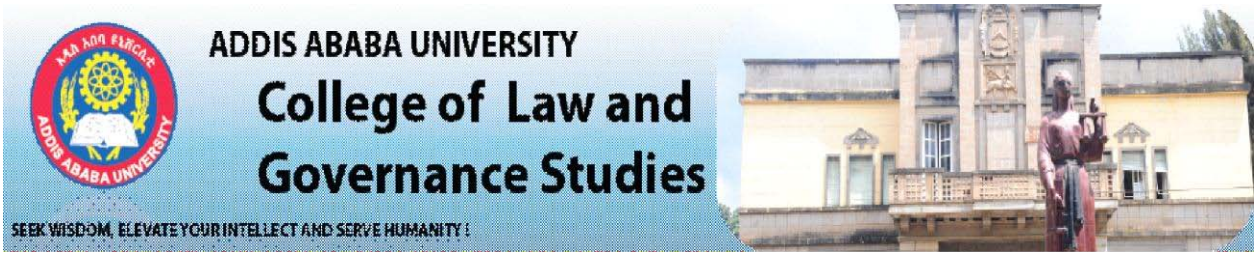


ADDISABABAUNIVERSITY

COLLEGEOFLAWANDGOVERNANCE STUDIES

SCHOOLOF LAW

LLMPROGRAMINBUSSINESS LAW

The Legal Framework for Data Protectionin Digital Financial Services in Ethiopia: The Case of Kacha Digital Financial Services S.C

BY:Nejat Ahmed Wolle

ADVISOR:Dr. Solomon Abay

A THESIS SUBMITTED TO THE SCHOOL OF GRADUATE STUDIES, SCHOOL OF LAW, ADDISABABAUNIVERSITY,INPARTIALFULFILLMENTOFTHEREQUIREMENTSFORTHE MASTEROF LAWS(LLM) DEGREEINBUSINESS LAW.

January, 2025

ADDISABABA

DECLARATIONSTATEMENT

I, Nejat Ahmed, declare that this paper is original and has never been presented inany institution or university. In addition, I also declare that all information used in this study hasbeen dulyacknowledged.

Name:Nejat Ahmed Signature:----------Date:----------

Advisor:Dr. Solomon Abay Signature:----------Date:----------

ADDISABABAUNIVERSITYCOLLEGEOFLAWANDGOVERNANCESTUDIES

SCHOOLOFLAW

GRADUATESPROGRAMSBOARDOFEXAMINERSTHESISAPPROVALSHEET

A thesis of Nejat, titled **"The Legal Framework for data protectionin Digital Financial Services in Ethiopia: The Case of Kacha Digital Financial Services S.C"**is approved bytheundersigned membersofthe examining Board.

Dr. Solomon Abay	----------	----------
Advisor	Signature	Date
_____	----------	----------
Examiner1	Signature	
	Date_____	---
----------	----------	
Examiner2	Signature	Date

Acknowledgement

I express my deepest gratitude to my thesis advisor, Dr. Solomon Abay, for his guidance and support throughout this LLM thesis research process. I am also thankful to my friends, classmates, and family members for creating a stimulating academic environment, providing encouragement, and believing in my abilities. I am deeply indebted to the interview participants who generously shared their knowledge and experiences.

I am genuinely grateful for the invaluable support, guidance, and contributions from everyone involved in this important milestone of my LLM-related research.

Contents

Acronyms

- **ACH** - Automated Clearing House
- **AMF** - Anti-Money Laundering
- **AML** - Anti-Money Laundering
- **API** - Application Programming Interface
- **ATMs** - Automated Teller Machines
- **CBE** - Commercial Bank of Ethiopia
- **CFT** - Countering the Financing of Terrorism
- **DFS** - Digital Financial Services
- **ETATS** - Ethiopian Automated Transfer System
- **FCM** - Firebase Cloud Messaging
- **GDP** - Gross Domestic Product
- **GDPR** - General Data Protection Regulation
- **HPR** - House of People's Representatives
- **HTTPS** - Hypertext Transfer Protocol Secure
- **ICCPR** - International Covenant on Civil and Political Rights
- **KYC** - Know Your Customer
- **M-banking** - Mobile Banking
- **MFI** - Microfinance Institutions
- **MNOs** - Mobile Network Operators
- **NBE** - National Bank of Ethiopia
- **OTPs** - One-Time Passwords
- **PC** - Personal Computer
- **PEPs** - Politically Exposed Persons
- **PII** - Personally Identifiable Information
- **POS** - Point-Of-Sale Transfer Terminals
- **PSS** - Premier Switch Solution
- **RTGS** - Real-Time Gross Settlement System

- **SIM cards** - Subscriber Identity Module Cards
- **SIEM** - Security Incident and Event Management
- **SSH** - Secure Shell
- **TSPs** - Technology Service Providers
- **UDHR** - Universal Declaration of Human Rights
- **USA** - United States of America
- **OTP** - One-Time Password

Abstract

This LLM thesis examines Ethiopia's regulatory landscape for personal data protection, particularly the 2024 Data Protection Proclamation's alignment with DFS practices. Using Kacha as a case study, it evaluates the effectiveness of existing laws and identifies gaps that could hinder personal data protection.

While Ethiopia has made progress in establishing a specific legal framework, the research has identified many gaps, including the ambiguity surrounding generic ambiguous terms, a lack of clarity on user consent, insufficient specificity that leaves room for interpretation, a lack of awareness among data consumers, and the absence of defined norms for data processing methods that prevent adequate consumer privacy protection in DFS. This situation requires legislative revision suited to the specific difficulties of DFS and the implementation of more consumer programs.

Additionally, it is admirable that the proclamation establishes a body overseeing organizations with previous functions. However, the researcher has recommended that instead of relying on an authority with pre-existing, more general responsibilities, a specialized organization for the protection of personal data be created to provide targeted, ongoing, and efficient oversight.

Though the findings of the research show that Kacha is making efforts to be dedicated to regulatory compliance and make mobile money services safe, critical issues were identified such as ambiguities in obtaining customer consent, lack of DPO, a lack of transparency in data handling practices during the complaint resolution process, burden on data subjects for data breaches, hierarchical and locational data management issues and the need for more straightforward guidelines and greater transparency in both company policies and the overarching regulatory framework. These concerns highlight the significance of making the practice align with the law.

The Legal Framework for Data Protection in Digital Financial Services in Ethiopia: The Case of Kacha Digital Financial Services S.C.

Chapter one

1. Introduction

1.1 Background of the study

The digital financial sector has transformed through the integration of information technology, driving the digitalization of services. Alternative channels such as internet banking, ATMs, and mobile banking (m-banking) have gained prominence.[1]

DFS has experienced significant global growth, including in Ethiopia. The launch of ATMs by the Commercial Bank of Ethiopia in 2001 marked the beginning of e-banking. In 2010, Zemen Bank pioneered internet banking services and established the Premium Switch Solutions consortium in 2012, enhancing interconnectivity among banks. The NBE's mandate for core banking processes and automation in 2011 facilitated widespread adoption. [2]

In 2020, the NBE introduced a directive that allowed non-traditional financial institutions to issue payment instruments. This directive expanded the range of services to include cash transactions, money transfers, bill payments, and microfinance products. Replacing the 2012 directive on mobile and agent banking services, the new directive introduced licensing and capital requirements. Moreover, it created opportunities for foreign investors to participate in Ethiopia's payment services sector, fostering financial inclusion, competition, and innovation within the industry. [3]

---

[1]Sakala, L., &Phiri, J. (2019) 'Factors Affecting Adoption and Use of Mobile Banking Services in Zambia Based on TAM Model' (2019) 7 Open Journal of Business and Management 1380-1394.

[2]Ababu, B. 'Regulation of Electronic Banking in Ethiopia: The Analysis of Legal Framework' (LL.M. dissertation, Addis Ababa University College of Law and Governance Studies, School of Law, June 2019).

[3]Aman and Partners, 'Reflection on the New Payment Instrument Issuers Directive', Monthly Issue <https://www.aaclo.com/insight/reflection-on-the-new-payment-instrument-issuers-directive/> accessed on 20 April 2023.

Ethiopia's mobile money service landscape currently consists of three licensed providers: Telebirr, a government-owned service; M-Pesa, a foreign company; and Kacha, the first private Ethiopian payment instrument issuer. Kacha's presence as a private entity reflects domestic players' growing interest and participation. With these three providers, Ethiopia offers a diverse range of options for digital payments, contributing to the expansion and development of the country's digital financial ecosystem.

Regarding operational mechanisms, Telebirr exclusively operates through Ethio Telecom SIM cards, while M-Pesa functions solely with Safaricom SIM cards. Conversely, Kacha works using both Ethio Telecom and Safaricom SIM cards. Consequently, it must implement additional security measures to protect data from both types of SIM cards, necessitating enhanced security protocols to ensure the safety and confidentiality of user information across multiple SIM card platforms.

The financial services sector is often recognized as particularly vulnerable to cybersecurity breaches, with this risk further amplified in the mobile money industry due to the increased usage of mobile devices. Therefore, data security is acknowledged as a crucial aspect of building trust and ensuring the continued growth and sustainability of mobile money services. Mobile money providers must implement robust security measures to safeguard against cyberattacks, preserving advancements in financial inclusion and facilitating further growth. Ethiopia had fragmented data protection legislation across various legal regimes to support this. However, in 2024, a new data protection regulation was enacted.

This thesis examined data protection regulation in Ethiopia's DFS sector, focusing on Kacha's practices. It evaluated how Kacha protects customer data and privacy while advancing digital transactions. The thesis explored the opportunities and challenges of Ethiopia's newly approved data protection proclamation. It contributes to understanding the regulatory landscape in Ethiopia's digital payment ecosystem. It aims to inform policymakers and stakeholders in fostering a more secure and privacy-conscious environment for digital financial transactions.

1.2 Statement of the Problem

The financial services industry is becoming increasingly digital. Over the last 50 years, tremendous technological transformation has radically changed the frontiers of human potential, enabling significant increases in productivity, new scientific advancements, and the formation of new communities and societal divisions.[4]

While the current legal frameworks for digital finance service providers in Ethiopia include licensing requirements, regulatory oversight, consumer protection measures, and compliance provisions, it is still unclear whether these frameworks adequately address customer privacy and data security concerns.

Despite the growing importance of privacy and data protection in digital finance, there is a lack of understanding about the privacy and data security practices of digital financial service providers in Ethiopia. This knowledge gap hinders the development of frameworks, compliance with regulations, consumer trust, and incident response capabilities. An evaluation is needed to identify strengths and areas for improvement and to develop best practices for a secure digital banking ecosystem in Ethiopia.

Furthermore, the recent enactment of the data protection proclamation No. 1321/2024 introduces a new legal framework for data protection in Ethiopia. It presents comprehensive regulations and requirements for collecting, storing, processing, and transferring personal data. However, evaluating the implementation capacity of DFS providers concerning this proclamation is essential. Specifically, it is necessary to understand how it enhances the privacy and security of digital financial transactions and how the proclamation will address the challenges they face in ensuring data protection.

Furthermore,limitedresearchexiststhatevaluatestheimpactofthedataprotectionlawondigital finance in Ethiopia and its effectiveness in mitigating privacy and security risks. It is crucial to examinetheextenttowhichthelawalignswiththepractices,consider the unique characteristics of digital finance, and provide sufficient guidance for service providers to comply with data protection requirements.

By focusing on Ethiopia's newly enacted data protection law and its implications for DFS, this

[4] Henri Arslanian and Fabric Fisher, The Future of Finance, PalgarveMacmillian , (2019) page 3

study aims to evaluate the law's effectiveness in addressing customer data protection challenges in the digital financial sector. The research assesses the practical implementation of the law, identifies gaps and areas for improvement, and proposes measures to enhance compliance and strengthen data protection practices. The findings will contribute to the development of a strong legal and regulatory framework for data protection in Ethiopia's digital financial sector, fostering a secure and trustworthy customer environment and promoting adherence to the practice.

1.3 Research Objectives

General Objective

Critically analyze the legal framework for data protection in digital finance in Ethiopia, focusing specifically on the data protection proclamation No. 1321/2024 and the case of Kacha DFS S.C., and propose measures to enhance privacy and data protection practices.

Specific Objectives

1. Evaluate the effectiveness of the current legal framework and regulations regarding data protection for DFS providers in Ethiopia, with a specific focus on Kacha, in ensuring the protection of customer data.
2. Evaluate Kacha's data protection practices, assessing their capacity to implement data protection regulations and identifying strengths, weaknesses, and areas for improvement.

1.4 Research Questions:

1. Whether and to what extent do current Ethiopian laws protect personal data privacy in the context of flourishing DFS providers in Ethiopia?
2. What are Kacha's data protection practices, and how can they be enhanced?

1.5 Research Methodology

The study employed a mixed-methods approach, combining Doctrinal and non-doctrinal methods. The researcher collected, analyzed, and interpreted the relevant provisions of the new data protection proclamation and other applicable laws and regulations provided by the NBE in light of DFS providers and data protection.

In addition to understanding how DFS providers acquire, process, safeguard, and transfer personal data and how they handle the new data protection regulation, the researcher has

analyzed Kachas's privacy statement by examining its policy and procedures, website, and terms as a primary data source.

The researcher also interviewed stakeholders, including management, relevant staff members, and customers, to clarify and address the research questions. These qualitative methods provided valuable insights into Kacha's specific data protection practices, challenges, and successes.

Kacha, Ethiopia's first private payment instrument issuer, is selected as the primary subject of analysis. It distinguishes itself from Telebirr and M-Pesa due to its unique operational model. Unlike Telebirr and M-Pesa, which operate exclusively through SIM cards owned by their respective telecom companies, Kacha operates via SIM cards owned by other companies. This distinction presents unique challenges for Kacha regarding technical integration, security measures, and interoperability. It implements additional security measures, such as authentication protocols, data encryption, fraud prevention mechanisms, and risk management strategies, to address these challenges. Investigating these security measures offers insights into Kacha's efforts to ensure transaction and user data integrity and security. Understanding the specific security measures adopted by Kacha enhances the broader understanding of secure digital payment practices in Ethiopia.

Analyzing Kacha, Ethiopia's first private payment instrument issuer, provides insights into the implications of private sector participation in the country's financial landscape. It helps understand the unique challenges and opportunities for local players in Ethiopia's digital payment sector. Additionally, studying Kacha sheds light on the regulatory environment governing DFS providers, promotes local innovations and advancements in Ethiopia's digital payment sector, highlights local players' contributions to the economy and financial inclusion efforts, and offers valuable insights into aligning local innovations with national development goals.

1.6 Significance of the Study

This thesis examinesKacha's role and impact, focusing on privacy and data protection considerations. As the digital payment landscape in Ethiopia continues to evolve, understanding the practices and regulatory environment surrounding private sector players is essential for informing the development of legal and policy frameworks.

Examining Kacha's operations offers valuable insights into the privacy and data protection measures adopted by local players in the digital payment sector. By exploring Kacha's infrastructural and operational protocols, this thesis contributes to a more thorough understanding of secure digital finance practices within the Ethiopian context.

Furthermore, this thesis sheds light on Ethiopia's regulatory environment governing digital financial service providers. Analyzing licensing requirements, compliance obligations, and consumer protection measures concerning privacy and data protection offers essential insights into the legal and policy landscape. These findings can guide the creation of tailored regulatory frameworks that foster innovation while protecting user privacy and data security within the digital payment ecosystem.

The significance of this thesis lies in its ability to bridge the gap between the practical realities of Ethiopia's digital finance industry and the evolving legal and policy considerations. This research serves as a valuable resource for legal scholars, practitioners, and policymakers aiming to foster a secure and privacy-conscious digital financial environment in Ethiopia by providing a detailed analysis of Kacha's role and impact. The insights gained from this study can inform future policy decisions and influence the legal landscape surrounding digital payment services in the country.

1.7 Literature Review

Literature on this issue is limited, and most existing publications are outdated for this research paper: either difficult to obtain or requiring payment for access, and either outdated or irrelevant to the research topic, often alleging a lack of legal infrastructure in the country and emphasizing the importance of a strong legislative framework to secure consumers' data, especially as DFS grow in Ethiopia.

In his work, Kinfe Michael discusses Ethiopian data privacy law and practice. International Data Privacy Law examines Ethiopia's constitutional safeguards for privacy, highlighting the flaws in existing laws and monitoring techniques that erode private rights. While the Constitution has strong privacy protections, a specific, comprehensive data protection statute is identified as a key deficiency in the legal structure. Yilma supports the development of a complete legislative

framework that addresses the acquisition, retention, and exchange of personal data, particularly in light of the growing concerns over data privacy in the digital era.[5]

In their article "Ethiopia Diagnostic Review of Financial Consumer Protection: Key Findings and Recommendations," Popovič, A., and others identify Ethiopia's fragmented approach to data protection, emphasizing the lack of a dedicated legal framework specifically for privacy and data protection. The research states that, while some sectoral legislation exists, it is insufficient to handle the difficulties of data privacy, particularly in industries such as finance, where large volumes of personal data are collected and exchanged without necessary customer consent. This lack of monitoring necessitates more stringent privacy legislation, and the authors suggest implementing a general data protection law that extends beyond financial services. [6]

In his article "Towards Data Protection Law in Ethiopia," A. Enyew contends that Ethiopia's current legislative frameworks are insufficient to address the difficulties posed by expanding ICTs, which increasingly threaten privacy. The author points out that, at the time, a law was being developed but had not yet been passed. The lack of a defined legal framework exposed consumers to privacy violations, particularly in the banking sector, where digital financial services became more common. Enyew underlines the importance of formal law in addressing these concerns and safeguarding customer data. [7]

MetagesTewabe's article "Legal Space for the Creation and Operation of Fintech in Ethiopia" in the Bahir Dar University Journal of Law critiques Ethiopia's fragmented regulatory environment, particularly in the fintech sector, where the legal framework is narrow and fails to address critical areas such as digital lending and data protection. The author observes that an outdated legislative structure impedes the rapid expansion of the fintech sector, exposing consumers to risks

[5]KinfeMichealYilma, Data privacy law and practice in Ethiopia, *International Data Privacy Law*, Volume 5, Issue 3, August 2015, Pages 177–189, https://doi.org/10.1093/IDPL/IPV008 accessed December 1, 2024.

[6]Popovič A, Boeddu G, Thorburn C, Traversa M, and Zanza A,*Ethiopia Diagnostic Review of Financial Consumer Protection: Key Findings and Recommendations* (2017) 1–74.

[7]Enyew A, 'Towards Data Protection Law in Ethiopia' in Carlo Baldi (ed), *Data Protection in Africa: A Comparative Perspective* (Springer 2016) 143–159 https://doi.org/10.1007/978-3-319-47317-8_7 accessed on December 1, 2024.

associated with data exploitation. Tewabe advocates for a flexible and adaptive regulatory approach that protects consumers while allowing for innovation in the fintech field.[8]

These findings share a common theme: before the 2024 Data Protection Proclamation, Ethiopia's legal landscape lacked a comprehensive and coordinated approach to data protection. While the literature continually calls for the establishment of such a regulatory framework, it was evident that data protection was an increasing concern, particularly as DFS gained traction.

The 2024 Data Protection Proclamation is a significant step toward addressing these concerns. However, since much of the evaluated literature predates the proclamation's implementation, it focuses on the need for a comprehensive legal framework rather than assessing the new law's effectiveness. Furthermore, given the scarcity of research on the subject, the full consequences of the proclamation, particularly concerning DFS, remain largely unknown. The effectiveness of the 2024 Data Protection Proclamation and its application in the digital financial services sector have yet to be thoroughly analyzed. It is critical to examine whether the legal requirements are being successfully enforced and whether the law effectively addresses the significant challenges posed by data privacy in a rapidly growing digital economy.

This study will be distinct from previous studies in that it will evaluate Ethiopia's legal framework for data protection in the context of DFS providers, particularly emphasizing the recent data protection proclamation. It will also investigate the practice of data protection in DFS providers, focusing specifically on Kacha Digital Financial Services, its compliance with the legislative framework, challenges, and next steps.

1.8 Scope and Limitations

Scope

The study focused on the legal frameworks of data protection practices of DFS providers in Ethiopia, with a specific focus on Kacha, and comparatively analyzed the alignment of the law and the practice.

[8]MetagesTewabe, 'Legal Space for the Creation and Operation of Fintech in Ethiopia' (2023) 13(2) *Bahir Dar University Journal of Law* 323–362.

The study employed a mixed-methods approach, combining Doctrinal and non-doctrinal methods. The researcher collected, analyzed, and interpreted the relevant provisions of the new data protection proclamation and other applicable laws and regulations provided by the NBE in light of DFS providers and data protection.

To understand how DFS providers acquire, process, safeguard, and transfer personal data, as well as how they are addressing the new data protection proclamation, the researcher analyzed Kachas' privacy statement, examining its policy and procedures, website, and terms as primary data sources. The researcher also interviewed stakeholders to elaborate on and address the research questions, which provided valuable insights into Kacha's specific data protection practices, challenges, and successes.

Moreover, the researcher reviewed relevant literature, including books, journals, unpublished materials, and online sources. Finally, the research analyzed the data derived from the aforementioned primary and secondary sources using content analysis.

Limitations

This LLM thesis faced several limitations. One of the main limitations is the lack of adequate local literature on DFS providers and data protection regulation. Even the literature that could be found is inaccessible. Finding specialized lawyers, key personnel, and policies is also tricky. In addition, the findings are specific to Ethiopia and may not be directly applicable elsewhere, given the dynamic nature of privacy regulations and industry cooperation. Technological advancements and regulatory changes could also render certain aspects outdated.

Enacting the new data protection proclamation close to the thesis submission required restructuring. Obtaining primary data was challenging due to unwilling interviewees and the unavailability of relevant documents and data from the company under investigation.

1.9 Organization of the study

The research will be divided into four chapters, with the current segment being one of them. The second chapter will provide an overview of digital financial services and data protection. The third chapter will examine Ethiopian legal frameworks regarding data protection, including case studies of Kacha, insights from stakeholder interviews, and document evaluations. The data analysis section will scrutinize the collected data, leading to the presentation of key findings. The paper concludes with final remarks and recommendations.

Chapter two

2 Digital Financial Services and Data Protection: Unpacking the Intersection of Privacy, Security, and Regulation

This chapter examines the evolution of DFS, emphasizing its definition, various forms, and the benefits it offers, especially regarding financial inclusion. It also discusses the crucial importance of data protection, highlighting the risks of data breaches, fraud, and identity theft, as well as the necessity for strong security measures to foster customer trust and ensure the secure management of sensitive financial information.

2.1 Evolution of DFS

The banking sector has transformed with the integration of information technology, driving the digitalization of services in response to evolving trends, customer needs, and market dynamics. Consequently, alternative channels such as internet banking, ATMs, and mobile banking (m-banking) have gained prominence.[9]

The digitization of banking encompasses a wide range of services, such as converting documents into digital format, utilizing electronic signatures, providing online trading platforms, and facilitating mobile payments to improve customer service, optimize internal processes, and maintain competitiveness. [10]

The evolution of electronic banking began in the 1970s with the rise of computerization, but its immediate impact on clients became clear in the 1980s with the introduction of ATMs. Advancements in telecommunications and information technology fueled banking innovation, leading to the creation of automated voice response (AVR) technology in the early 1990s, which enabled telephone banking. Banks gradually expanded their services to include customer-owned PCs using proprietary software, initially catering to business clients. A significant milestone occurred in 1995 with the introduction of Security First Network Bank in the United States, the

[9] Factors Affecting Adoption (n 1) 1380.

[10]MaghsoudAmiri and others ‘Evaluation Of Digital Banking Implementation Indicators And Models In The Context Of Industry 4.0: A Fuzzy Group Mcdm Approach’ [2023] Article *In* Axioms 10

world's first online bank, which was followed by internet banking services from major institutions such as Citibank and Bank of America. [11]

i. Digital Finance: Definition, forms and benefits

DFS includes the online operations of banks, providing customers with a variety of services that were traditionally confined to physical bank branches[12]by utilizing various types of technology, such as internet banking and mobile banking. [13]

It is also defined as "Digital Banking services that we make available to customers who accept this Agreement and enroll in our Consumer Online Banking, Business Online Banking, and Mobile Banking Channels. Digital Banking also includes services that are available within one or more Channels after additional enrollment and acceptance of Related Documents." by the Commerce Bank of Oregon.[14]These services include tasks such as accessing bank statements, withdrawing cash, transferring funds, managing checking and savings accounts, opening new accounts, handling loans, making bill payments, managing checks, and monitoring transaction records.[15]

ii. Forms of DFS

DFS can take different forms that enable users to conduct transactions at their own convenience, regardless of location or time.[16]

a. **ATM:** ATMs are electronic terminals that allow consumers to perform various banking transactions, including cash withdrawals, deposits, and fund transfers, requiring an ATM card and PIN for access.

---

[11]Ayana Gemechu 'Adoption of Electronic Banking System In Ethiopian Banking Industry: Barriers And Drivers' (Degree Of Master Of Science In Accounting And Finance thesis, Addis Ababa University, School Of Business And Public Administration, 2012) 11

[12]'What Is Digital Banking? Meaning, Types and Benefits' https://sdk.finance/what-is-digital-banking/What is a digital bank? Accessed April 3, 2024

[13] Evaluation of Digital Banking (n 11) 10

[14] The Commerce Bank of Oregon A division of Zions Bancorporation, N.A., Member FDIC, Digital Banking Service Agreement (Consumer & Business) (Version January 2022)

[15] What Is Digital Banking? (n 13)

[16] Adoption of Electronic Banking (n 12) 11

b. **POS:** The system enables consumers to make retail purchases using a debit card, where the funds are transferred directly from the cardholder's account to the store's account. This card resembles a credit card, but with a significant difference.[17]
c. **Internet Banking** is a system that enables bank customers to conduct transactions through personal computers, using web technology to access a wide range of banking services remotely.[18]
d. **Mobile Banking:**This service enables customers to perform banking services such as checking account balances and transferring funds using short text messages (SMS) on their mobile phones.[19]It is offered by banks and financial institutions and allows customers to conduct financial transactions remotely using mobile devices with a SIM.[20]
e. **Mobile money** is a payment service conducted through a mobile device's digital wallet linked to the user's phone number, operating within a financial regulatory framework to enable peer-to-peer transfers, merchant payments, and cash withdrawals.[21]

This service has been enabled by widespread mobile technology use and high phone penetration, with innovative business models supporting the first wave of DFS, exemplified by M-Pesa in Kenya. This has led to 850 million registered mobile money accounts across 90 countries, with daily transactions of $1.3 billion, particularly in Sub-Saharan Africa, where 21% of the population has a mobile money account. It serves as a foundation for advanced financial services like digital lending and insurance. [22]

They provide functionalities like money transfers, receipts, and mobile payments through mobile phones. They aim to serve the unbanked by establishing agent transaction points outside of traditional banking outlets. The agent network exceeds formal service outlets to ensure broad accessibility.[23]

---

[17] ibid

[18] Adoption of Electronic Banking (n 12) 11

[19] Ibid

[20]equbamariamkidaneasegu, *'The limits of electronic banking regulation in Ethiopia' (*Editions universitaireseuropeennes 2018)21

[21] Ibid 22

[22]CeylaPazarbasioglu and others, *Digital Financial Services* (World Bank Group, April 2020)13

[23] GSMA, *Mobile Money in Ethiopia: Advancing Financial Inclusion and Driving Growth* (June 2023) 76

iii. Significance of DFS

DFS leads to cost savings for banks, enhances usability, enables personalization, and provides unique features such as cryptocurrency purchasing and customizable security settings, thereby improving the overall banking experience. [24]

Access to affordable financial services is crucial for poverty reduction and economic growth. Developed financial systems can allocate capital and risks more efficiently, leading to higher economic growth, reduced poverty, and decreased income inequality. At the micro level, financial inclusion reduces poverty and improves lives by facilitating daily transactions, government transfers, remittances, and savings. This enables investments and provides resilience against shocks, serving as the first step towards accessing a broader range of financial services, including savings, insurance, and credit. [25]

DFS have emerged from technological and business model innovations, allowing them to lower costs, increase speed, transparency, security, and availability of tailored financial services for the poor at scale, as digitization reduces frictions across various economic processes, with low marginal costs per account or transaction enabling efficiencies of scale and cost reduction, while enhancing transparency through data trails that can contribute to credit-scoring mechanisms for informal market participants.[26]In addition, mobile money specifically offers accessibility, security, convenience, and versatility, making it a convenient and inclusive tool for managing finances.[27]

iv. Challenges in DFS sector

The expansion of DFS poses several challenges that require attention, including data governance, cybersecurity, operational risks, financial integrity, regulatory arbitrage, macro-financial risks, and fair competition. Data protection frameworks are needed to safeguard consumer data, while cybersecurity and operational risks can threaten the stability of DFS infrastructure. Upholding

[24] What Is Digital Banking? (n 13)

[25]*Digital Financial Services* (n 24) 13

[26]*Digital Financial Services* (n 24) 13

[27]Unveiling the Power of Mobile Money (n 19)

financial integrity is crucial to counter illicit activities, and regulatory arbitrage along with gaps in legal frameworks can introduce risks related to stability, integrity, and consumer protection. [28]

The sector faces significant vulnerability to cyber breaches, as mobile devices and customer mobility contribute to increased risks of data breaches in mobile money services. Recognizing data security as vital for building trust and sustaining mobile money growth, the industry knows that a loss of consumer trust can result in declining market share and hinder the adoption of financial access-enhancing technology advancements. Additionally, non-compliance with data protection laws in the event of breaches poses an additional risk for DFS providers, underscoring the importance of security measures.[29]

The widespread adoption of digital finance has been hindered by a lack of user trust, primarily due to concerns around data protection. Customers are hesitant to embrace digital banking services because the sensitive nature of financial transactions makes them wary of the security and privacy risks involved. This perceived risk is a significant obstacle, and to drive greater adoption, digital banking providers must address and mitigate these trust issues to build user confidence in the system.[30]

2.2 Personal data, security, privacy, and their regulation

DFSs, which collect significant amounts of personal and non-personal data, rely on security measures to prevent data breaches and safeguard customer information. Personal data has evolved into a major resource over time. Many researchers describe it in various ways to convey its significance in contemporary society. Personal data is referred to as a commodity, property, and precious commodity. It is described as the "new oil" of information and digital civilization. [31]

[28] *Digital Financial Services* (n 24) 18

[29] *Data Protection in Mobile Money* (n 4) 6.

[30] Kinana Ahmad Jammoul, 'Online Banking Operations Management: Security Concerns on Trust in Mobile Banking System' (Degree of Doctor of Philosophy, Brunel Business School Brunel University, London, United Kingdom 2016)

[31] Lloyd,IJ, Information technology law, (Oxford University Press 2014) P 22

Data security includes both physical and logical security measures that protect against unauthorized access, loss, modification, or destruction of personal data, thereby reducing privacy violations and potential financial harm. [32]

As per article 6(2) of the new data proclamation of Ethiopia data is defined as:
"information that: is being processed by means of equipment operating automatically in response to instructions given for that purpose, (b) is recorded with the intention that it should be processed by means of such equipment mentioned in lit. (a),(c) is recorded as part of a filing system or with the intention that it should form part of a filing system, or (d) does not fall within lit. (a), (b) or (c) but forms part of any other accessible public record;"
In addition, as per article2 (17) of the proclamation personal data is defined as "any information relating to an identified or identifiable natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;"
Further, the proclamation defined personal data breach as "breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed;"
In the provision of mobile money services, the collection of personal data is essential to meet regulatory requirements such as KYC and Anti-Money Laundering/Countering the Financing of Terrorism (AML/CFT) provisions. [33] Mobile money providers gather various types of personal data, including identity information, transactional history, and location data, to ensure compliance and enable the delivery of financial services.[34] However, responsible data usage is paramount to maintaining consumer trust and protecting individuals' control over their personal information. Some governments in developing countries are recognizing these concerns and

[32]*Data Protection in Mobile Money* (n 4)) 6

[33]*Ibid*, 5

[34] Ibid, 2

considering the establishment or revision of data protection laws to safeguard citizens' privacy rights.[35]

Regarding mobile money security, encryption techniques and multi-factor authentication measures are employed to safeguard user funds and ensure secure access to digital wallets. Strong encryption helps protect sensitive information stored within the digital wallet, making it difficult for unauthorized individuals to access and interpret. Multi-factor authentication requires users to verify their identity through multiple independent factors, such as passwords, mobile devices, or biometric data, adding an extra layer of security.[36]In addition, DFS providers must establish effective organizational data governance mechanisms to protect personal data and mitigate the risks of cyber breaches, which helps build trust and confidence among users, thereby promoting the overall growth and sustainability of the industry.[37]

While consent from the data subject is generally regarded as the most common lawful basis for data processing, relying solely on consent may prove less effective in mobile money services targeting underserved populations. Users in these contexts might have limited knowledge or understanding of data privacy and face barriers when additional steps or requirements are necessary to access these services. Therefore, mobile money providers must balance regulatory compliance and user accessibility, taking into account the specific needs and circumstances of their target populations. [38]

To enhance DFS, key measures include prioritizing data protection and privacy regulations, establishing conducive legal frameworks, adopting payment systems laws, implementing comprehensive e-money insurance, enabling non-banks as DFS providers, simplifying customer due diligence, developing consumer protection frameworks, establishing widespread agent networks, and prioritizing security controls against cyber-attacks. Mobile money providers must

[35] ibid

[36]Unveiling the Power of Mobile Money (n 19)

[37]*Data Protection in Mobile Money* (n 4) 2

[38] ibid

develop organizational policies, incident response plans, and appoint a responsible individual to oversee implementation. [39]

2.3 Evolution of DFS in Ethiopia

In response to the changing technological landscape and customer demands, Ethiopia's banking sector has embraced e-banking. The NBE has mandated the implementation of core banking technologies in all commercial banks, resulting in the introduction of various e-banking products and services by both private and government-owned banks. This modernization effort includes the establishment of the Ethiopian Automated Transfer System (ETATS), which interconnects bank branches through core banking systems. [40]

Under the NBE's mandate, the ACH system has been established for electronic check clearing as part of the RTGS. This system enables electronic credit clearing for high-volume, low-value interbank payments, such as salaries and utility expenses. Furthermore, the NBE has promoted the development of inter-bank retail payment card switches to enhance the card-based transaction infrastructure in Ethiopia. [41]

Two prominent inter-bank retail payment card switches operate in Ethiopia. EthSwitch, a Visa-based domestic transaction switch, ensures interoperability of e-banking products and services, allowing customers to access financial services through any ATM and POS terminal in the country, regardless of their home bank. Another card switch, the Premier Switch Solution (PSS), is owned by a consortium of six banks and facilitates interbank card transactions specifically among its member banks. The NBE provides final settlement services to switch members through a "Payment and settlement account" held at the National Bank. [42]These initiatives are designed to modernize the payment and settlement systems in Ethiopia.[43]

In parallel with the NBE's efforts, individual banks have made significant strides in offering e-banking services to meet customer needs. The Commercial Bank of Ethiopia (CBE) introduced

[39] *Data Protection in Mobile Money* (n 4) 7

[40] *The limits of electronic banking (n 22)*12

[41] Ibid 13

[42] *ibid*

[43] *Ibid*, 14

ATM services in 2001, but due to infrastructure limitations, it initially struggled to utilize its Visa membership fully. In contrast Dashen Bank, emerged as a pioneer in e-payment systems and has remained a primary player since 2006. They have strategically placed ATMs in convenient locations, expanded their card offerings, and even introduced mobile commerce in partnership with technology companies.[44]Other banks, such as Wegagen Bank and Zemen Bank, have also made progress in e-banking by implementing payment system solutions, developing ATM networks, and providing internet banking services. Zemen Bank pioneered internet banking services in 2010 and established the Premium Switch Solutions consortium in 2012, enhancing interconnectivity among banks. The NBE's mandate for core banking processes and automation in 2011 facilitated widespread adoption. [45]

Additionally, collaborative efforts have been noted in Ethiopia's banking sector. For instance, Awash International Bank, Nib International Bank, and United Bank established the Fettan ATM network, aiming to install numerous ATMs and POS terminals nationwide.[46]These advancements, from implementing core banking technologies to introducing ATMs, online banking, mobile commerce, and interconnectivity among banks, highlight the remarkable progress of e-banking in the country.[47]

Financial inclusion is a key priority for Ethiopia, and significant progress has been made through the National Financial Inclusion Strategy. Established in 2016 and refreshed in 2020, the strategy aims to provide affordable financial services to individuals and businesses. However, Ethiopia still lags behind its East African neighbors in formal financial inclusion, with fewer than half of adults having bank accounts. To address this, the strategy targets increasing financial inclusion from 46% to 70% of adults by 2025, focusing on scaling digital payments through mobile money services. The recent liberalization of the telecom sector allows non-banks, including mobile network operators, to offer mobile money services, drawing inspiration from successful

[44] Adoption of Electronic Banking (n 12) 12

[45] Regulation of Electronic Banking (n 2)

[46]Adoption of Electronic Banking (n 12) 13

[47]ibid14

implementations in other parts of Sub-Saharan Africa. The goal is to raise digital payment usage from 20% in 2020 to 49% by 2025. [48]

Since 2016, significant improvements have been made in Ethiopia's financial inclusion. Owning a transaction account, which includes deposit accounts, credit accounts, and mobile money wallets, is considered a fundamental aspect of financial inclusion. The number of transaction accounts per 100 adults has increased substantially, growing by approximately 2.4. There is an average of 159 transaction accounts per 100 adults, compared to a baseline of 68.27 in 2015. This indicates a substantial increase in individuals' access to financial services in Ethiopia, reflecting progress in expanding financial inclusion. [49]

In 2020, the Ethiopian government liberalized the telecoms sector, allowing non-banks, including mobile network operators (MNOs), to offer mobile money services. This decision was influenced by the success of MNOs in other parts of Sub-Saharan Africa in increasing financial inclusion through mobile money. By leveraging the potential of mobile money services, Ethiopia aims to overcome barriers to financial inclusion and drive greater access to DFS for its population. Ethiopia has made remarkable progress in enhancing financial inclusion and access to banking services. The number of transaction accounts per 100 adults has grown by approximately 2.4, averaging 159 accounts compared to the 2015 baseline of 682. The percentage of financially included adults has more than doubled, reaching around 45% in 2020, exceeding the target by 77%. Bank branches have increased from seven to twelve per 100,000 adults, surpassing the initial target by 50%. The agent network, including banking and mobile money agents, has experienced significant growth, expanding from three to 77 agents per 100,000 adults in four years.[50]

2.4 Evolution of DFS Services in Ethiopia

In Ethiopia, the evolution of mobile money services began in 2015 with the introduction of mobile banking under a bank-led model. The country's first mobile banking service, M-BIRR, was launched through a collaboration between five microfinance institutions (MFIs) and Ethio Telecom. Around the same time, Hello Cash, another mobile banking service, was introduced by

[48] NBE, *National Financial Inclusion Strategy-II 2021-2025* (September 2021)

[49] ibid

[50] ibid

Lion Bank, the Cooperative Bank of Oromia, and Somali Microfinance Bank. However, during this initial phase, mobile banking services had limited scale, with MFIs and banks primarily focusing on specific products and serving urban areas. Challenges related to scaling operations and limited investment hindered the widespread adoption and growth of mobile banking services.[51]

In 2016, banking and mobile money agents were almost non-existent, with a baseline of three per 100,000 adults. This has increased by over 25 to 77 agents per 100,000 adults as of 2020. In 2016, mobile money was minimal, with mobile money wallets making up less than 1% of transaction accounts. Since then, mobile money accounts have increased by 10, with 8 million mobile money wallets registered as of June 2020. [52]However, challenges related to scaling operations and limited investment have hindered the widespread adoption and growth of mobile money services.[53]Between 2016 and 2020, the number of banking and mobile money agents increased from almost non-existent to 77 agents per 100,000 adults. Mobile money accounts also experienced substantial growth, rising by a factor of 10, with approximately 8 million registered mobile money wallets as of June 2020.[54]

In 2020, the NBE introduced a directive that allowed non-traditional financial institutions to issue payment instruments. This directive expanded the range of services to include cash transactions, money transfers, bill payments, and microfinance products. It also introduced licensing and capital requirements. Moreover, it created opportunities for foreign investors to participate in Ethiopia's payment services sector, fostering financial inclusion, competition, and innovation within the industry. [55]

Ethio Telecom, the state-owned mobile operator and the sole MNO in Ethiopia until 2022, recently launched its mobile money service called telebirr. Then, Safaricom, a Kenyan MNO, entered the Ethiopian market in September 2022 and obtained its mobile money license in May

[51]*Mobile Money in Ethiopia (n 25)* 14

[52]*National Financial Inclusion Strategy (n 51) 8*

[53]*Mobile Money in Ethiopia (n 25)* 4

[54]*National Financial Inclusion Strategy (n 51)*8

[55] Reflection on the New Payment Instrument Issuers Directive (n 3) 36

2023. In 2023, Kacha became the first private payment instrument issuer after receiving its license from the NBE.[56]

Mobile money services in Ethiopia have significant potential to lift 700,000 people out of poverty, contribute $5.3 billion to GDP, and provide a safety net. However, success depends on enabling policies, interoperability, access points, and trust. As the ecosystem matures, mobile money can support various use cases, and the government has prioritized increasing the country's lagging financial inclusion through its 2021-2025 National Financial Inclusion Strategy. [57]

2.4.1 Introduction of mobile money service providers

i. Tele Birr

The only government-owned telecom company, Ethiopian Telecommunication Corporation, owns Telebirr. This financial technology platform was launched in 2021 with the motto of "financial access for all." Huawei developed the platform to facilitate cashless financial transactions, including credit services. This mobile money service allows users to deposit and withdraw cash, purchase airtime, cover utility payments, make international remittances, and access credit services using different models such as Endekise, mela, and Sanduq. [58]

Telebirr's financial technology model involves stakeholders such as commercial banks, Ethiopian telecommunication corporations, and various government institutions. Telebirr collaborates with nine international remittance companies, Ethiopian Airlines, Ethiopian Electricity, and commercial banks. [59]

ii. M-PESSA

Kenya's mobile money sector, led by Safaricom's M-Pesa, which was introduced in 2007, has transformed the country's financial landscape. With over 58.3 million mobile wallets by December 2019, M-Pesa has enabled widespread access to formal financial services for more

[56] *Mobile Money in Ethiopia (n 25)* 7

[57] Ibid 8

[58] Ousman Mohammed Yimam, 'Digital Financial Inclusiveness Through Financial Technology in Ethiopia: Case Study on TeleBirr'[2023] Current Debates on Social Sciences 217 <https://www.researchgate.net/publication/376953218> accessed on 13 April 2024

[59] Digital Financial Inclusiveness (n 57) 219

than 80% of the population. Initially focused on person-to-person payments, M-Pesa expanded to include person-to-business transactions, utility bill payments, and partnerships with banks to offer savings accounts and digital credit products. This innovative model has driven financial inclusion, lifted households out of poverty, and revolutionized the way Kenyans engage in financial transactions.[60]

M-PESA expanded its operations to Ethiopia in August 2023, aiming to replicate its successful model from Kenya to serve diverse population segments. Its entry into Ethiopia marked a significant milestone alongside Telebirr. If M-PESA can achieve success in Ethiopia, it may pave the way for other private mobile money providers, thereby increasing competition in the market.[61]

iii. Kacha

Kacha DFS S.C. is the first private payment instrument issuer. With a subscribed capital of ETB 200 million and a consortium of thirteen esteemed individuals from various backgrounds, including professionals, entrepreneurs, and industry experts, Kacha brings together a diverse and talented team united by a common vision.

According to AbrehamTilahun, CEO of Kacha, Kacha offers a range of user-friendly services through its mobile app and USSD interface. It provides underserved populations in Ethiopia with innovative and secure financial solutions, prioritizing user data security through encryption and infrastructure, ensuring uninterrupted access across Ethio Telecom and Safaricom SIM cards.

According to MikiyasFekadu, Data Analytics & Mobile Money Commercial Manager of Kacha, Kacha's entry into Ethiopia's digital payment sector was prompted by the country's significant financial inclusion challenges and the promising, yet largely untapped, market opportunities. [62]

---

[60] *Digital Financial Services* (n 24) 33

[61] Mijail Popov, 'Africa's Mobile Money Battle: Can M-PESA succeed in Ethiopia?' payments and Commerce Market Intelligence <https://paymentscmi.com/insights/m-pesa-ethiopia-africa-mobile-money/> accessed 09 April 2024

[62] Interview with MikiyasFekadu, Data Analytics & Mobile Money Commercial Manager of kacha

2.5 Evolution Of DFS Regulations in Ethiopia

Ethiopia has enacted key regulations and directives to foster digital finance and enhance financial inclusion. The developments are summarized as follows:

- In 2011, the National Payment System Proclamation (No 718/2011) was introduced to regulate payment systems and financial transactions.
- In 2012, the Licensing and Supervision of the Business of Financial Institutions: Regulation of Mobile and Agent Banking Services (Directive no. FIS/01/2012) provided guidelines for licensing and supervising mobile and agent banking services.
- In 2019, the Amendment to Banking Business Proclamation (Proclamation no. 1159/2019) relaxed entry restrictions to the banking sector and allowed foreign investment.
- In 2020, the Use of Agents Directive (Directive no. FIS 02/2020) regulated the use of agents for mobile money services, increasing access to financial services.
- Also, in 2020, the Licensing and Authorization of Payment Instrument Issuers (Directive no. ONPS 01/2020) allowed nonbank entities to provide mobile money services.
- The Amendment: Authorization of MFIs to Convert to Banks (Directive no. SBB/74/2020) enabled eligible microfinance institutions to become banks.
- The Payment System Operator Directive (Directive no. ONPS 02/2020) regulated entities operating as payment system operators.
- In 2023, the National Payment System Amendment (Proclamation no. 1282/2023) updated regulations to align with evolving technologies.

2.5.1 Mobile Money Regulation Evolution in Ethiopia

Mobile money regulation in Ethiopia has undergone significant changes to promote financial inclusion and innovation. In 2012, the NBE issued a directive allowing licensed financial institutions to offer mobile banking services and utilize agent networks, facilitating partnerships between institutions and technology providers. However, in 2020, the government introduced reforms to transition from a bank-led to a hybrid model, including directives enabling non-financial institutions to provide mobile money services and opening the telecom sector to foreign

investment. These reforms aimed to diversify the mobile money landscape, support various DFS channels, and enhance inclusion, competition, and innovation within the sector. [63]

Chapter three

3 Examining Ethiopia's Legal Framework for Data Protection in Digital Finance: A Case Study of Kacha

This chapter explores Ethiopia's legal framework for data protection in digital finance and Kacha DFS S.C.'s policies, procedures, and practices. The research is based on a document assessment and interviews to determine how the organization adheres to general principles for data protection in digital finance and the provisions of Ethiopia's new Personal Data Protection Proclamation. It also evaluates the company's efforts to meet regulatory requirements, offering insights into the Personal Data Protection Proclamation's effectiveness in protecting consumer data in Ethiopia's evolving DFS sector.

3.1 General frameworks for the protection of Data in DFS

i. The Constitution

Article 26 of the Constitution provides that everyone has the right to privacy, which includes the right not to be subjected to the search of their home, person, or property, or to the seizure of any property in their possession. [64] Moreover, Article 26(2) stipulates that 'everyone has the right to inviolability of their notes and correspondence, including postal letters, and communication made by telephone, telecommunications, and electronic devices.'[65]This provision safeguards personal data in the digital realm by extending privacy protections to all electronic communications.

[63]*Mobile Money in Ethiopia (n 25)* 14.

[64] Constitution of the Federal Democratic Republic of Ethiopia Proclamation No. 1/1995, Art 26(1)

[65] Constitution of the Federal Democratic Republic of Ethiopia Proclamation No. 1/1995, Art 26(2)

Article 26(3) of the Constitution envisages exceptions where these rights may be limited. Thus, the right to privacy can be restricted in 'compelling circumstances and in accordance with specific laws whose purposes are safeguarding of national security or public purpose, the prevention of crimes or the protection of health, public morality or the rights and freedom of others.' [66]

Ethiopia is also a party to a number of international and regional human rights instruments that provide for the right to privacy and protection of personal information including the Universal Declaration on Human Rights 1948, the International Covenant on Civil and Political Rights 1966, the Convention of the Rights of the Child 1989, and the African Charter on Rights and Welfare of the Child 1990.[67] According to Article 9 of the Constitution, these and other human rights instruments ratified by Ethiopia form an 'integral part' of the country's laws.[68] For instance, the United Nations Human Rights Council resolution passed in 2016 stresses that "the same rights that people have offline must be protected online," especially as it relates to the protection of the freedom of expression as indicated in the UDHR and the ICCPR, both of which Ethiopia has ratified.[69]

ii. Civil Code

The privacy-related rights recognized under the Civil Code include the Constitutional right not to be subjected to search except in cases provided by the law. Article 11 provides that 'no person may have their freedom restricted, or be subject to a search, except in cases provided by the law.'[70] This provision recognizes the constitutional right to privacy and restricts the freedom of individuals from being subjected to searches, except in cases provided by the law. While this

[66] ibid, Art 26(3)

[68] ibid, Art 9

[69] Emma Boyle, 'UN declares online freedom to be a human right that must be protected' [2016] Independent 36<https://www.independent.co.uk/life-style/gadgets-and-tech/un-declares-online-freedom-to-be-a-human-right-that-must-be-protected-a7120186.html > accessed on 19 April 2024

[70] CivilCodeoftheEmpireofEthiopiaof1960,NegaretGazeta,Extraordinaryissue,ProclamationNo.165,19thyear No. 2, art.11

provision does not explicitly mention data protection in digital finance, it establishes a general principle that protects individuals' privacy rights.

In the context of DFS, this provision can imply that individuals have the right to keep their financial information private, and financial institutions should not infringe upon this right without proper legal justification. It suggests that any search or access to a person's financial data should be conducted within the bounds of the law.

iii. The Criminal Code

Articles 604 to 606 of the Criminal Code criminalize violations of privacy safeguards guaranteed by the Constitution. These provisions establish legal protections against unauthorized access, intrusion, or disclosure of personal information.Under Articles 604 and 605 of the Criminal Code, anyone who commits any of the acts listed as violations of domicile or restricted area privacy is subject to up to five years of imprisonment in aggravated cases. [71]

In addition, according to Article 606 of the Criminal Code, the violation of the privacy of correspondence or consignments, including intrusion into one's letter, telegram, telecom, and other electronic correspondence, among others, is punishable, upon complaint, by up to six months of imprisonment or a fine.

Regarding DFS, financial institutions are expected to implement security measures to safeguard customer information from unauthorized access, hacking, and data breaches. Violations of these privacy safeguards may lead to legal consequences for individuals involved in the unauthorized access or disclosure of customer data.

iv. The Criminal Procedure Code

[71]Ethiopian Criminal Code (2004), Proclamation No. 414/2004, Federal NegaritGazeta, Year 10, No. 25, art.604 and 605

Article 32 of the Criminal Procedure Code provides that no person or premises will be searched without a court warrant except for certain exceptions the law provides. These exceptions include: where the offender is followed in hot pursuit and enters the premises or disposes of articles that are the subject matter of an offense in the premises; and where there is a reasonable cause for suspecting that articles which may be material evidence are concealed and there are reasonable grounds for believing that delay would likely result in removal of such articles. [72] In the context of DFS, this provision could potentially come into play if there is a need to search premises or seize electronic devices or data storage devices as part of a criminal investigation related to banking activities or financial crimes.

v. Licensing and Authorization of Payment Instrument Issuers Directive

The directive issued in April 2020 introduced significant changes to the banking landscape by allowing nonbank companies to offer various services previously limited to banks. This directive replaces and repeals the 2012 Mobile and Agent Banking Services Directive and operates under the National Payment System Proclamation No. 718/2011. [73]

To protect data and operations, payment instrument issuers seeking authorization and licensing must meet specific requirements outlined in Article 4 of the directive. These requirements include establishing a dependable core system supported by a network infrastructure,[74] implementing security policies and procedures to maintain the integrity, authenticity, and confidentiality of data and operations.[75] Additionally, payment instrument issuers must develop a comprehensive risk management framework that addresses a range of risks, including operational, technology, communication, cybersecurity, third-party, liquidity, reputational, and

[72] Criminal Procedure Code of Ethiopia (1961), Proclamation No.185/1961, Federal NegaritGazeta, art 32

[73] Reflection on the New Payment Instrument Issuers Directive (n 3) 36

[74] Licensing and Authorization of Payment Instrument Issuers Directive No. ONPS/01/2020, art 4(6)(c) (iv) -

[75] Licensing and Authorization Directive (n 73) art 4(6) (c) (vi)

legal risks.[76] They must also have established policies and procedures in place for KYC[77] and AML and CFT measures.[78]

In addition, the application shall include operational policies and procedures that provide detailed information about the initial and future products and services to be offered. These policies outline how the products and services align with existing processes and systems, pricing structures, sustainability measures, and affordability considerations. Practical administrative and management functions, accounting processes and reporting, transparent process flows depicted through diagrams, compliant transaction authentication methods like two-factor authentication, and a policy and procedure manual should also be included. Additionally, participation in a national or international payment system, procedures to safeguard user funds, proposed product or service names, an internal control system, and terms and conditions for agents, merchants, and other third parties should be documented. These comprehensive operational policies and procedures ensure clarity, compliance, and data protection throughout the company's operations.[79]

The directive also emphasizes the role of the National Bank in overseeing payment instrument issuers, their systems, agents, and outsourcing counter parties.[80] Payment instrument issuers must maintain records of relevant information and submit it to the National Bank within seven calendar days after the end of each quarter. This information includes any instances of cybersecurity breaches and data loss.[81]Furthermore, according to Article 12(2) (f), payment instrument issuers must enter into user agreements when opening accounts. These agreements should explicitly state the confidentiality of all users' information, ensuring the protection and privacy of their data.

vi. Financial Consumer Protection Directive No. FCP/01/2020

[76] ibid art 4(6) (d)

[77] ibid (n 73) art 4(6) (e)

[78] ibid (n 73) art 4(6)(e)

[79] ibid (n 73) art 4(6)(b)

[80] ibid (n 73) art 13(1)

[81] ibid art 13(2)

The Financial Consumer Protection Directive requires financial service providers to keep confidential and secure the financial consumers' data they collect. They may only use and disclose such data for legitimate purposes agreed upon by the financial consumer, security provider, or as permitted by law. Furthermore, financial service providers must implement policies and procedures to ensure the confidentiality and security of financial consumers' data. They are also required to inform financial consumers and security providers about their policies and make them available. [82]

vii. National Bank Circular

The National Bank Circular aims to implement the Directives on the Regulation of Mobile and Banking Services No. FIS/01/2012 clarifies the relationship of financial institutions with third parties, including Technology Service Providers ('TSPs'). The National Bank Circular obliges financial service providers engaged in agent and mobile banking to retain data centers and related infrastructure on the premises of financial institutions with which they have acquired, leased, or have special agreements for the same purposes. It prohibits TSPs from accessing any customer data unless they are authorized by the financial institution for specific periods and purposes related to support and maintenance.[83]

3.2 A Comparison of the Data Protection Proclamation and Kacha's Data Protection Practices

3.2.1 Preamble and scope

This proclamation emphasizes the need for a specific law in Ethiopia to regulate personal data protection and establish a dedicated institution for this purpose. It recognizes the significance of such legislation in promoting a strong digital economy, defining the rights and responsibilities of

[82] ibid art 5(4)

[83]Dadimos Haile and DerejeAshenafi, 'Ethiopia - Data Protection Overview', One Trust Data Guidance Regulatory Research Software <https://www.dataguidance.com/notes/ethiopia-data-protection-overview> accessed on 13 April 2024

stakeholders, addressing related issues, and cultivating a robust culture of personal data protection.[84]

This Proclamation applies to processing personal data through automated means or filing systems.[85] It covers data controllers and processors in Ethiopia or those outside Ethiopia but using equipment in Ethiopia and having a representative there.[86]It includes private and public institutions of the federal and regional governments, including city administrations.[87]However, it does not apply to personal data processing done by individuals for personal or household purposes, information exchange between government agencies on a need-to-know basis, exempted cases, or the transit of personal data through Ethiopia from outside the country.[88]

The Preamble indicates that the Proclamation will have substantial implications for DFS providers such as Kacha, requiring them to integrate their activities with new legal criteria for handling personal data. Providers will be required to follow strict regulations for collecting, storing, processing, and sharing personal data, mandating the establishment of robust data protection policies and procedures to secure client information. They will also manage data processing risks and prevent breaches by developing methods for quickly recognizing, reporting, and responding to occurrences. Maintaining customer trust and preventing legal penalties will necessitate investment in risk management systems and personnel training. The Proclamation will also demand greater transparency, as providers must inform customers about their rights and how their data is processed, which could alter how relationships with customers are managed.

Furthermore, the Proclamation seeks to establish a unified international framework for personal data security, allowing Ethiopian providers to benefit from secure cross-border data transfers while encouraging collaboration with international financial institutions and fintech companies. This could open new market opportunities and drive growth for Ethiopian DFS. While the new

[84] Personal Data Protection (2004), Proclamation No. 1321 /2024, Federal NegaritGazeta 30th Year No 35 , preamble

[85] Ibid Art 3(1)

[86] Ibid Art 3(2)

[87] Ibid Art 3(3)

[88] Data Protection Proclamation (n 110) Art 3(4)

regulations will present challenges, such as the need for investments in technology, training, and compliance processes, the long-term benefits include increased customer loyalty, improved trust, and the ability to foster innovation in a secure and trusted environment, as described in the previous chapter. This regulatory framework aims to enable providers to position themselves for long-term success, contributing to the establishment of a more secure and competitive DFS ecosystem both domestically and globally.

In an interview with FetahiHailegiorgis, Infrastructure and Security Manager of Kacha, he explained that Kacha's infrastructure aligns closely with the data protection proclamation law, built to meet international standards, including the General Data Protection Regulation (GDPR). He highlighted that GDPR applies to European citizens' data, regardless of location, and Kacha's system complies with it. However, Fetahi noted that adjustments are needed in areas like incident notification, 24/7 monitoring, and addressing gaps to comply fully with the Proclamation. He also emphasized that Kacha has already implemented security measures to protect customer data and transactions on its digital wallet platform.89

Central to Kacha's operational framework are its objectives of ensuring customer privacy and data security. By integrating privacy considerations into every facet of its service offerings, from initial product design to ongoing data handling practices, Kacha strives to balance safeguarding customer privacy and providing seamless digital finance experiences. [90]

Operations and technology constitute the focal points for addressing security, privacy, and data concerns, encompassing customer handling intricacies and platform strength.

According to insights from interviews with Kacha's operations team, the department responsible for ensuring compliance with privacy and data protection legislation is crucial for administering privacy controls, interpreting legislative frameworks, and responding to privacy incidents. Their responsibilities include formulating rules, monitoring user consent, and ensuring adherence to national data protection legislation in the digital banking sector. Furthermore, Kacha has a specialized department oversees compliance efforts and conducts regular reviews to analyze and assure the continuous effectiveness and alignment of policies with changing requirements. [91]

[89] Interview with FetahiHailegiorgis, Infrastructure and Security manager of Kacha

[90] Interview with MikiyasFekadu, Data Analytics & Mobile Money Commercial Manager of kacha

[91] Interview with sizanaTesfaye, Operations Manager of kacha

Kacha's four main policies; customer protection, KYC, operations, and risk management were presented to and approved by the National Bank of Ethiopia in 2022. However, there have been no adjustments to these policies since the execution of the data protection proclamation, and no changes are planned, as they are intended to conform to the proclamation, according to Fetahi. Although the policies and procedures will be compared to the relevant sections of the proclamation throughout the study paper, concerns about their effectiveness persist. Once filed and approved by the NBE, there is no official process to verify their effectiveness, and the fact that periodic assessments are undertaken by internal staff raises the possibility of bias.

According to interviewees operational processes and workflows at Kacha are crafted to prioritize privacy and data security.[92]Kacha takes a systematic approach to customer data management, dividing consumers into two levels based on transaction volume. The company services a wide spectrum of stakeholders, including B2C and C2B businesses, payment system operators, merchants, agents, and master agents. Each stakeholder group is subject to distinct security rules designed to protect their data while also ensuring the integrity of Kacha's payment ecosystem.[93]

3.2.2 Principles of Processing of Personal Data

Personal data processing must adhere to ethical standards such as legality, fairness, and transparency, and provide persons with clear information. To maintain data minimization, data should be acquired for particular, legitimate objectives, with no incompatible uses, and adequate, relevant, and not excessive. Accuracy, timely updates, storage limitations, and proper security measures are required to preserve integrity and privacy. To uphold data sovereignty, individuals must maintain control over their information under applicable laws. This framework protects privacy and supports appropriate data handling.[94]

Concerning lawfulness, personal data should only be processed if one of the conditions specified in Article 7 is met. These conditions include obtaining consent, fulfilling contractual obligations, complying with legal requirements, protecting vital interests, responding to emergencies, or pursuing legitimate interests while respecting individuals' rights and freedoms. [95]

[92]EndalkachewGirma, Training and Business Support Specialist at Kacha

[93] ibid

[94] Ibid Art 6

[95] Ibid art 7

3.2.2.1 Data Processing at Kacha

Policy paragraphs 3.1 and 14 of Kacha's Customer Protection and KYC Policy and Procedures underline the necessity of gathering only the information required for account creation and service delivery. These rules define identification requirements consistent with the Financial Anti-Money Laundering (AML) and Counter-Financing of Terrorism (CFT) Compliance Directive, assuring compliance with legal standards for specific client categories. The policies also specify a list of documentation necessary from various consumers, which is displayed below.

Type of Accounts	Account Level	Minimum Customer Due diligence requirements for opening and maintaining mobile wallet accounts
Individual Customer	Level 1	▪ Full Name ▪ Date of Birth ▪ Residential Address ▪ Telephone Number ▪ Recent Photo of User ▪ Introduction by another person who is already registered for the service
	Level 2	▪ Full Name ▪ Date of Birth ▪ Residential Address ▪ Telephone Number ▪ Recent Photo of User ▪ Identity Card of the User (Residence ID, Passport, Driving license, Any other legally accepted ID)
Enterprise Customer	-	▪ Full Name ▪ Date of Birth ▪ Business Address ▪ Telephone Number ▪ Recent Photo of the authorized User ▪ Business License or equivalent

Type of Accounts	Account Level	Minimum Customer Due diligence requirements for opening and maintaining mobile wallet accounts
		▪ Identity Card of the authorized User (Residence ID, Passport, Driving license, Any other legally accepted ID)
Merchant	-	▪ Memorandum of Association (Where applicable) ▪ Articles of Association (Where applicable) ▪ Tax payer identification certificate (Where applicable) ▪ Bank account information (Where applicable) ▪ Business License ▪ Name of the owner ▪ Owner contact information ▪ Business address ▪ Information of Employees of the merchant
Agent	-	▪ Memorandum of Association (Where applicable) ▪ Articles of Association (Where applicable) ▪ Tax payer identification certificate (Where applicable) ▪ Bank account information (Where applicable) ▪ Business License ▪ Name of the owner ▪ Owner contact information ▪ Business address ▪ Information of Employees of the Agent
Walk In user	-	▪ Full Name ▪ Date of Birth ▪ Residential Address ▪ Telephone Number ▪ Recent Photo of User ▪ Identity Card of the User

In addition, Kacha's Operations Policy and Procedures emphasize transparency by adopting a fixed-percentage pricing structure for services,[96]designed to enable customers to understand and relate costs to transaction values. The policy mandates that reports on account balances, transaction types, fees, and commissions are accessible to users and regulatory authorities, fostering accountability. [97]Additionally, Branch Operations Policies require start-of-day and end-of-day reconciliations, aimed at ensuring transparency in cash management.[98]

According to the reconciliation Manager, who does not want his or her name to be mentioned, the reconciliation department carries out the reconciliation process daily to efficiently track transactions. While users can see transaction types and account balances while using the service, reconciliation is primarily an internal activity.

The policy requires Kacha DFS to ensure that all service locations, including agents and branches, follow set branding and compliance requirements. Regular monitoring of agent operations is recommended to ensure compliance with legal and regulatory obligations. However, with a small number of active branches and agents, determining the whole feasibility of these methods at this time is difficult. An Agent and Merchant Onboarding and Monitoring Manager and Officer have been assigned to oversee the implementation and monitoring of these operations.[99]

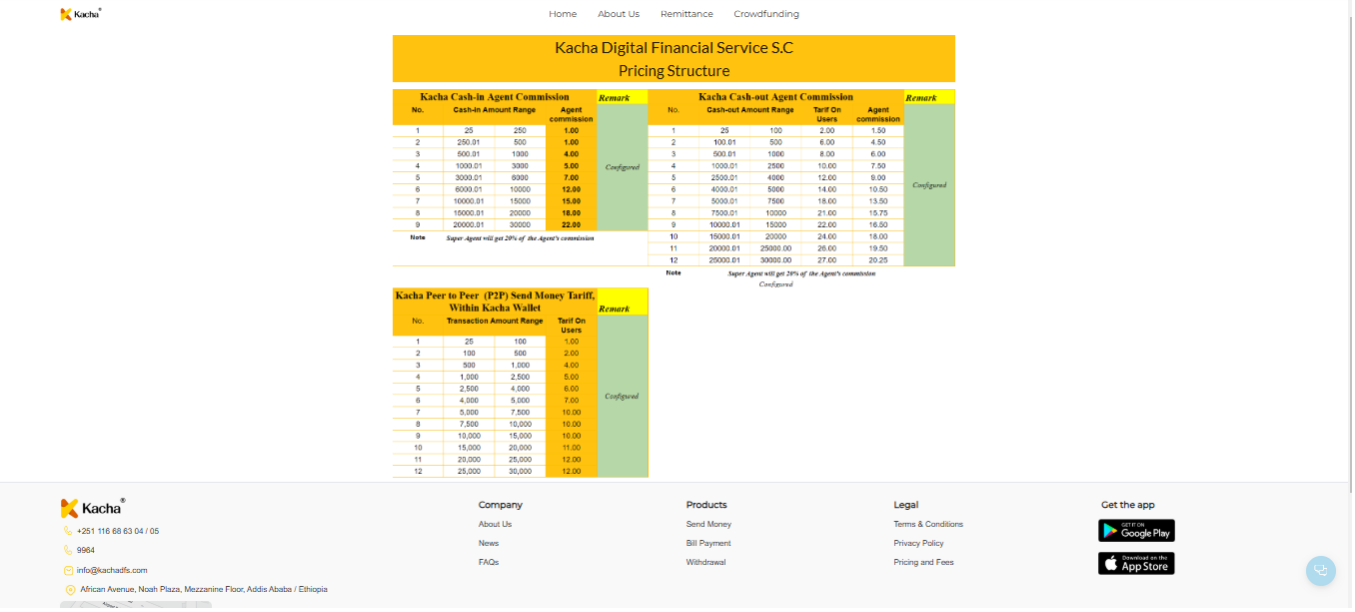
Regarding fees, Kacha has published its pricing structure on its website, as provided below. The information is available for Level One and Level Two users and is in English. While this ensures some level of transparency, there is room for improvement in accessibility and inclusivity, given that services are offered in multiple languages, including Amharic, Somali, Tigrigna, and Oromifa. This gap highlights an opportunity to make pricing information more inclusive and wholesome. Additionally, the applicable proclamation does not provide detailed guidance on the extent to which transparency should be implemented, leaving room for interpretation in the application of these standards.

[96]Operations Policy and Procedures of Kacha DFS(Article 9.1)

[97]ibid (Articles 12.1 and 12.2)

[98]ibid (Article 14)

[99] Ibid, Article 3.10



The policy incorporates privacy principles by outlining security measures to protect customer information and transactions. Multi-factor authentication, including two-factor authentication (2FA), is required for most transactions to enhance account security. For low-value transactions under 1,000 Birr, single-factor authentication is applied in alignment with the National Bank of Ethiopia (NBE) Directive ONPS/01/2020.[100]

‘‘The system applies industry standard and best practices for authenticating transactions, and as a basic level of security, the system processes transactions following a two-factor authentication method. Two-factor authentication will include a minimum of two out of the following: Something you have (e.g., a Mobile phone sim card or ID), something you know (e.g., a password or a PIN code), or something you are (e.g., physical presence or biometric). The Security features that are used in the Kacha system will include PIN code, biometrics, and Password’’[101]

The policy also includes system-wide safeguards, such as float management, [102]designed to prevent unauthorized access and ensure operational integrity. Furthermore, customer education

[100] ibid(Article 10)

[101] Interview with Fetahi(n115)

[102] ibid(Article 13.1)

initiatives[103] are incorporated to promote awareness of personal data security, which emphasizes data protection by design. However, based on the interviews, consumer awareness has not yet begun and is still only at the policy level, since customer awareness is still in the process, with the exception of promotional postings on social media and some instructive posts. Interviewees did, in fact, describe several awareness development activities for agents and partners that they perceive to be customer awareness creation measures, but it appears that the concept of customers has been left open to interpretation.

3.2.2.1.1 **Consent**

As DFSrely on technology and personal data, Consent is the basis for several or all responsibilities, roles, and consequences. However as B. Benjamin, the use of consent as a basis for processing personal data is regarded as problematic because it is not providing adequate data protection in online environments. This is because of different reasons which one of the reason is there is a consent transaction overload. Second, there is an "information overload," which suggests that data subjects are supplied extensive, often challenging and extremely legalistic, information in consent transactions.[104]

In terms of lawfulness, personal data should only be processed if one of the conditions specified in article 7 is met. These conditions include obtaining consent, fulfilling contractual obligations, complying with legal requirements, protecting vital interests, responding to emergencies, or pursuing legitimate interests while respecting individuals' rights and freedoms.[87]

Accordingtoarticle2(5)ofthedataprotectionproclamationconsentstandsfor "The voluntary, specific, and informed expression of a data subject's wishes regardingtheprocessingoftheirpersonaldata.Itcanbegiventhroughawrittenstatement,verbal Affirmations,oranyclearaffirmativeactionthatindicatesagreementtotheprocessingofpersonal data."

While digital service providers, including Kacha, typically obtain consent through electronic confirmation (such as clicking an "Agree" button), it is important to consider whether this

[103] ibid(Article 10)

[104] B Benjamin, The Consent Paradox: Accounting for the Prominent Role of Consent in Data Protection, and Hansen, MaritKosta, EleniNai-Fovino, Igor Fischer-Hübner, Simone (Ed.), Privacy and Identity Management. The Smart Revolution, (Springer International Publishing) P 7

method adequately fulfills the requirement of explicit affirmative action. This is especially relevant when serving underserved communities with lower levels of education, as additional measures should be taken to ensure that individuals fully understand and are informed about the terms and conditions to which they are agreeing.

According to Article 7 of the Proclamation, data processing can only occur when the data subject has given explicit consent. Article 8 specifies the conditions for valid consent, stating that it must be freely given, informed, precise, unambiguous, and based on an active action by the data subject, such as checking a box or clicking a button.

However, Kacha's asking for approval only after all the data has been entered into the digital registration form raises problems. According to best practices in data protection, consent should be sought before any processing of personal data occurs, ensuring that individuals have complete control and awareness of how their data will be used. The uncertainty arises from defining what constitutes a clear and adequate manner for getting permission in this circumstance.

Furthermore, Article 8 grants the data subject the right to withdraw consent at any time, with prior information on how to do so. Article 7 also states that the data controller cannot condition the provision of goods, services, or contracts on consent for unnecessary data processing. The burden of proof for obtaining valid consent falls on the data controller, who must present it clearly and separately from other matters.

The term "clear" in the context of getting consent can be subjective, as various circumstances, including the nature of the material, the target audience, and regulatory requirements, determine its interpretation. Clarity entails giving information in an understandable format for the average user, free of ambiguity or jargon.

In discussions with Kacha consumers, a consistent theme arose regarding their understanding of consent and the value of personal information. Many clients, such as BetelehemShiferaw, interpreted consent as implicitly granted by utilizing the service without actively engaging with the terms and conditions. Despite conceding that the agreement was officially obtained by clicking the agreed-upon button, Bethlehem acknowledged not completely understanding the terms since they were too long and complicated. Other interviewees expressed similar sentiments, believing that consent is obtained merely through the utilization of the service and

finding the terms and conditions difficult to follow. Furthermore, when addressing the registration procedure, users indicated minimal concern about the personal data collected, instead focusing on the security of their funds and the regularity of transactions. This pattern indicates a lack of knowledge about the importance of protecting personal data and a tendency to see consent as implied rather than actively sought.

3.2.2.1.2 Kachawallettermsandconditionreview

Kachas has made terms and conditions available on its official website, and upon registration via USSD or application.

It disclaims liability for unauthorized access or breaches, whether intentional or negligent, which places the burden of security solely on the users, potentially leaving them vulnerable to data breaches or financial losses resulting from security lapses on the Company's part.

Users also bear responsibility for the accuracy and authenticity of instructions provided to the Company, which can be challenging given the complexities of online transactions and potential risks of fraud or manipulation, which puts users at a disadvantage, especially in cases where unauthorized transactions occur due to security vulnerabilities in the Company's systems.

While the Company asserts its commitment to transaction authentication and record-keeping, users have limited recourse in disputing transactions or holding the Company accountable for errors or discrepancies. The Company's records serve as conclusive evidence unless discrepancies are reported within a short timeframe, potentially undermining users' ability to challenge erroneous or unauthorized transactions effectively.

The Company also promises to address user complaints promptly. However, the value of this process may be questionable, especially considering the lack of specific timelines or escalation procedures outlined in the terms and conditions. Users may face challenges seeking recourse for data privacy violations or security breaches, particularly if the Company's response is inadequate or delayed.

Further, it is also worth noting that Kacha provides its services in five languages: English, Amharic, Somali, Oromifa, and Tigrigna. However, the terms and conditions and information provided on its website are only in English and Amharic, which raises questions about whether this is considered clear to speakers of other languages. This lack of clarity may create issues for non-English and non-Amharic speakers, potentially leading to misunderstandings or

difficulties in fully understanding the terms and conditions.

3.2.3 Framework for Responsible Data Processing

Starting with Article 12, the proclamation emphasizes the importance of justice and transparency, ensuring that data subjects receive clear, accessible, and honest information about data processing. Building on this, Article 13 emphasizes the purpose limitation principle, requiring that data be used only for specified purposes disclosed in advance, with further processing permitted only if it is consistent with the original purpose or serves specific needs, such as research, provided that safeguards are in place. Article 14 focuses on data accuracy by requiring controllers to take reasonable steps to ensure correctness and allowing data subjects to report mistakes. Meanwhile, Article 15 addresses storage limitations by allowing data preservation only when necessary by law or for authorized purposes, while also protecting historical, statistical, or research applications against exploitation. Article 16 emphasizes the importance of integrity and confidentiality, requiring data controllers to ensure the dependability of personnel and processors who handle data. In contrast, Article 17 emphasizes the need for strong technical and organizational safeguards, such as encryption and regular security assessments, to protect against unauthorized access, loss, or damage. Together, these articles form a complete framework for protecting personal information.

3.2.3.1 Responsible Data Processing at Kacha

Kacha's Customer Protection Policy mandates that service points, including agents, branches, and outlets, display clear identifying signs in accordance with Article 3.3. These materials include outdoor metal branding, posters, fliers, pull-up banners, snapper frames, light boxes, and service desk branding. However, the implementation of these provisions has been limited. According to the researcher's physical observations, even the limited number of agents lacks this material. Unless a customer asks, there is no way to know they are Kacha agents (agents/outlets refused to provide a picture). While the small number of operational service points may partially explain this, the lack of alignment between policy and practice raises questions about the current level of compliance with the Proclamation. Additionally, the scope of the Proclamation's applicability to digital services remains undefined, complicating compliance assessments.

Furthermore, the policy requires receipts to be issued for all transactions impacting account balances, ensuring customers have clear transaction records. While digital receipts are available, paper receipts are not provided. A company representative has stated this is because Kacha operates as a digital service, and no demand for paper receipts has been observed.

In addition, the policy stresses openness in terms of product features, risks, costs, and commissions, with the goal of providing clients with clear, understandable information to avoid misunderstandings or hidden charges. It also emphasizes client data confidentiality, limiting access to critical information, and utilizing encryption for security. However, constraints on stop-payment instructions are also provided for transactions approved with a valid PIN, in order to minimize potential conflicts.[105]

Despite these protections, implementation issues have been identified. According to an anonymous company official, limited hierarchical data accessibility might impede effective decision-making, while illegal access to sensitive data by certain workers poses security problems. Vulnerabilities in dashboard access outside of office situations reveal additional concerns that might result in unauthorized information leaks. The lack of explicit regulations and recommendations in the data protection proclamation raises the danger of inconsistent practices and security issues.

The KYC Policy, notably Article 5.2, creates a framework for customer identification and risk management by categorizing clients as people, businesses, or walk-ins, and assigning risk levels under Article 5.3 to ensure compliance with anti-money laundering (AML) regulations. High-risk clients are subjected to enhanced due diligence (EDD), whereas low-risk customers are subject to simplified due diligence (SCDD). Article 5.4 requires secure storage and regular customer data updates, prohibits unauthorized disclosures, and Article 5.5 imposes regulatory sanctions for inaccurate information. Article 5.6 describes special measures for Politically Exposed Persons (PEPs), ensuring that PEPs are scrutinized more closely. Article 7 emphasizes ongoing customer activity monitoring through periodic reviews and anomaly detection.

[105] Ibid, Article 3.9

In contrast, Article 4 defines accountability for KYC compliance as oversight by the Board, management, and RCMD, supported by audits and staff training under Article 9. The Operations Policy, specified in Articles 13.2 and 13.3, includes steps to ensure operational integrity, such as cash and e-float reconciliations, dual vault control, and separate trust accounts for e-money floats. Finally, Article 11 of the Risk Management Policy requires third-party processors to follow data protection legislation and adopt controls to protect customer information.

3.2.3.2 SecurityProtocolsand Measures at kacha

According to Fetahi, personally identifiable information (PII) and financial data are secured using advanced techniques. Data at rest is stored in an isolated environment accessible only through internal systems and APIs, ensuring protection against external threats. Additionally, encryption protocols such as HTTPS are applied to data in transit, bolstered by dedicated encrypted channels for partner transactions. Management practices prioritize local data security, supplemented by access control mechanisms such as SSH version 2 and TLS/SSL protection using SSH keys. ’With the current proclamation, suitability seems to be subjective. Where in this case is determined by the services Kacha is giving.’[106]

Kacha employs a monitoring system consisting of Security Incident and Event Management (SIEM) tools and gray log management systems. These systems detect and categorize threats, promptly alerting the organization to unauthorized activities. ’Despite experiencing a breach during a public test, the continuous monitoring framework enabled effective risk mitigation.’[107]

While lacking a structured incident response process, Kacha has established procedures and manuals for managing security incidents. However, there exists a clear need for the development of detailed incident response protocols to ensure timely and effective resolution.[108]

Regular internal security assessments form the cornerstone of Kacha’s approach to evaluating its security posture. Although rudimentary, these assessments are conducted regularly, focusing on identifying vulnerabilities amidst the dynamic nature of the startup environment. External audits

[106] Interview with Fetahi(n115)

[107] ibid

[108] ibid

by certified consultants and authorities complement internal evaluations, bolstering the organization's overall security stance.[109]

3.2.4 Rights of Data Subjects

The data protection proclamation grant individuals several rights concerning the processing of their personal data. These rights ensure transparency, control, and accountability in the handling of personal information. The right of access empowers individuals to obtain information about the processing of their personal data. They can confirm whether their data is being processed, access the data itself, learn about its origin and duration of storage, and gain other relevant details necessary for transparent processing.[110] In some cases, there may be exceptions to the right of access. These exceptions arise when disclosing the personal data would infringe upon another individual's privacy, when the data is privileged or obtained during legal proceedings, when access could harm someone's health or safety, or when the data consists of evaluative or opinion material related to employment or benefits.[111]

Individuals also possess the right to rectify inaccurate or incomplete personal data. If they believe their data is incorrect or misleading, they can request the data controller to correct it. The data controller is obligated to rectify the data and inform any third parties who received the incorrect information to ensure its accuracy.[112] In addition, individuals have the right to request the erasure of their personal data under certain circumstances. This includes situations where the data is no longer necessary for its original purpose, the individual withdraws consent, and there is no other legal basis for processing, the individual objects to the processing and there are no overriding legitimate grounds, or the data has been unlawfully processed. The data controller must also inform any third parties who have access to the data about the erasure request.[113]

---

[109] ibid

[110] Data Protection Proclamation (no110) art 25

[111] Ibid art 26

[112] Ibid art 27

[113] Ibid art 28

Additionally, individuals have the right to object to the processing of their personal data based on compelling legitimate grounds. This includes objections to direct marketing activities and related profiling. If an objection is raised, the data controller must cease processing the personal data for the objected purpose. [114]

In certain situations, individuals can request the restriction of processing their data. This may occur when the accuracy of the data is contested, the data controller no longer requires the data but the individual needs it for legal purposes, the processing is unlawful, and the individual opposes erasure, or the individual has objected to the processing pending verification of legitimate grounds. During the restriction period, the data controller can only process the data with the individual's consent, for legal claims, protection of rights, or public interest. The data controller must inform the individual when the processing restriction is lifted.[115]Moreover, individuals have the right not to be subject to decisions based solely on automated processing if it produces legal effects or significantly affects them. This includes decisions resulting from profiling. They can obtain human intervention, express their views, and receive information about decision-making. However, certain exceptions exist for decisions that are necessary for contractual obligations, authorized by law with suitable safeguards, or based on explicit consent.[116]

Individuals also possess the right to data portability. This means they can receive the personal data they have provided to a data controller or processor in a structured, commonly used, and machine-readable format. They also have the option to request the direct transmission of the data to another data controller. However, this right does not apply if the processing is necessary for public interest tasks or may adversely affect the rights and freedoms of others. Data controllers and processors must promptly comply with data portability requests free of charge.[117]

3.2.4.1 Right of data subjects at kacha

[114] Ibid art 29

[115] Ibid art 30

[116] Ibid art 31

[117] Ibid art 32

Article 3.5 of the Consumer Protection Policy assures that customers are provided with clear terms and conditions for all financial products, including risks, responsibilities, and features. These terms must be available at all interaction points, including branches and digital platforms, to enable customers to make informed decisions. While written agreements are intended to define rights and duties, the existing practice of acquiring customer assent solely through a unilateral "I agree" button raises issues about the fairness of these agreements, particularly given the lack of precise recommendations in the proclamation. Article 3.6 requires that customers be adequately informed about fees, charges, and promotional materials, with this information available at all points of contact. Customers are guaranteed access to their transaction history under Article 3.7, which promotes transparency and accountability by allowing them to evaluate their last ten transactions.

History is available on both the application and USSD versions of the service. However, why is there only a 10-day history? How about the rest? This service differs from traditional financial sectors in that it does not have a physical presence; nevertheless, does this indicate that customers must visit the office to obtain a complete statement? Based on the interviews, there is no procedure for this because there was no issue so far, but Kacha's operations team contended that the entire history is in the system. The proclamation is also unclear because it lacks specifics and leaves room for interpretation.

In terms of customer service, the Operations Policy commits to providing 24/7 help via various channels such as phone, Chabot, email, and SMS. The firm collects and analyzes consumer feedback to improve its services, displaying a continual commitment to meeting client demands while remaining transparent in its operations. Because there is no document to evaluate this other than the interviewee's comments, it is impossible to determine whether this is feasible. This will be considered in the section where complaints are discussed.

Furthermore, the Risk Management Policy addresses customer data protection in Articles 7 and 9, which detail procedures for addressing requests for access, correction, and deletion of personal data. The policy also incorporates risk mitigation methods to ensure customers can exercise their rights without excessive impediments. These, together with the KYC Policy article 9, require that personal data be processed by gathering only necessary data and using it for specified reasons.

According to Fetahi, the proclamation grants individuals the right to have their data erased. However, this conflicts with the national bank regulation, which requires companies to retain

data for 10 years. These two laws create a contradiction in terms of data management requirements. Additionally, implementing data erasure appears challenging from an infrastructure standpoint due to existing technological limitations.

Furthermore, the system is self-onboarding and does not provide a process for data correction. While the corporation says no such request was made, the lack of such requests does not explain the absence of a procedure or policy. As stated in the law, a framework should already be in place to protect these rights. Furthermore, developing particular restrictions for digital service providers in this regard appears important.

3.2.5 Data Controllers and Data Processors

Chapter Four of the Proclamation focuses on the registration, obligations, and responsibilities of data controllers and data processors.

- **Registration**

It emphasizes the importance of registering with the authority to process personal data, which involves providing specific information about the purposes of data processing and making separate entries in the Register for each purpose.[118]

According to the proclamations Article 2 sub article 36 of the proclamation “Authority” means the Ethiopian Communications Authority established as per the Communications Proclamation No. 1148/2019.”

The Authority established by the Proclamation is given several powers, as detailed in various articles. According to Article 7, the Authority is responsible for establishing administrative structures as deemed necessary and collecting service fees for its services. Article 8 stresses the Authority's duty in developing public understanding of the Proclamation's requirements, ensuring that personal data is processed by set principles, and monitoring personal and sensitive data use. Article 9 empowers the Authority to research developments in data processing and technology, whereas Article 10 mandates knowledge creation and capacity-building efforts connected to privacy rights and technology. Article 11 requires the Authority to work with international supervisory organizations and evaluate third-party states' data protection requirements. Articles

[118] Ibid art 33

12 and 13 give the Authority investigative powers, including requesting relevant information for administrative action and retaining records on data controllers and processors. Finally, Article 14 enables the Authority to issue injunctions to prevent the loss or manipulation of personal data, enforcement notices for noncompliance, and administrative fines for Proclamation infractions.[119]

The Authority established by the Proclamation has broad powers, including delegating functions to regional or federal governments (Sub-article 16) and imposing penalties (Sub-article 15). However, several of its terms are ambiguous, raising worries about overreach and inconsistent implementation. For example, wording like "exercise and perform such other functions" (sub-article 18) is unclear, potentially granting uncontrolled power. The lack of precise criteria for imposing administrative penalties and issuing injunctions (Sub-article 13) may result in arbitrary decisions, while delegating responsibility to less-equipped regional or federal authorities may lead to inefficiencies. Furthermore, the Proclamation does not clarify how international collaboration (sub-article 9) would be managed or how privacy protections will be maintained in cross-border transactions. While Sub-Article 4 emphasizes public education, it lacks a specific implementation plan. More explicit norms, more inclusive decision-making processes involving civil society and other stakeholders, and improved transparency would all help the Proclamation establish more effective and fair data protection measures.

- **obligations and responsibilities**

Once registered, data controllers and data processors have certain obligations and responsibilities to ensure compliance with the Proclamation. They must implement suitable technical and organizational measures to protect personal data, encompassing data security, record-keeping, data protection impact assessments, compliance with authorization or consultation requirements, and the appointment of a data protection officer. Internal policies and mechanisms should be established to evaluate the effectiveness of these measures.[120]

[119] Data Protection Proclamation (no110) Article 5

[120] Ibid, art 42

In the event of a personal data breach, prompt reporting is crucial. Data controllers must notify the authority within 72 hours of becoming aware of the breach, while data processors must promptly inform the data controller. These notifications should include detailed information about the breach, such as its nature, the number of affected data subjects and records, contact details of the data protection officer, potential consequences, and steps taken to address the breach.[121] Furthermore, data controllers are responsible for communicating the breach to affected data subjects within the same timeframe, providing clear and comprehensive information. However, there may be cases where communication with data subjects is not necessarily due to factors like adequate protection measures or disproportionate effort required for communication.[122]

The proclamation includes fundamental elements to preserve individuals' privacy rights, including transparency, accountability, and responsible data management. Article 45 empowers the data protection authority to inspect security measures, whereas Article 46 requires data controllers and processors to keep detailed records of processing activities. Organizations must complete a Data Protection Impact Assessment (DPIA) for high-risk processing (Article 47) and get prior authorization for data transfers to jurisdictions that lack adequate protections (Article 48). The principle of Data Protection by Design and Default (Article 49) necessitates the implementation of adequate security measures and the limitation of data processing to just necessary reasons. Furthermore, data controllers must safely erase personal data once its purpose has been met (Article 50), but joint data controllers must define explicit obligations (Article 51). Finally, the proclamation enhances accountability by forcing companies to comply with its standards (Article 52), increasing data privacy and security.

3.2.5.1 Data Controllers and Processors atKacha

According to Mikiyas, Kacha adopts a strong risk management strategy, particularly emphasizing the security of customer data and transactions. This approach encompasses initiatives to enhance awareness among staff and customers regarding security best practices,

[121] Ibid, art 43

[122] Ibid, art 44

strict adherence to internal and external standards, and the implementation of stringent security protocols to mitigate unauthorized access and data breaches.

Kacha's operations policy and procedures state that risk management and compliance activities are critical to the company's operations. The organization uses evaluations and mitigation measures to protect its digital services and maintain legal and regulatory compliance. System and process changes are methodically managed to avoid negative consequences, and they are supported by business continuity plans that address unexpected disruptions. [123]

The Risk Management Policy and Procedure created by Kacha emphasizes the necessity of protecting customer data and privacy within the firm to promote and preserve the safety and soundness of the financial system while guaranteeing regulatory compliance. The implementation of effective risk management practices and a risk-awareness culture, which extends to protecting

customer data, are critical to achieving this goal.[124]

The policy framework addresses various risks, including operational, technological, security, and legal concerns that may jeopardize consumer information. It requires consistent implementation of data protection measures across all corporate operations by regulatory directions.[125]

The policy stresses client data protection by fostering risk management solutions, informed decision-making, and continual risk mitigation improvement. It provides responsibility by outlining roles and duties at all organizational levels. To address data security and privacy concerns, the policy incorporates rigorous identity verification, encryption for sensitive data, and prompt breach investigations to prevent identity theft. It also enforces stringent access restrictions, authentication procedures, disaster recovery plans, and encryption to prevent illegal access and mitigate the effects of a breach. Fraud detection, monitoring, and whistleblower protection all improve security by decreasing potential losses.[126]

The Customer Protection Policy offers clear and accessible customer support, as described in Article 3.8, by offering several contact alternatives and established service hours. The Risk

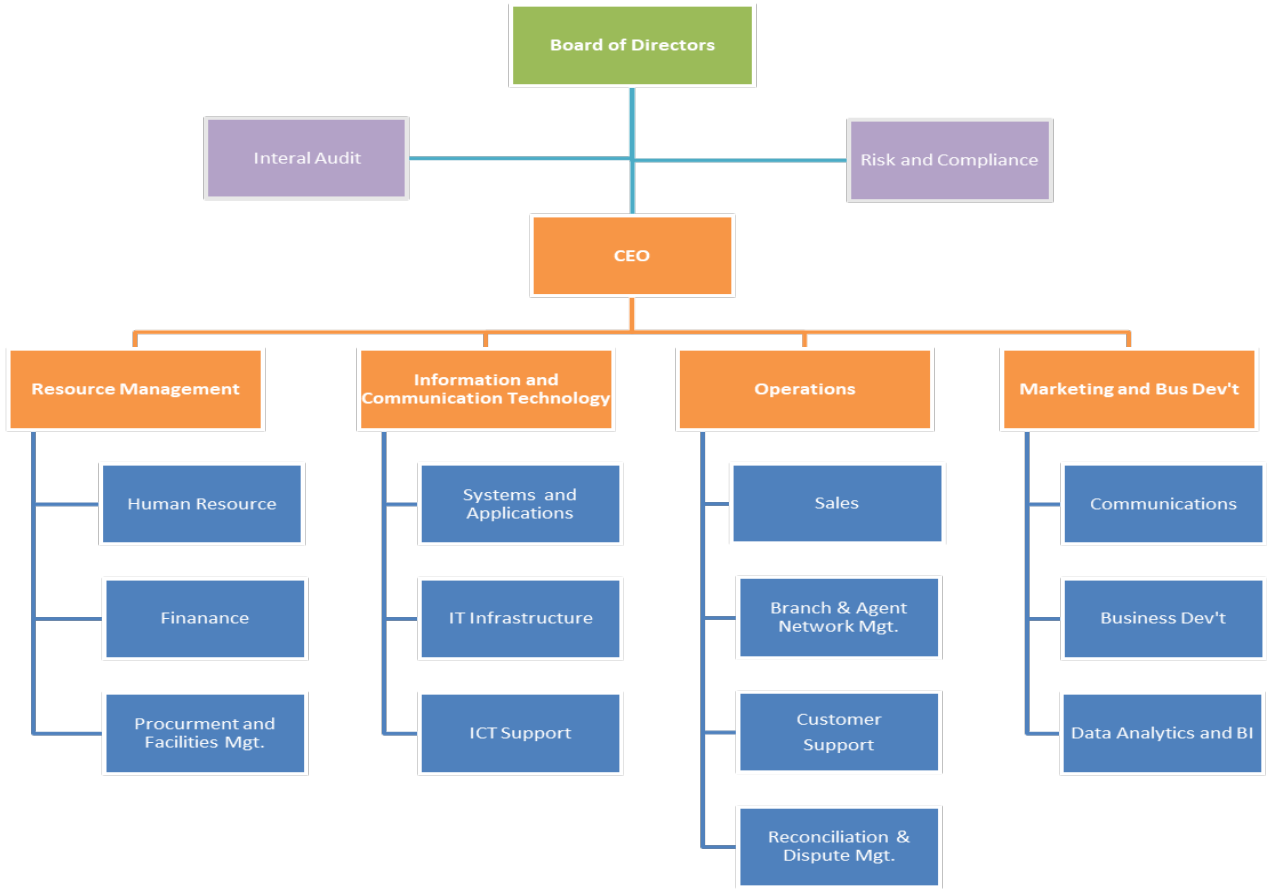
[123] Operations policy and procedure of Kacha DFS, article 7-10

[124] Risk management policy and procedure of Kacha DFS, article 14

[125] Ibid 16-18

[126] Ibid, preface

Management Policy, notably Articles 3 and 4, emphasizes risk assessments and a risk-based approach to data processing. Article 6 stresses security risk management, while Article 8 outlines incident management methods for detecting, reporting, and dealing with data security breaches. Article 10 addresses data retention and minimization, ensuring that personal data is only stored for as long as necessary, but there are worries about the total removal of deleted data. Article 2 defines the function of a Data Protection Officer (DPO) to ensure compliance with data protection legislation, which is in line with Article 15 of the proclamation. Section 6.1.3 of the policy outlines procedures for dealing with stolen customer identities, such as account termination and contacting authorities to prevent identity theft. Furthermore, Article 11 of the Operations Policy assures Kacha's organizational structure is consistent with the Payment Instrument Issuers Directive (ONPS/01/2020), demonstrating its dedication to regulatory compliance and industry standards.



The lack of a dedicated department or official for data protection reveals a structural deficit within Kacha. At the same time, interviewees indicate that Fetahi serves as an informal

focal point for these issues. The absence of a clear framework for tackling this issue creates ambiguity regarding potential remedies. Furthermore, the data protection proclamation does not include explicit guidance for analyzing and managing new risks or developing structured incident response protocols. This gap is also seen in Kacha's internal policies, despite assurances from the security infrastructure manager about its execution. In practice, emerging risks are controlled with external consultants, whilst incident response is mainly based on consumer notifications via phone calls.

3.2.6 Complaints

The data protection proclamation grants data subjects the right to submit written complaints to the authority regarding violations of their rights.[127] The authority is required to investigate the complaint unless it determines that it is not made in good faith. Within twenty-one days, the authority must inform the data subject of its decision, and if dissatisfied, the data subject can appeal to the Federal High Court within sixty days. This article ensures that data subjects have means to seek remedies for potential violations of their rights.

Individuals had to rely on informal and opaque processes with service providers before a comprehensive data protection law was enacted, making it challenging to seek remedies for data privacy abuses. Adding Article 58 to the data protection proclamation closes this gap by allowing data subjects to register written complaints with an impartial authority, establishing an organized and open redress procedure. This clause improves accountability by forcing the authority to communicate judgments within a set time range, allowing individuals to assess the success of investigations. Furthermore, introducing an appeal mechanism to the Federal High Court improves data subjects' rights by providing a judicial review if they disagree with the

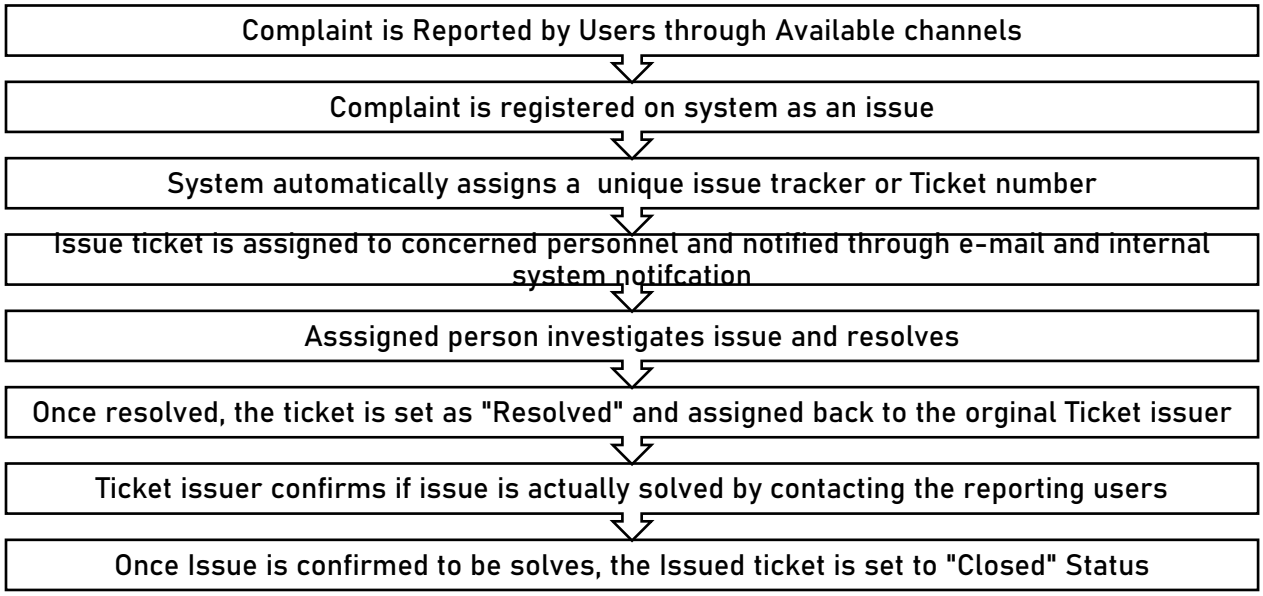
[127] Data Protection Proclamation (no110) article 58

authority's judgment. Article 58 offers a strong framework for dealing with data privacy infractions, giving individuals clear redress, transparency, and legal safeguards.

3.2.6.1 Customer complaint handling practice at kacha

The Customer Protection Policy, as detailed in Article 4, outlines a structured approach to managing disputes. It introduces a formal issue management system that handles the logging, assignment, and resolution of complaints. This system is designed to ensure transparency throughout the process, with regular reporting and analysis aimed at improving the quality of services. The policy ensures that complaints are addressed organized, with ongoing evaluation to refine processes and maintain customer satisfaction.

Below is the workflow of the case management system and process



The Complaint Handling and Redressal Procedure stated in Policy Articles 5.1-5.6 develops a four-tier system to address 80% of complaints within five business days while focusing on efficiency and customer service. Regular staff training ensures that complaints are handled promptly and correctly. However, the policy lacks clarity and adequate safeguards for protecting client data during the complaint process. It does not explain how data is acquired, stored, processed, or safeguarded, raising worries about unauthorized access and usage. The lack of defined data retention and deletion policies and poor coverage of data breach protocols undermines client confidence.

Furthermore, while the policy includes several complaint methods, it does not ensure privacy protections. These shortcomings underscore the importance of clear data protection safeguards in Kacha's complaint resolution process. Furthermore, the larger data protection proclamation lacks explicit recommendations addressing these problems, emphasizing the importance of legislative measures to promote transparency and security in managing customer complaints.

According to interviewees from the operations department, Kacha prioritizes customer satisfaction by addressing data protection concerns through various measures. The primary avenue for customer assistance is a call center facility operating seven days a week and offering multilingual support. Customers can lodge complaints through multiple channels, such as phone calls, social media, or written forms in multiple local languages, to manage complaints and address issues raised by customers. [128]

As Tigisti, junior customer support officer, implied 'Upon receiving a complaint, personnel and agents follow a set procedure that involves active listening, documentation, apology for any inconvenience, thorough understanding of the issue, ownership of the resolution process, and timely communication with the customer regarding the progress and resolution.'

Even though the company refused to provide numeric data, call center agents have pleaded that all complaints are recorded and analyzed monthly to identify systemic trends and recurring issues.

Though the data protection proclamation does not provide complaint redressal or application by data subjects to data controllers, as well as complaint addressing mechanisms, in terms of response times, Kacha aims for prompt acknowledgment of complaints within one business day and strives to resolve them within thirty working days. Investigations for at least 80% of complaints are targeted to be completed within five business days, with customers kept informed of the progress within seven business days.[129]Regular reviews of complaint handling procedures and systems are conducted to ensure their effectiveness and identify improvement areas. Through adherence to these procedures, Kacha seeks to promptly address customer

[128] Interview with, GizeworkMelesse, Senior Operations Officer of Kacha

[129] ibid

concerns, provide appropriate redressal, and enhance service quality continually.[130]During an interview, GizeworkMelesse, Senior Operations Officer of Kacha, discussed the complaint handling process at Kacha. Complaints are received through Telegram, social media, app chat, website, and the contact center. The most common types of complaints include pin resets, disputed transactions, and device errors. Resolving disputed transactions often takes longer due to involvement with other banks, over which it has no control. This delay in resolution can lead to customer frustration. After resolving a complaint, the customer is informed of the resolution through an outbound call.

AtoNatnaelBelayneh, a Kacha customer, shared his experience of a significant delay in resolving his complaint filed through the contact center. His complaint involved a money transfer from Kacha to NBE that did not reach the intended recipient. The resolution process took two weeks, causing considerable inconvenience for him. Interestingly, during the complaint handling process, Natnael gave the contact center agent his phone number, as his primary concern was the disputed transaction.

In contrast, another Kacha customer named FahmiMuhumed filed a complaint through Kacha's social media page. Although there was a delay in response via social media, Fahmi's issue, a pin reset, was quickly resolved within five minutes after being contacted by the contact center agents. Gizework explained that a pin reset is generally considered a support request rather than a complaint, and customers can often handle it independently without requiring assistance from the contact center agents. Gizework also pointed out that customers often overlook disclosing their data during the complaint reporting process. This lack of focus on data privacy arises when customers are primarily concerned with addressing their specific issues, such as disputed transactions or PIN resets. However, it is essential to reiterate that Kacha prioritizes the security and confidentiality of customer data, ensuring it remains protected and inaccessible to unauthorized parties.

3.2.7 Third party transfer

[130]ibid

The Proclamation states that the transfer of personal data to a third-party jurisdiction for processing can only occur if the third party ensures appropriate levels of protection. The transfer is subject to the provisions of the Proclamation.[131]

The Proclamation outlines the factors to consider when assessing the appropriate level of protection before the data transfer takes place. These factors include the nature of the data, the purpose and duration of the processing operation, the countries involved, the laws in the third-party jurisdiction, and the professional rules and security measures followed in that jurisdiction.[132]

It also addresses situations where appropriate levels of protection are absent. In such cases, limited forms of transfer may be authorized by the Authority, provided that the data subject's rights are not violated. The Authority must ensure that the data subject consents to the transfer and may require the severance or reduction of certain aspects of the data.[133]

However, it emphasizes that the transfer of personal data to a third-party jurisdiction that does not provide appropriate levels of protection is strictly prohibited, regardless of any limited forms of transfer mentioned earlier.[134]

It sets forth the conditions under which a data controller or processor may transfer personal data to a third-party jurisdiction. These conditions include providing proof of the existence of appropriate levels of protection, obtaining explicit consent from the data subject after informing them of the risks involved, transferring data that is necessary for contractual obligations or other specific purposes, or transferring data from a register intended for public information.[135]

Furthermore, it explains the necessity of transfers in various situations, such as contractual obligations, pre-contractual measures, and contracts in the interest of the data subject, important

[131] Data Protection Proclamation (no110) Article 18

[132] Ibid article 19

[133] Ibid, article 19

[134] Ibid, article 19

[135] Ibid, article 20

public interests, legal claims, or protection of vital interests when the data subject is physically or legally incapable of giving consent.[136]

To protect the rights and fundamental freedoms of data subjects, it grants the Authority the power to request the demonstration of security safeguards and compelling legitimate interests from individuals transferring data to a third-party jurisdiction. The Authority also has the Authority to prohibit, suspend, or impose conditions on transfers as necessary.[137]These measures establish a framework for responsible handling of personal data, including assessing and ensuring appropriate levels of protection, obtaining consent, and allowing oversight to protect customers' rights in the context of DFS.

Based on these, DFS providers are responsible for protecting their customers' personal data. When transferring this data to a third-party jurisdiction for processing, ensuring that the third party offers adequate data protection measures is crucial. This includes considering factors such as the sensitivity of the data, the purpose and duration of processing, the laws in the receiving jurisdiction, and the security measures followed by the third party. Suppose the third-party jurisdiction does not provide sufficient data protection. In that case, limited forms of transfer may be allowed with the authorization of the relevant authority, but the rights of data subjects must not be violated. DFS providers must obtain explicit customer consent for such transfers and take additional measures to minimize risks.

Kacha DFS does not have a formal policy or procedure regarding transferring personal data to third-party jurisdictions, nor is this issue included in the existing policies and procedures. However, in practice, Kacha collaborates with a third-party entity that evaluates customers' loan statuses using data from Kacha. Although Kacha has refused to provide the contract between the organization and the third party for review, they have stated that it includes provisions to secure the data and measures to prevent data breaches.

Despite the assurances provided regarding data protection in the contract, Kacha's lack of a formal policy and procedure regarding third-party data transfers raises concerns. The absence of

[136] Ibid, article 20(2)

[137] Ibid article 21

clear guidelines for managing such transfers increases the potential for non-compliance with data protection regulations, especially as there is no documented mechanism for overseeing these processes. Additionally, without access to the contract, it is difficult to assess whether the data security measures fully comply with legal and regulatory standards or if customer rights are effectively safeguarded.

3.2.8 Criminal offenses and sanctions

The data protection proclamation introduces the concept of criminal offenses and corresponding sanctions for violations of the provisions outlined in the proclamation. This article specifies various types of offenses related to the handling of personal data and defines the penalties for each offense.[138]

The offenses listed in Article 64 include various actions that can violate data protection regulations. These offenses encompass failure to notify a personal data breach, improper implementation of security measures, processing personal data in contravention of the proclamation, failure to respect data subject rights, re-identifying personal data, and unlawfully selling or transferring personal data, among others.

The penalties for these offenses vary depending on the severity of the violation. Lesser offenses may result in simple imprisonment, fines, or both. On the other hand, more severe offenses can lead to serious imprisonment, higher fines, or both. In some instances involving institutions, significant damage, sensitive data, or children's data, the fines can be as high as four percent of the institution's total worldwide turnover.

These penalties serve as a deterrent and punishment for individuals and institutions that fail to comply with data protection regulations. By imposing these penalties, the data protection proclamation emphasizes the importance of responsible data handling, respect for data subject rights, and adherence to the provisions outlined in the proclamation. The aim is to ensure that individuals and institutions prioritize data protection and take the necessary measures to prevent violations, protecting the privacy and rights of individuals whose data is being processed.

[138] Ibid, article 64

According to this article, DFS providers can be held accountable for their actions related to personal data handling. They may face criminal charges if they fail to comply with the regulations. DFS providers are entrusted with their customers' sensitive personal data, such as financial information. If they fail to fulfill their obligations regarding data protection, they may commit offenses outlined in Article 64. For example, if a DFS provider improperly implements security measures, leading to a data breach, they can be held accountable for this offense. Similarly, suppose they process personal data in contravention of the proclamation or fail to respect the rights of data subjects, such as failing to provide individuals with access to their data or not honoring their consent preferences. In that case, they can be considered in violation of the regulations. Furthermore, DFS providers must lawfully handle personal data and not engage in activities like selling or transferring personal data unlawfully or without appropriate consent. Violating these provisions can result in criminal charges and penalties as outlined in Article 64.

Kacha DFS has established policies and procedures related to compliance with data protection regulations. However, what is currently lacking is a precise mechanism for imposing sanctions on individuals or teams managing customer data. The absence of a defined sanction framework creates potential gaps in accountability, as there are no specified consequences for non-compliance or mishandling of personal data. Without a precise sanction mechanism, employees and stakeholders may not fully understand the seriousness of data protection violations or the potential repercussions for failing to follow procedures. This lack of clarity can undermine efforts to enforce data protection measures effectively and ensure customer data is handled responsibly.

3.3 Challenges

The analysis of interview responses for the thesis identified several key challenges faced by Kacha in delivering secure DFS. These challenges encompass both operational and strategic aspects of the organization's endeavors.

Operational issues with two-factor authentication have been observed, particularly delays in OTP transmission caused by Firebase Cloud Messaging (FCM) issues and challenges in handling authentication across various devices. Furthermore, specialized staff and consumer education procedures are still in a severe dearth. Strategically, limited data accessibility and weaknesses in dashboard access outside the workplace jeopardize decision-making and information security.

Although biometric approval for transactions is meant to improve security, it poses operational challenges. Furthermore, the lack of precise standards in the data protection proclamation increases the potential for inconsistency in data management and security breaches.

Kacha's problems include keeping up with technological advancements, which necessitate ongoing research, development, and consumer education investment. Infrastructure-related challenges increase complexity, such as regulatory rule alignment, breach reporting deadlines, and third-party data sharing management. Furthermore, the discrepancy between the data protection proclamation's "right to be forgotten" and national bank standards that require data retention for ten years creates a legal and operational quandary. The discrepancy between data protection legislation and sector-specific regulations needs a thorough legal investigation and potential regulatory changes.

Concerns have been raised about the effectiveness of breach fines as deterrents. The complexity of breach notification and documentation requirements makes it difficult to ensure timely and correct reporting. Addressing these concerns necessitates strategic investments in technology, infrastructure, and human resources, as well as improved tracking and reporting methods and regular staff training to maintain regulatory compliance.

Chapter four

4. Conclusion and Recommendation

4.1 Conclusion

Ethiopia's legal framework for personal data protection in DFS was previously scattered across various legal structures; however, the recently issued data protection proclamation has strengthened it.

While Ethiopia has made progress in establishing a legislative framework with the Proclamation, many gaps persist that hinder effective consumer privacy protection. These include the ambiguity surrounding generic terms, the lack of specificity on issues that allows for interpretation, the unclear guidelines on user consent, and the absence of defined standards for data processing methods.

Furthermore, the study emphasizes the challenges faced by DFS providers in enforcing these rules, suggesting that current regulatory systems are inadequate in ensuring compliance and effectively protecting consumer rights. This requires legislative revisions tailored to the specific challenges of DFS and additional consumer programs.

It is also admirable that the Proclamation creates a body overseeing organizations that handle and manage personal data. However, this authority has previous functions and obligations, and this Proclamation gives it broad and general mandates and powers. Since these institutions are new and special by nature, their alignment with protecting personal data should be observed uninterrupted, which may necessitate the creation of an institution entirely focused on them.

The research findings show that Kacha is trying to be dedicated to regulatory compliance and make mobile money services safe. However, the assessment highlights critical issues such as

ambiguities in obtaining customer consent, lack of DPO, a lack of transparency in data handling practices during the complaint resolution process, burden on data subjects for data breaches, hierarchical and locational data management issues and the need for more straightforward guidelines and greater transparency in both company policies and the overarching regulatory framework. These concerns highlight the significance of making the practice align with the law. Kacha must also establish technological and organizational measures to comply with the data protection Proclamation. However, the Proclamation does not include precise rules for establishing appropriateness, which might lead to interpretation issues. This lack of transparency may erode customers' trust in data security, increasing the risk of unwanted access or misuse.

This thesis emphasizes the significance of continuously evaluating and upgrading the legal and regulatory frameworks controlling data privacy in Ethiopia's DFS sector. Addressing identified inadequacies and improving the compatibility of the data protection proclamation with the unique issues inherent in DFS will be critical in protecting the data of the country's financial consumers.

4.2 Recommendation

In light of these findings, several recommendations are proposed to enhance Ethiopia's legal and regulatory landscape for data protection.

- Policymakers should prioritize developing comprehensive laws to address data protection issues specific to DFS, including a clear description of consent, data management, and user rights.
- Instead of depending on an authority with pre-existing, more general responsibilities, create a specialized organization to protect personal data to provide targeted, ongoing, and efficient oversight.
- Engaging stakeholders in data protection talks, including customers, service providers, and legal experts, can promote a collaborative approach to building effective policies and procedures that preserve user privacy.
- Educating consumers about their rights and data protection can increase trust in DFS.

Bibliography

Books

- EqubamariamKidaneAsegu, *'The limits of electronic banking regulation in Ethiopia' (*Editions universitaireseuropeennes 2018)
- Lloyd, Information technology law, Oxford University Press (2014)
- YimamOusman, 'Digital Financial Inclusiveness Through Financial Technology in Ethiopia: Case Study on TeleBirr Chapter' [2023] Arsi University, current debates in health science
- B Benjamin, The Consent Paradox: Accounting for the Prominent Role of Consent in Data Protection, In: Hansen, Marti Kosta, EleniNai-Fovino, Igor Fischer-Huebner, Simone (Ed.): Privacy and Identity Management. The Smart Revolution, Springer International Publishing
- Henri Arslanian and Fabric Fisher, The Future of Finance, PalgarveMacmillian , (2019)

Journals/Articles

- L. Sakala, & J. Phiri, 'Factors Affecting Adoption and Use of Mobile Banking Services in Zambia Based on TAM Model'(2019) Vol.7 No.3 Open Journal of Business and Management 1380
- AmiriMaghsoud and others, 'Evaluation Of Digital Banking Implementation Indicators And Models In The Context Of Industry 4.0: A Fuzzy Group Mcdm Approach' [2023] Article *In* Axioms first page number

- Popovič A, Boeddu G, Thorburn C, Traversa M, and Zanza A, Ethiopia Diagnostic Review of Financial Consumer Protection: Key Findings and Recommendations (2017) 1–74.
- MetagesTewabe, 'Legal Space for the Creation and Operation of Fintech in Ethiopia' (2023) 13(2) Bahir Dar University Journal of Law 323–362

Web sources

- Popov Mijail, 'Africa's Mobile Money Battle: Can M-PESA succeed in Ethiopia?' payments and Commerce Market Intelligence <https://paymentscmi.com/insights/m-pesa-ethiopia-africa-mobile-money/> accessed 09 April 2024
- Boyle Emma , 'UN declares online freedom to be a human right that must be protected' [2016] Independent< https://www.independent.co.uk/life-style/gadgets-and-tech/un-declares-online-freedom-to-be-a-human-right-that-must-be-protected-a7120186.html > accessed on 19 April 2024
- 'Reflection on the New Payment Instrument Issuers Directive' [2020] Aman and partners <https://www.aaclo.com/insight/reflection-on-the-new-payment-instrument-issuers-directive/> accessed on 20 November 2023, page 36
- 'Unveiling the Power of Mobile Money Vs. Mobile Banking' [2024] comviva<https://www.comviva.com/blog/unveiling-the-power-of-mobile-money-vs-mobile-banking/#:~:text=Mobile%20Money%20operates%20independently%20of,Q.> accessed on 13 November 2024
- KinfeMichealYilma, Data privacy law and practice in Ethiopia, International Data Privacy Law, Volume 5, Issue 3, August 2015, Pages 177–189, https://doi.org/10.1093/IDPL/IPV008 accessed on December 1, 2024.
- Enyew A, 'Towards Data Protection Law in Ethiopia' in Carlo Baldi (ed), Data Protection in Africa: A Comparative Perspective (Springer 2016) 143–159 https://doi.org/10.1007/978-3-319-47317-8_7 accessed on December 1, 2024.
- Haile Dadimos and AshenafiDereje, 'Ethiopia - Data Protection Overview', One Trust Data Guidance Regulatory Research Software <https://www.dataguidance.com/notes/ethiopia-data-protection-overview> accessed on 13 April 2024

- ‘What Is Digital Banking? Meaning, Types and Benefits’ https://sdk.finance/what-is-digital-banking/What is a digital bank? Accessed April 3, 2024

Official government publications and reports

- The Commerce Bank of Oregon, A division of Zions Bancorporation, N.A., Member FDIC, *Digital Banking Service Agreement (Consumer & Business)* (Version January 2022).
- NBE, *National Financial Inclusion Strategy-II 2021-2025* (September 2021)
- PazarbasiogluCeyla and others, *DFS*(World Bank Group, April 2020) 13.
- Maina Juliet, *Data Protection in Mobile Money* (GSMA, March 2019) 6.
- GSMA, *Mobile Money in Ethiopia: Advancing Financial Inclusion and Driving Growth* (June 2023)14.

Working papers and thesis

- HerbergJavan, ‘Injunctive Relief for Wrongful Termination of Employment’ (DPhil thesis, University of Oxford 1989)
- Gemechu Ayana, ‘Adoption of Electronic Banking System In Ethiopian Banking Industry: Barriers And Drivers’ (Degree Of Master Of Science In Accounting And Finance thesis, Addis Ababa University, School Of Business And Public Administration, 2012)
- JammoulKinana, ‘Online Banking Operations Management: Security Concerns on Trust in Mobile Banking System’ (Degree of Doctor of Philosophy, Brunel Business School Brunel University, London, United Kingdom 2016)
- B. Ababu ,' Regulation of Electronic Banking in Ethiopia: The Analysis of Legal Framework' (LL.M. dissertation, Addis Ababa University College of Law and Governance Studies, School of Law, June 2019).

Laws

- CivilCodeoftheEmpireofEthiopiaof1960,NegaretGazeta, extraordinaryissue,ProclamationNo.165,19thyear No. 2.
- FDRE, Constitution of the Federal Democratic Republic of Ethiopia Proclamation No1/1995,*Federal NegaritGazeta*, Year 1, No 1 Addis Ababa, 21st August 1995.
- NBE Establishment (as Amended) Proclamation, 2008,

FederalNegaritGazetta, Proc. No.591, 14th Year No 50.

- Licensing and Authorization of Payment Instrument Issuers Directive No. ONPS/01/2020
- Criminal Procedure Code of Ethiopia (1961), Proclamation No.185/1961, Federal NegaritGazeta
- Ethiopian Criminal Code (2004), Proclamation No. 414/2004, Federal NegaritGazeta, Year 10, No. 25
- Personal Data Protection (2004), Proclamation No. 1321 /2024, Federal NegaritGazeta 30th Year No 35

Interviews

- FetahiHailegiorgis, Infrastructure and Security manager, Kacha DFS, (Addis Ababa, April 15, 2024)
- AbrehamTilahun, CEO, Kacha DFS, (Addis Ababa, April 12, 2024)
- Gizewerkmelesse, Senior Operation Officer, Kacha DFS (Addis Ababa, April 10, 2024)
- MikiyasFekadu, Data Analytics & Mobile Money Commercial Manager, Kacha DFS (Addis Ababa, April 10, 2024)
- EndalkachewGirma, Training and Business Support Specialist, Kacha DFS (Addis Ababa, April 10, 2024)
- Tigisti, Junior Customer Support Officer, Kacha DFS (Addis Ababa, April 10, 2024)
- NatnaelBelayneh, Kacha Customer (Addis Ababa, May 10, 2024)
- BetelehemShiferaw, Kacha Customer (Addis Ababa, May 11, 2024)
- EmebetGemechu, Kacha Customer (Addis Ababa, May 11, 2024)
- FahmiMuhumed, Kacha Customer (Addis Ababa, May 11, 2024)
- TezeraTeshome, Kacha Customer (Addis Ababa, May 10, 2024)
- Daniel Techanie, Kacha Customer (Addis Ababa, May 10, 2024)
- AbdirahmanIbraahim, Kacha Customer (Addis Ababa, May 10, 2024)
- Medina Kedir, Kacha Customer (Addis Ababa, May 11, 2024)
- FissehaAbreha, Kacha Customer (Addis Ababa, May 10, 2024)
- Michael tefera, Kacha Customer (Addis Ababa, May 10, 2024)

Interview Questions

For Infrastructure and Security Manager

Pre-enactment of the Data Protection Proclamation

1. What security protocols and measures has Kacha implemented to safeguard customer data and financial transactions?
2. How does Kacha monitor security breaches or suspicious activities within its digital financial systems?
3. What are Kacha's procedures for incident response and handling security incidents?
4. How frequently does Kacha conduct security audits and assessments to evaluate its security posture?
5. What steps did Kacha's security team take to align its security protocols and practices with the requirements specified in the data protection proclamation before its approval?
6. How did the data protection proclamation influence Kacha's security procedures and incident response protocols?
7. What steps were taken to ensure compliance with the provisions outlined in the data protection proclamation?
8. What challenges do you anticipate in maintaining data security and privacy at Kacha?

Post-enactment of the Data Protection Proclamation

9. What are the top priorities for security improvement at Kacha in the coming year?
10. How has the data protection proclamation impacted Kacha's approach to security protocols, incident response procedures, and overall security posture?

11. Can you describe any specific security measures or enhancements that Kacha has implemented in response to the requirements of the data protection proclamation, and how these measures have strengthened customer privacy and data security?

For Data Analytics & Mobile Money Commercial Manager and/or the CEO

Pre-enactment of the Data Protection Proclamation

1. What motivated Kacha to enter the digital payment market in Ethiopia?
2. How does Kacha differentiate itself from other digital payment instrument issuers in Ethiopia?
3. What are Kacha's primary goals and objectives regarding customer data security?
4. How does Kacha ensure compliance with regulatory requirements regarding data protection?
5. What challenges has Kacha encountered in establishing and maintaining secure digital finance services?
6. How does Kacha plan to address emerging cybersecurity threats and challenges in the digital payment sector?

Post-enactment of the Data Protection Proclamation

7. How is Kacha advancing its data protection initiatives, particularly in response to the data protection proclamation?
8. What specific actions did the company undertake due to the approval of the data protection proclamation?

For Operations Manager and/ or Training and Business Support Specialist

1. Can you describe the operational processes and workflows ensuring privacy and data security at Kacha?
2. How does Kacha manage customer data throughout its lifecycle, from collection to storage and processing?
3. What role does the operations team play in ensuring compliance with regulatory requirements related to privacy and data protection?
4. How does Kacha handle customer inquiries or complaints regarding privacy or security concerns?
5. Can you discuss recent operational improvements or initiatives to enhance security and efficiency?
6. How does Kacha ensure operational procedures align with data protection policies and protocols?
7. What are the key operational challenges Kacha faces in delivering secure digital finance services and providing secure operational supports to customers?

For Senior Operations Officer

1. Could you explain the different channels through which Kacha receives customer complaints?
2. What are the most common types of complaints that Kacha encounters?
3. Could you elaborate on the factors that contribute to delayed resolution of disputed transactions?
4. How does Kacha ensure the security and confidentiality of customer data during the complaint handling process?
5. In your experience, what are the main challenges customers face when reporting complaints, and how does Kacha address them?
6. Can you provide insights on how Kacha communicates the resolution of complaints to customers?

For Customers

1. What are your primary concerns when using Kacha's services?
2. Can you describe your understanding of the consent process when using Kacha's application or service?
3. How do you perceive the importance of reading and understanding the terms and conditions before giving consent?
4. As a DFS consumer, how do you perceive the sensitivity and personal nature of the information you provide during the registration process?
5. Can you describe your experience filing a complaint with Kacha?