strengthen the bank's resilience against cyber threats.
- **Enhanced Regulatory Compliance:** Aligning data protection practices with international standards like the GDPR will ensure adherence to global regulations. This not only reduces legal and financial risks but also builds customer trust and confidence in the banking system, positioning banks as dependable and secure entities in the eyes of their clients.
- **Empowered Workforce:** Regular training and awareness initiatives will provide employees with the knowledge and skills necessary to manage personal data responsibly. By cultivating a thorough understanding of privacy standards and best practices, banks can reduce human error and ensure consistent compliance with data protection policies throughout the organization.

These practical recommendations serve as a guide for Ethiopian commercial banks to improve their data protection framework, achieve regulatory compliance, and create a secure and trustworthy banking environment.

6.5 Limitations of the Study

Although this study provides valuable insights and practical contributions, it has several limitations that should be acknowledged:

- **Narrow Scope of Analysis**: The research mainly concentrates on commercial banks in Ethiopia, which may limit the applicability of the findings to other sectors or regions. Future research could broaden the scope to encompass various industries or international settings to offer a more comprehensive view of data protection practices.
- Potential Bias in Data Collection: The study depends on self-reported data gathered through questionnaires and interviews. This method may introduce biases, such as selective reporting or misinterpretation, and may not fully reflect the complexity of the banks' data protection practices. Including additional data sources, such as audits or case studies, could yield a more thorough analysis.

- Dynamic Nature of Regulations and Technologies: Data protection laws, standards, and technologies are continuously changing. While the proposed framework aims to tackle current challenges, ongoing updates may be required to maintain its relevance and effectiveness. Future research should take into account emerging trends and innovations in data protection to ensure the framework remains flexible over time.

Recognizing these limitations emphasizes areas for further investigation and highlights the necessity for ongoing assessment and adaptation to address the evolving landscape of data protection.

6.6 Recommendations for Future Research

This study provides a foundation for exploring data protection practices in Ethiopian commercial banks, but several avenues for future research could further enrich the field:

1. **Cross-Industry Comparisons**
   Future studies could investigate data protection practices in other sectors, such as telecommunications, healthcare, or e-commerce, to provide comparative insights. Examining how different industries approach data protection can highlight best practices, challenges, and unique considerations that may inform broader frameworks or policies.
2. **Regulatory Impact Analysis**
   Research could assess the effectiveness of regulatory interventions by the National Bank of Ethiopia and other regulatory bodies in enforcing data protection standards. Analyzing how these regulations influence compliance, customer trust, and operational efficiency would provide valuable insights into their impact and areas for improvement.
3. **Role of Emerging Technologies**
   Future research could explore the integration of emerging technologies like artificial intelligence, blockchain, and machine learning in enhancing data protection. These technologies have the potential to revolutionize data security by enabling automated threat detection, secure data transactions, and robust privacy-preserving mechanisms.
4. **Longitudinal Evaluations**
   Conducting longitudinal studies would allow researchers to evaluate the long-term effectiveness and adaptability of the proposed framework. Tracking the implementation

of the framework over time could reveal insights into its sustainability, scalability, and impact on compliance and customer trust.

By addressing these areas, future research can provide deeper and broader insights into data protection practices, fostering innovation and improved compliance across various industries and contexts.

Reference

Abraham, R., Schneider, J., & vom Brocke, J. (2019). Data governance: A conceptual framework, structured review, and research agenda. *International Journal of Information Management*, *49*, 424–438. https://doi.org/10.1016/J.IJINFOMGT.2019.07.008

Aly Bouke, M., Alshatebi, S. H., Abdullah, A., Cengiz, K., & Atigh, H. El. (n.d.). *African Union Convention on Cyber Security and Personal Data Protection: Challenges and Future Directions*.

Anant, V., Donchak, L., Kaplan, J., & Soller, H. (2020). The consumer-data opportunity and the privacy imperative. *McKinsey & Company*, *April*, 1–14.

Azamat, X. (2023). International Journal of Law and Policy | Volume: 1 Issue: 5 2023. *International Journal of Law and Policy*, *1*(5), 1–8.

Baker, W., Goudie, M., Hutton, A., Hylender, C. D., Niemantsverdriet, J., Novak, C., Ostertag, D., Porter, C., Rosen, M., Sartin, B., & Tippett, P. (2010). *Data Breach Investigations Report 2010*. *October*, 1–66.

Baskerville, R., Baiyere, A., Gregor, S., Hevner, A., & Rossi, M. (2018). Design science research contributions: Finding a balance between artifact and theory. *Journal of the Association for Information Systems*, *19*(5), 358–376. https://doi.org/10.17705/1jais.00495

Benedicta Ehimuan, Ogugua Chimezie, Ob, Onyinyechi Vivian Akagha, Oluwatosin Reis, & Bisola Beatrice Oguejiofor. (2024). Global data privacy laws: A critical review of technology's impact on user rights. *World Journal of Advanced Research and Reviews*, *21*(2), 1058–1070. https://doi.org/10.30574/wjarr.2024.21.2.0369

Borghard, E. D. (2018). *Protecting Financial Institutions Against Cyber Threats: A National Security Issue*.

Bradley, S. (2024). *eRepository @ Seton Hall Comparative Analysis of Two Data Privacy Regulatory Schemes : The GDPR and the CCPA Comparative Analysis of Two Data Privacy Regulatory Schemes : The GDPR and the CCPA*.

Byun, D. Y. (2020). Privacy or Protection : The Catch-22 of the CCPA. *Loyola Customer Law Review*, *32*(2), 246–266.

Calder, A., IT Governance (Organization). Privacy Team., European Union., & European Parliament. (n.d.). *EU general data protection regulation (GDPR) : an implementation and compliance guide*.

Creswell, J. W. (2014). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. Sage Publications.

Emmanuel Magnus-Eweka. (2023). *Navigating the Challenges to Digital Transformation The Case of a Pan African Commercial Bank.*

Excel G Chukwurah, & Samuel Aderemi. (2024). Harmonizing Teams and Regulations: Strategies for Data Protection Compliance in U.S. Technology Companies. *Computer Science & IT Research Journal*, *5*(4), 824–838. https://doi.org/10.51594/csitrj.v5i4.1044

Folorunso, A., Wada, I., Samuel, B., & Mohammed, V. (2024). *Security compliance and its implication for cybersecurity Security compliance and its implication for cybersecurity*. *November*. https://doi.org/10.30574/wjarr.2024.24.1.3170

Gashi, F. (2016). *PROTECTION OF PERSONAL DATA AND PRIVACY IN BANKING*. *December 1996*.

Giurgiu, A., & Lallemang, T. (n.d.). *The General Data Protection Regulation: a new opportunity and challenge for the banking sector*.

Govindarajan, V., Srivastava, A., & Enache, L. (2019). How India plans to protect consumer data. *Harvard Business Review*.

Gutwirth, S., Poullet, Y., De Hert, P., & Leenes, R. (2011). Computers, privacy and data protection: An element of choice. In *Computers, Privacy and Data Protection: An Element of Choice*. Springer Netherlands. https://doi.org/10.1007/978-94-007-0641-5

Haile, D. (2024). *E THIOPIA ' S NEW PERSONAL DATA PROTECTION LAW : A S TEP Securing Ethiopia ' s Digital Future : A Path Forward*. *2016*(1321).

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design Science in Information Research 1. *Design Science in IS Research MIS Quarterly*, *28*(1), 75–105.

Hoofnagle, C. J., Sloot, B. van der, & Borgesius, F. Z. (2019). The European Union general data protection regulation: What it is and what it means. *Information and Communications Technology Law*, *28*(1), 65–98. https://doi.org/10.1080/13600834.2019.1573501

Hustinx, P. (n.d.). *"EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation."*

Illman, E., & Temple, P. (2019). California consumer privacy act: What companies need to know. *Business Lawyer*, *75*(1), 1637–1646.

Kinfe Micheal Yilma and Halefom Hailu Abraha. (2015). The Internet and Regulatory Responses in Ethiopia : *Mizan Law Review*, *9*(1), 108–153.

Kitayama, T. and. (n.d.). Japan Personal Information Protection Commission. *2020*.

Md Abdul Ahad Maraj, M. H. M. M. R. M. S. H. (2024). Advancing Data Security in Global Banking: Innovative Big Data Management Techniques. *Global Mainstream Journal*, *1*(2), 26–37. https://doi.org/10.62304/ijmisds.v1i2.133

Ml, A. /, & Zahid, F. (2023). Security and Compliance Aspects of Data Integrity in Banking. In *INTERNATIONAL JOURNAL OF COMPUTER SCIENCE AND TECHNOLOGY (IJCST)* (Vol. 7, Issue 1).

Pardau, S. L. (2018). *THE CALIFORNIA CONSUMER PRIVACY ACT : TOWARDS A EUROPEAN-STYLE PRIVACY REGIME IN THE UNITED Modality-Focused Laws Laws Protecting Children ..... The The Ballot Initiative ..... 89 California Consumer Privacy Act Consumers ? What*.

Rodrigues, G. A. P., Serrano, A. L. M., Vergara, G. F., Albuquerque, R. de O., & Nze, G. D. A. (2024). Impact, Compliance, and Countermeasures in Relation to Data Breaches in Publicly Traded U.S. Companies. *Future Internet*, *16*(6). https://doi.org/10.3390/fi16060201

Serrado, J., Pereira, R. F., Mira da Silva, M., & Scalabrin Bianchi, I. (2020). Information security frameworks for assisting GDPR compliance in banking industry. *Digital Policy, Regulation and Governance* , *22*(3), 227–244. https://doi.org/10.1108/DPRG-02-2020-0019

Shelagh Heffernan. (2005). *Modern Banking* (4th ed.). John Welly & Sont Ltd.

Sion, L., Landuyt, D. Van, & Joosen, W. (2021). An Overview of Runtime Data Protection Enforcement Approaches. *Proceedings - 2021 IEEE European Symposium on Security and Privacy Workshops, Euro S and PW 2021*, 351–358. https://doi.org/10.1109/EuroSPW54576.2021.00044

Štarchoň, P., & Pikulík, T. (2019). GDPR principles in data protection encourage pseudonymization

through most popular and full-personalized devices - mobile phones. *Procedia Computer Science*, *151*, 303–312. https://doi.org/10.1016/j.procs.2019.04.043

Suh, B., & Han, I. (2003). The Impact of Customer Trust and Perception of Security Control on the Acceptance of Electronic Commerce. *International Journal of Electronic Commerce*, *7*(3), 135–161. https://doi.org/10.1080/10864415.2003.11044270

Taherdoost, H., Business, H., Sdn, S., Group, C., & Lumpur, K. (2016). Sampling Methods in Research Methodology ; How to Choose a Sampling Technique for. *International Journal of Academic Research in Management (IJARM)*, *5*(2), 18–27.

Tayyba Jabeen, Yasir Mehmood, Hamayun Khan, Muhammad Fawad Nasim, S. A. N. (2025). *Spectrum of Engineering Sciences*. *3*(1), 143–161.

Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review*, *34*(1), 134–153. https://doi.org/10.1016/J.CLSR.2017.05.015

Uunanen, T. U. T. (2006). *D EVELOPING F EATURE S ETS FOR G EOGRAPHICALLY D IVERSE E XTERNAL E ND U SERS : A C ALL FOR V ALUE - BASED P REFERENCE M ODELING*. 41–55.

Varisco, L., Pavlovic, M., & Pillan, M. (2019). Anticipating Ethical Issues When Designing Services that Employ Personal Data. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *11583 LNCS*, 113–131. https://doi.org/10.1007/978-3-030-23570-3_10

Warikandwa, T. V. (2021). Personal data security in south africa's financial services market: The protection of personal information act 4 of 2013 and the european union general data protection regulation compared. *Potchefstroom Electronic Law Journal*, *24*. https://doi.org/10.17159/1727-3781/2021/v24i0a10727

Weber, S., & Duarte, C. (2022). Advanced Sampling Methods. *Circuit Design*, 253–314. https://doi.org/10.1201/9781003337539-9

Wolff, J., & Atallah, N. (2020). *early gdpr penalties*. *11*(May).

Yadav, N., Pandey, S., & Gupta, A. (2023). *Data Privacy in Healthcare : In the Era of Artificial Intelligence*. https://doi.org/10.4103/idoj.idoj

Yousafzai, S. Y., Pallister, J. G., & Foxall, G. R. (2003). A proposed model of e-trust for electronic banking. *Technovation*, *23*(11), 847–860. https://doi.org/10.1016/S0166-4972(03)00130-5

Appendices

Appendix A: Survey questioner

Personal Data Protection in Ethiopian Commercial Banks

Introduction

Dear Participant,

I am Maereg Seyoum, a Master's student at the Addis Ababa University College of Information Systems. As part of my thesis research, I am conducting a comprehensive study on personal data protection practices in Ethiopian commercial banks.

This questionnaire aims to gather insights into the current state of data protection within the banking sector and identify opportunities for improvement. Your responses will be instrumental in developing recommendations for a robust data protection framework that aligns with international standards, such as the EU General Data Protection Regulation (GDPR).

Your participation is voluntary, and all responses will be treated with the utmost confidentiality. Thank you for your time and valuable contributions.

Sincerely,

Maereg Seyoum

+251911572578

maereg.seyoum@gmail.com

Section 1: General Information

Which department do you work in?

a) IT Department

b) Compliance/Legal

c) Risk Management

d) Operations

e) Other (please specify): _____

What is your job role?

a) Data Protection Officer

b) IT Manager

c) Compliance Manager

d) Risk Manager

e) Other (please specify): _____

How many years of experience do you have in your current role?

a) Less than 1 year

b) 1–3 years

c) 4–6 years

d) 7–10 years

e) More than 10 years

Does your bank currently have a designated Data Protection Officer (DPO)?

a) Yes

b) No

c) I don't know

Questionnaires

	Questions	**Strongly Disagree**	**Disagree**	**Neutral**	**Agree**	**Strongly Agree**
Section 2	Existing Data Protection Practices (RQ1)					
2.1	The current data protection measures implemented by our bank are robust and effective in safeguarding customer information.					
2.2	The security measures implemented by our bank to protect customer data are comprehensive and highly effective.					
2.3	The bank consistently conducts security audits to ensure the highest standards of data protection are maintained.					
2.4	The training provided to employees of our bank on data protection practices is highly effective in equipping them with the necessary skills and knowledge to safeguard sensitive information.					
2.5	Our bank effectively manages third-party vendors who have access to customer data, ensuring compliance with stringent data protection standards.					
Section 3	Key Components of a Data Protection Framework (RQ2)					

	Questions	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
3.1	Regular data encryption is vital for protecting customer data, as it plays a key role in ensuring confidentiality and preventing unauthorized access to sensitive information.					
3.2	Having a dedicated Data Protection Officer (DPO) at our bank is essential for ensuring effective data protection, as it establishes accountability and fosters a culture of compliance with data privacy regulations.					
3.3	Access control measures, such as user authentication, are critical components of our bank's data protection framework, as they safeguard sensitive information by ensuring that only authorized personnel can access it.					
3.4	Regular staff training is crucial for ensuring compliance with data protection policies, as it empowers employees with the knowledge and skills necessary to uphold privacy standards and effectively protect sensitive information.					
3.5	Regular monitoring and audits are highly significant for maintaining data protection standards, as they provide ongoing assessments of our security measures and ensure compliance with established protocols.					
Section 4	Implementation of the Framework (RQ3)					
4.1	Our bank is highly adaptable and ready to implement a comprehensive data protection framework, enabling us to respond effectively to evolving regulatory requirements and industry best practices.					
4.2	Our bank's management is fully committed to implementing robust data protection practices, prioritizing the safeguarding of sensitive information and fostering a culture of privacy throughout the organization.					
4.3	Our bank's employees are highly likely to adhere to data protection protocols when equipped with comprehensive training and the necessary resources, ensuring a strong commitment to safeguarding sensitive information.					
4.4	Regulatory guidelines from authorities, such as the National Bank of Ethiopia, play a crucial role in effectively supporting the implementation of data protection measures, providing a robust framework for compliance and best practices					
4.5	Our bank is fully prepared and committed to aligning with international data protection standards, such as the GDPR, demonstrating a proactive approach to					

	Questions	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
	safeguarding customer information and ensuring compliance with global best practices					

How you can handle if the data breaches or data protection incidents that have occurred in your bank.

_____
_____

Please suggest any components that you think should be included in a data protection framework for Ethiopian banks.

_____
_____

What role do you think external regulators (e.g., National Bank of Ethiopia) should play in helping banks implement data protection frameworks?

_____
_____

What resources (financial, technological, or human) would your bank need to fully implement a comprehensive data protection framework?

_____
_____

Please provide any additional recommendations for successfully implementing a data protection framework in Ethiopian banks.

Appendix B: Interview Questions

Dear Participant,

I am Maereg Seyoum, a Master's student at the College of Information Systems, Addis Ababa University. As part of my thesis research, I am undertaking a thorough investigation into personal data protection practices in Ethiopian commercial banks.

This interview question aims to collect important insights regarding the current state of data protection in the banking sector and to identify potential areas for improvement. Your response for the interview will be instrumental in formulating recommendations for a strong data protection framework that is applicable for Ethiopian commercial banks that meets international standards, like the EU General Data Protection Regulation (GDPR).

Participation is completely voluntary, and all responses will be kept strictly confidential and used exclusively for academic purposes. By sharing your knowledge and experience regarding the subject matter, you are helping to make significant progress in the protection of personal data within Ethiopia's banking system.

The interview session won't take more than 45 minutes.

Thank you for your time, thoughtful responses, and valuable contribution to this significant study.

Sincerely,

Maereg Seyoum

+251911572578

maereg.seyoum@gmail.com

Questions

1. ***Data Protection Officer (DPO)***

- What challenges does your bank face in appointing or maintaining a dedicated Data Protection Officer (DPO)?
- How do you think the role of a DPO could enhance compliance with GDPR-aligned data protection standards in your organization?

Effectiveness of Customer Data Protection Mechanisms

- In your view, what are the most significant weaknesses in the current customer data protection mechanisms at your bank?
- What measures do you believe are necessary to improve the effectiveness of these mechanisms, particularly in line with GDPR?

Security Audits

- How frequently does your bank conduct security audits, and what challenges prevent consistent auditing practices?
- Are there additional steps your organization could take to make audit processes more comprehensive and aligned with international standards?

Employee Training and Awareness

- Why do you think employee training on data protection is perceived as ineffective by some staff?
- What types of training or awareness programs would you recommend to better align employees with GDPR-compliant data protection protocols?

Third-Party Vendor Management

- How does your bank ensure that third-party vendors comply with data protection standards?
- What gaps do you see in the current vendor management strategies, and how can they be improved to ensure GDPR alignment?

Regulatory Guidelines and Support

- Do you believe the National Bank of Ethiopia provides sufficient guidance and monitoring to support data protection efforts? Why or why not?
- What additional support or oversight from regulatory bodies would help your bank achieve better compliance with GDPR-like frameworks?

Data Breach Preparedness

- How prepared is your bank to respond to a data breach, and what areas of the current incident response procedure need improvement?
- What additional steps or tools could be incorporated to strengthen breach detection, containment, and reporting processes?

Budget and Resource Allocation

- In what ways do budgetary constraints impact the implementation of advanced data protection technologies (e.g., encryption, Data Loss Prevention systems)?
- How would you prioritize resource allocation to align your bank's data protection practices with GDPR?

Alignment with International Standards

- What challenges does your bank face in aligning its data protection framework with international standards such as the GDPR?
- Are there specific elements of GDPR compliance (e.g., data minimization, data portability) that are particularly difficult to implement in your bank?

Comprehensive Monitoring and Risk Management

- How effective are your bank's current monitoring and risk assessment practices in identifying vulnerabilities?
- What enhancements do you recommend for achieving more comprehensive and proactive risk management in line with GDPR?

Policy Development and Implementation

- What gaps do you see in your bank's existing data protection policies, and how can these be addressed to meet GDPR standards?
- How effectively are these policies communicated and enforced across different departments in the bank?

Employee Adherence to Protocols

- What are the biggest barriers preventing employees from adhering to data protection protocols?
- How can the bank foster a stronger culture of compliance and accountability among its staff?

Data Encryption and Access Controls

- Do you think the bank's encryption practices and access controls are sufficient to prevent unauthorized access to sensitive data? Why or why not?
- What specific improvements would you suggest to strengthen these technical controls?

Regulatory Development and Enforcement

- What specific measures has the National Bank of Ethiopia (NBE) implemented to ensure that commercial banks comply with personal data protection regulations, particularly in alignment with international standards like the EU-GDPR?

Role of Oversight and Monitoring

- How does the NBE monitor and assess the effectiveness of data protection practices within Ethiopian commercial banks, and what mechanisms are in place to address non-compliance or breaches?

Guidance and Support for Banks

- What kind of guidance, resources, or training does the NBE provide to commercial banks to help them establish and maintain robust personal data protection frameworks?

Incident Response and Reporting

- What are the requirements for commercial banks in Ethiopia to report data breaches or security incidents to the NBE, and how does the regulatory body respond to such incidents to mitigate risks?

Collaboration and Future Improvements

- How does the NBE plan to collaborate with other stakeholders, including international organizations, to enhance personal data protection regulations, and what future initiatives are being considered to strengthen the regulatory framework?

Appendix C: Framework Demonstration Meeting

Meeting Agenda: Artifact Demonstration Session for the Proposed Personal Data Protection Framework

Date: November 29, 2024

Time: 2:00 PM – 2:45 PM

Venue: Microsoft Teams (Virtual)

Attendees: Directors, Managers, Experts, and Specialists

Objective

The session aims to present the proposed Personal Data Protection Framework designed and developed for Ethiopian commercial banks, aligning with the EU GDPR. Attendees are encouraged to provide valuable feedback during the session, which will be instrumental in refining and enhancing the framework.

Agenda and Time Slots

- 2:00 PM – 2:02 PM: *Introduction*
  A brief overview of the research study, its purpose, and the motivation behind the framework's development.
- 2:02 PM – 2:10 PM: *High-Level Framework Presentation*
  A concise presentation of the overarching structure and objectives of the proposed personal data protection framework.
- 2:10 PM – 2:25 PM: *Detailed Framework Presentation*
  An in-depth walkthrough of the framework, covering its components, implementation strategies, and alignment with GDPR standards.
- 2:25 PM – 2:45 PM: *Q&A Session*
  Open floor for attendees to ask questions, share insights, and provide feedback on the proposed framework.

Outcome

By the end of the session, the attendees' feedback will be gathered to fine-tune the framework and ensure its practical relevance and effectiveness for Ethiopian commercial banks.