PARADIGM INITIATIVE

AN ANALYSIS OF DATA PRACTICES OF DIGITAL LENDING APPLICATIONS IN AFRICA

A REVIEW OF 19 COUNTRIES

AN ANALYSIS OF DATA PRACTICES OF DIGITAL LENDING APPLICATIONS IN AFRICA

A REVIEW OF 19 COUNTRIES

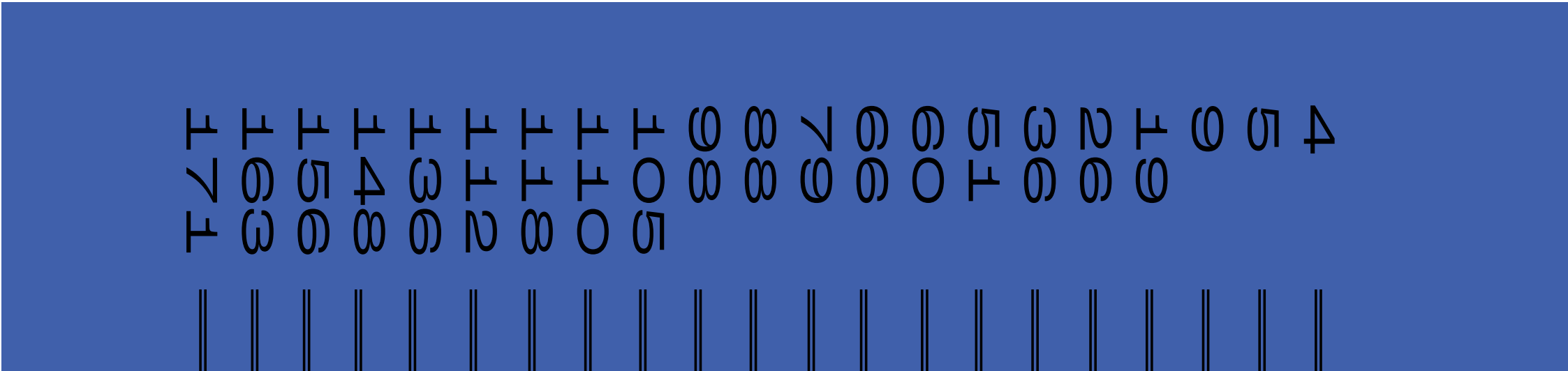
June 2022.

Authors: 'Gbenga Sesan, Bonface Witaba, Dércio Tsandanza, Jackline Akello, Steven Akomian
Copy Editor: Nana Nwachuckwu

Paradigm Initiative
374 Borno Way
Yaba
Lagos, Nigeria
hello@paradigmhq.org

PARADIGM INITIATIVE
@ParadigmHQ

Contents



Introduction

With the proliferation of digital infrastructure across African countries, there has been an increase in internet access. The regulation of telecommunications companies supports a reduction in connection costs, thereby increasing the number of internet users. Sharing information, including personal data, has become more accessible and widespread with this increase. With ease came concerns of abuse of access to personal data by corporations, identity theft by individuals, and malicious targeting using personally identifiable information. The European Union responded to these concerns on the safety of personal data by enacting the General Data Protection Regulation (GDPR). Across the world, it has spurred countries to enact comprehensive data protection laws and establish data protection authorities.

The GDPR came into effect in 2018, impacting thousands of businesses located in Africa due to globalization and the ordinary fact that these businesses process data belonging to EU residents. With the GDPR, e-commerce websites or targeted advertising providers and their Africa-based processors became subject to the new provisions, particularly the international transfer of personal data. This new regulation means that the EU required high standards of data protection regulations from African countries to guarantee the safety of personal data of its residents and citizens for a free flow of data between the two continents.

Four years after the European Union enacted the General Data Protection Regulation (GDPR), many African countries still struggle with guiding principles for data protection. While more than 20 countries in Africa have enacted data protection laws, with the latest countries being Rwanda, Nigeria, South Africa, Kenya, Morocco, and Ghana, some gaps allow technology-driven corporations unfair access to data that falls through the loopholes of protection. Without adequate protection for personal data, new financial corporations ('fintechs') are capitalizing on the availability of this data to target vulnerable digital natives and migrants with 'payday' loans. These loans are small loans offered via mobile lending applications or websites to eligible persons through targeted adverts. These loans are often double-digit loans. The loans are approved without background checks in exchange for personal data, including but not limited to employer information, mobile phone contact lists etc. Collection for defaulting on these loans use a 'public shame' mechanism.

Paradigm Initiative studied data protection and lending applications in nineteen (19) African countries. This report details these countries' data protection laws, the protection loopholes exploited by these 'fintechs', and the types of personal data exposed and collected by these lending app corporations.

Angola

Country Profile

Located in Southern Africa, Angola is a Portuguese-speaking country with an estimated population of 31 million people[1] with an estimated GDP of 208.034 billion as of 2019. The South African Lusophone nation gained its independence from Portugal in 1975.[2] The current President, João Lourenço, was elected in 2017, after more than 30 years of governance by the previous head of state, José Eduardo dos Santos.

1 Angola stats, World Bank https://data.worldbank.org/country/AO > accessed 15 August 2021.
2 Barrow Munslow, 'Angola: The Politics of Unsustainable Development' (1999) 20(3) Third World Quarterly 551-568.

Data Protection in Angola

According to DLA Piper,[3] Angola regulates data privacy and protection issues under the Data Protection Law (Law no. 22/11, 17 June 2011),[4] the Electronic Communications and Information Society Services Law (Law no. 23/11, 20 June 2011)[5] , and the Protection of Information Systems and Networks Law (Law no. 7/17, 16 February 2017).[6]

Data Guidance notes[7] that Presidential Decree 214/16 of 10 October 2016 establishes rules that govern the structure and operation of the regulatory body, the national Data Protection Agency (APD).[8] Angola has also enacted Law 11/20 of 23 April 2020 on the Identification and Location of Cellular Phones[9] , and Electronic Surveillance[10] carried out by Police Authorities.

Angola has three mobile phone companies, Movicel, Unitel, and the state-owned company

3 https://www.dlapiperdataprotection.com/index.html?t=law&c=AO > accessed 15 August 2021.
4 https://platform.dataguidance.com/sites/default/files/lei_de_proteccao_de_dados_pessoais_v.pdf > accessed 15 August 2021.
5 https://minttics.gov.ao/fotos/frontend_10/gov_documentos/lei_das_comunicacoes_electro_19324146535f1886da78b9b...s_sociedade_da_informacao.pdf > accessed 15 August 2021.
6 https://minttics.gov.ao/fotos/frontend_10/gov_documentos/redes_e_sistemas_informaticos_20864175955f109a14374be.pdf > accessed 15 August 2021.
7 https://www.dataguidance.com/notes/angola-data-protection-overview > accessed 12 August 2021.
8 https://apd.ao/ao/ > accessed 13 August 2021.
9 https://apd.ao/fotos/frontend_1/editor2/200420_lei_11-20_de_23_abril-identificacao_celular_vigilancia_electronica.pdf > accessed 13 August 2021.
10 https://apd.ao/fotos/frontend_1/editor2/200222_lei_2-20_de_22_janeiro-videovigilancia.pdf > accessed 13 August 2021.

Angola Telecom, which had a telephone service monopoly until 2005. Internet penetration in Angola is 31%, while mobile phone access stands at more than 15 million users, representing 46% of the total population. [11]

Freedom on the Net 2020 report[12] rates Angola's "Internet freedom status" as "partly free."[13] There are no government restrictions on access to the Internet. Aside from child pornography and copyrighted material, the government does not block or filter Internet content. There are no restrictions on the type of information exchanged online.

Financial System and Fintech in Angola

The National Bank of Angola (BNA) is the primary entity that manages the financial sector in Angola. Regarding electronic transactions, the highlight is the Law for the Prevention and Combat of Money Laundering, Terrorist Financing, and Proliferation of Weapons of Mass Destruction.[14] It stipulates that financial institutions that allow wire transfers shall include duly verified information in the message or payment form accompanying the transfer, including full name, account number, address, and, where applicable, the name of the originator's financial institution. There is minimal regulation about mobile apps like Xikila Money.

On 26 July 2021, AllAfrica reported[15] that Angola had emerged as the most vulnerable country as professional cybercriminals worldwide target Africa's burgeoning population of mobile phone users. According to the "State of Mobile Fraud in Africa" report,[16] Angola is one of the most vulnerable countries in Africa, where 34 per cent of mobile transactions are suspicious.

The report also explained[17] that malicious apps secretly contain malware and are programmed to make payments on behalf of users without their knowledge. There is also clickjacking, where a fraudster intercepts a legitimate click and unknowingly directs the user to a website to steal. This website can steal sensitive financial and other personal details.

Statista reported[18] that as of March 2021, 29.4 million mobile banking transactions were registered in Angola, a substantial increase compared to the same month in the previous year. People did 7.4 million bank operations with a mobile device in March 2020 on the App Multicaixa Express, launched in 2019. After setting up one or more debit cards on the App, the user can use a mobile device to execute online payments, purchases, and transfers.

11 Digital 2021 in Angola – Hootsuite https://datareportal.com/digital-in-angola, accessed on 20 May 2021.
12 Freedom House Angola https://freedomhouse.org/country/angola/freedom-net/2020, accessed on 1st June 2021.
13 Angola scored 62/100 points https://freedomhouse.org/country/angola/freedom-net/2020 > accessed 14 August 2021
14 Law No. 05/2020 of 27 January https://www.bna.ao/uploads/%7B5ff3bf3f-eba6-4b79-94e4-f16d8a01e74c%7D.pdf > accessed 12 August 2021
15 https://allafrica.com/stories/202107260738.html > accessed 13 August 2021.
16 https://www.techfinancials.co.za/2021/07/26/mobile-fraud-continues-to-hit-africa-hard/ > accessed 15 August 2021.
17 https://www.bizcommunity.africa/Article/410/793/218325.html > accessed 15 August 2021.
18 https://www.statista.com/statistics/1228848/number-of-transactions-with-mobile-banking-in-angola/ > accessed 15 August 2021.

Xikila Money: The Money Lending Mobile Application

Launched in 2017 by Banco Postal,[19] Xikila Money was a platform that allowed using the mobile phone as a digital wallet and, on that basis making various payments via mobile. The application uses mobile phones as bank accounts to make financial transactions and issue loans.[20] To start using the Xikila Money service, opening an account at a Xikila Money branch and making a deposit is necessary. The application is available for Android and iOs users.[21]

Suspension of the Application

The platform seemed to have been successful in Angola. In a news report published in 2017,[22] the Angola Journal mentioned that the App had already reached 100,000 clients in seven months, increasing over 40,000 accounts in just two months. However, a decision by the Central Bank of Angola (BNA) changed the story in 2019.

The main reason announced by the BNA was Banco Postal's inability to comply with the financial liquidity required to operate in Angola.[23] Banco Postal had 200 local points of the Xikila Money network in the capital Luanda, and the city of Huambo[24] and the bank claimed to have over 250,000 customers before its closure. At the moment, the Xikila Money website no longer works.[25]

Analysis of the Apps

Xikila Money	Information Collected and Processed by the App	
	Permissions sought	Since the application was associated with a Bank, one of the main permissions required was the personal identification of the client and its financial transaction history.
	Information collected from the user	Read phone status and identity Approximate location (network-based) Precise location (GPS and network-based) Find accounts on the device Read users contacts Find accounts on the device
	Information collected from the user's device	Receive data from the Internet View network connections Full network access Close other apps Control vibration Prevent device from sleeping

19 https://www.menosfios.com/conheca-xikila-money-um-servico-permite-efectuar-pagamentos-via-mobile/ > accessed 11 August 2021.
20 Xikila Money – New financial service changes face of banking in Angola https://www.youtube.com/watch?v=PW392kJVm7w > accessed 14 August 2021.
21 https://play.google.com/store/apps/details?id=tagattitude.mwallet.app.xikila and https://appadvice.com/game/app/xikila-money/1261392972 > accessed 14 August 2021.
22 https://www.jornaldeangola.ao/ao/noticias/detalhes.php?id=393253 > accessed 14 August 2021.
23 https://novojornal.co.ao//sociedade/interior/bna-tambem-fechou-o-xikila-money-um-servico-bancario-inovador-em-angola-e-de-utilidade-confirmada-pelos-utilizadores-65247.html > accessed 16 August 2021.
24 News report https://sol.sapo.pt/artigo/650953/joao-lourenco-limpa-sistema-bancario > accessed 12 August 2021.
25 http://www.xikilamoney.co.ao/ > accessed 14 August 2021.

	Use of user's information by the App	Read phone status and identity View Wi-Fi connections Record audio – The App requires a Microphone for secure validation of transactions
	Storage of user information by the App	ID information Bank account Transactions with other users

The withdrawal of the Postal Bank licence and the banning of the Xikila Money app limits our analysis. However, we were able to note through Google Play that the last update to the App was made in May 2018, almost a year before it was banned by the Angolan government, especially since the terms and conditions of use should contain the privacy policy are inaccessible.[26] On the one hand, the lack of a website did not allow access to more data on how third parties authenticate cookies' or track user information.

Although it remained on the Angolan market for a short period, Xikila Money represented a new method of circulating finance in Angola. From the information obtained in what remains of the application, we note a large volume of data collected from its users. An important thing to note is the silence on the Data Protection Agency during the time Xikila Money was operating in the country. There is no record that the DPA ever commented on how the App collected and used information from its clients.

For example, one of the main problems that still prevails today is that some clients and workers have lost their accounts and are still waiting for compensation from Banco Postal.[27] Article 16 of the Data Protection Act states that "the processing of personal data regarding credit and solvency can only be carried out with the consent of the data subject and with the authorisation of the Data Protection Agency." However, this did not happen, and Xikila Money customers are still unaware of the future of their data after the ban of Banco Postal.

26 http://www.xikilamoney.co.ao/TermosUtilizacao > accessed 17 August 2021.
27 https://www.novagazeta.co.ao/artigo/1186 / https://valoreconomico.co.ao/artigo/80-dos-trabalhadores-do-extinto-banco-postal-continuam-no-desemprego > accessed 17 August 2021.

Cameroon

Country Profile

Located in Central Africa, Cameroon, or the Republic of Cameroon, has 25,876,380 inhabitants[28]. It shared a border with Nigeria, Chad, the Republic of Central Africa, Congo, Gabon, Equatorial Guinea, and a maritime opening on the Gulf of Guinea. Two official languages: French and English, are spoken there. Its GDP is estimated at 39.01 billion USD (2019) and represents more than 40% of that of the Economic and Monetary Community of Central Africa, of which it is a member. It practices a presidential system.

28 countryeconomy.com. 2022. Cameroun. [online] Available at: <https://fr.countryeconomy.com/pays/cameroun> [Accessed 11 February 2022].

Data Protection in Cameroon

Cameroon does not have a precise legal framework adapted to protect personal data. Pending the establishment of legislation and the appointment of an independent body responsible for protecting personal data, only electronic communications and the ICT market are regulated. The regulations emanate from the following texts:

- Law no.2010 / 012 of December 21, 2010, relating to cybersecurity and cybercrime,
- Law no.2010 / 013 of December 21, 2010, governing electronic communications,
- Law no. 2010/021 of December 21, 2010, governing electronic commerce,
- Law no 2006/018 of December 29, 2006, governing advertising, and
- Law n ° 2011/012 of May 6, 2011, on consumer protection.
- At the regulatory level, Decree no 2013/0399 / PM of February 27, 2013 sets the terms for protecting consumers of electronic communications services.
- Cameroon has ratified the African Union (AU) Convention on Cybersecurity and Personal Data Protection of June 27, 2014, at the continental level.
- And at the community level, Cameroon has adopted Directive No 07/08-UEAC-133-CM-18 and Regulation No 03/16-CEMAC-UMAC-CM of December 21, 2016, relating to systems and incidents of payment which deal with questions relating to personal data collected during relations transactions relating to various electronic communication services.

.

The Telecommunications Regulatory Agency (ART)[29] and the National Agency for Information and Communication Technologies (ANTIC)[30] manage these different regulations. Still, they have a narrow margin of action on protecting personal computer data. Indeed, the protection of personal computer data by ART appears to be an incident in its regulatory missions and remains limited to the telecommunications sector, which is not the only one where personal data may be restricted. The ANTIC finds its origin in the law on electronic communications, although the law has specified its field of intervention on cybersecurity and cybercrime. The analysis of these missions suggests that they cover the protection of personal computer data in their rather broadly worded tasks. However, on closer inspection, the missions do not reveal a particular qualification of ANTIC in the protection of personal data. The law on cybersecurity and cybercrime of 2010 is restricted to personal data protection at the criminal level. This restriction is because it is impossible to intervene in the event of a contentious activity relating to the protection of personal data, both for the criminal and administrative judges [31]. This restricted process suggests abuses in the processing of personal data in Cameroon.

Introduction

The almost generalized development of Mobile Money (MM) in Sub-Saharan Africa (SSA) is struggling to impose itself in Central Africa[32]. According to the 2019 report from the World Association of mobile operators(GSMA), about 400 million active accounts in SSA, fewer than 10% were located there. Cameroon dominates the other countries in terms of MM development in this zone. Its MM penetration rate is 15%, and the volume of associated transactions represented 76% out of 7,964 billion FCFA achieved in 2018 in Central Africa.

Due to MM's activities, transactions are mainly carried by mobile telephone operators, namely Orange Cameroon and MTN Cameroon. These two leaders of the mobile telephony market in Cameroon achieved a cumulative turnover of 500.3 billion FCFA during the year 2020. According to Orange Cameroon, the Orange Money service launched in 2011 represents a turnover of 9,600 billion FCFA per year, that is to say nearly twice the budget of the State of Cameroon during the financial year 2021. At the end of 2020, MTN Cameroon achieved a 1.73 billion rand (about 66 billion FCFA) turnover. These two operators offer more than 20 million mobile telephone subscribers in Cameroon, deposit and withdrawal activities, money transfers, bill payments, salaries, and all that is merchant payment, etc., from their accounts MM. Aware of the potential of this market, they decided to turn to microcredit activities. Orange Money Cameroon, therefore, submitted a request for

29 The Telecommunications Regulatory Agency (ART) is a public administrative establishment with legal personality and financial autonomy, created by the law on electronic communications. As a public administrative establishment, ART is under the administrative supervision of the Ministry of Posts and Telecommunications (MINPOSTEL) and under the financial supervision of the Ministry of Finance (MINFI). Its creation is governed by Decree n ° 2012/092 and n ° 2012/180 of April 2012 on the creation, organization and functioning of the National Agency for Information and Communication Technologies.

30 ANTIC a public administrative establishment endowed with legal personality and financial autonomy whose main missions are to ensure on behalf of the State: the promotion and follow-up of the action of the public authorities in matters of Technologies Information and Communication (ICT); regulation, control and monitoring of activities related to the security of information systems and electronic communications networks as well as electronic certification in collaboration with ART.

31 Article 74 of Law n ° 2010/012 of December 21, 2010 relating to cybersecurity and cybercrime.

32 Central Africa brings together the 6 countries of the Central African Economic and Monetary Community (CEMAC): Cameroon, Central African Republic, Congo, Gabon, Equatorial Guinea and Chad. And the Democratic Republic of Congo (DRC).

approval in 2019 to develop its services by moving towards micro-credit. MTN Cameroon is finalizing a similar approach at the end of 2020. Fintechs and companies of the economic and banking ecosystem not domiciled in Cameroon are driving these mobile application based loan-offers. These applications are Treoloans App[33], Cameroon Direct Loan Hub[34] and Kiva[35].

In a macroeconomic environment without a fundamental regulatory framework for personal data protection, the proliferation of these offers, beyond the expected benefits on financial inclusion, can pose problems for their users' privacy. The question is whether the data processing practices of these applications, as defined in their policies and conditions of use, take into account the interest of respect for the protection of privacy? This study aims to analyze the privacy policies and the terms and conditions of these applications and examine their compliance with the various laws related to protecting consumers (users) in Cameroon. The first part includes an overview of the data collected by these applications. The second part examines their processing activities concerning the various laws related to consumer protection. The last part ends by indicating whether or not these applications comply with the law protecting personal data.

Overview of data collected by digital credit applications in this study

TreoLoans App[36] Download link: Google Play Store	Information collected and processed by the application

33 Treoloans App is a mobile application for obtaining unsecured loans between 5,000 and 30,000 FCFA (approximately US $ 9) and at monthly interest rates between 10% and 30% in Cameroon. It is offered to individuals with MM accounts with the mobile operators Orange Money Cameroon and MTN Money Cameroon from April 2019.

34 Cameroon Direct Loan Hub is an offering of EasyLoan for digital loans. Basically, EasyLoan does not lend its own funds but simply provides a platform for loan providers and applicants to connect. Its objective is to do away with the traditional banking protocol between agents in need of financing and agents with financing capacity.

35 Kiva App is an offer of Kiva US for digital loans. Kiva is a crowdfunding platform that allows loan providers and applicants to easily connect and interact. Its objective is to do away with the traditional banking protocol between agents in need of financing and agents with financing capacity. Members of the Kiva offer can benefit from loans starting at $ 25. Currently, the Kiva community is made up of 1.9 million people who have benefited from crowdfunding estimated at $ 1.4 billion in loans to 3.4 million borrowers in over 90 countries.

36 Terms and Conditions of TreoLoans App. The TreoLoans Privacy Policy is contained in the Terms and Conditions.

	sought Permissions	When starting the application, TreoLoans App asks. Access the user's position, precise position (GPS and network) and approximate position (network). • Access the camera to take photos and shoot videos • Access user identity information and search for accounts on the user's device • Access Photos / Multimedia / Files, edit or delete the contents of the USB storage memory and play the contents of the USB storage memory. • Access users' phone numbers, view and edit contacts search for accounts on the device and directly call phone numbers. • Access storage, edit or delete the contents of the USB storage memory, and play the contents of the USB storage memory. • Access the Microphone and record an audio file. • Access Wi-Fi connection information and view Wi-Fi connections • Perform various actions: receive data with the internet connection, run on startup, prevent the device from going to sleep, change audio settings, view network connections and have full network access
	Information collected from the user	When subscribing to the loan service, TreoLoans App collects personal information about the user without specifying the nature or the quality of this data.
	Information Collected from the User's Device Information collected using the website	TreoLoans App collects various information about a user's device without specifying the data type. TreoLoans provides no information on the website
	Information received from third parties	The App gives no Information on data obtained from various third parties.
	The App's use of user information	The TreoLoans privacy policy states that it collects user data for various purposes not specified in its privacy policy.

	Information Shared with Third Parties Duration of Data Access to Third Parties	TreoLoans shares user information with various third parties not specified in its privacy policy. The TreoLoans privacy policy states that it shares information with third parties without specifying the duration of data access granted to them.
	Tracking Technologies / Website Cookies	The TreoLoans privacy policy and website are silent on the use of cookies.
	Storage of User Information by the App	The TreoLoans Privacy Policy states that they take every measure to ensure the security of data collected about users. However, they provided no information on the storage period of the data collected.

Cameroon Direct Loan Hub[37] External Download Link and Google Play store	information collected and processed by the application	
	Sought Permissions	When starting the application, Cameroon Direct Loan Hub asks. View network connections and get full network access
	Information Collected from User	Cameroon Direct Loan Hub's privacy policy is silent on the information it collects from users.
	Information Collected From User's Device Information Collected While UsingWebsite Cameroon Direct Loan Hub'sCameroon Direct Loan Hub	Cameroon Direct Loan Hub's privacy policy does not say anything about information collected on a user's device. Cameroon Direct Loan Hub's privacy policy is silent on information collected from its website. In addition, the website of the application provider is not accessible.
	Information received from third parties	Cameroon Direct Loan Hub's privacy policy does not say anything about information from various third parties.
	Use of user information by the App	Cameroon Direct Loan Hub's privacy policy does not say anything about the purpose of the data collected from users.
	Information shared with third parties Duration of data access to third parties	Cameroon Direct Loan Hub's privacy policy does not say anything about the information shared with third parties. Cameroon Direct Loan Hub's privacy policy is silent on how long third parties can access users' personal information and how long they keep it.
	Tracking Technologies / Website Cookies	Cameroon Direct Loan Hub's privacy policy is silent on using "cookies". In addition, the website associated with the application is not functional.
	Storage of user information by the App	Cameroon Direct Loan Hub's privacy policy does not say anything about the data collected's security, confidentiality, and retention period.

37 Cameroon Direct Loan Hub and the provider of its application do not have a Privacy Policy.

Kiva[38] Download Link: Google Play Store and Apple Store	information collected and processed by the application	
	Sought Permissions	When starting the application, Kiva App asks. Receive data from the Internet . View network connections . Benefit from full network access . Prevent the device from going to sleep Kiva App also reserves the right to add further permission requests for its user interface.
	Information collected from the user	When subscribing to the loan service, Kiva App collects the user's information: first and last name, photo, email address and physical address, telephone number, company description and finances, personal references, desired loan terms, payment account and some demographic information, user social media information.
	Information Collected From User's Device Information Collected While Using the website Kiva	Kiva App collects the following information from a user's device: device information including mobile type and phone number current location information provided by GPS technology and other location services User payment account credentials Once a user uses the website Kiva App on their mobile phone, the name, email address and a means of authenticating the account to the user (for example, a password) are collected. Information and comments posted on any other web page hosted by Kiva (such as a loan page, blog, or volunteer forum) or through the Kiva Lender Mail feature are also collected.
	Information received from third parties	The App obtains information from other Group entities, Kiva (subsidiaries), Credit Assessment Bureaus (BIC), Mobile network providers, collection agencies, business partners, etc.

38 Privacy Policy of Kiva App

	The App's Use of User Information	privacy policy Kiva's states that it collects user data for the following purposes: Verifying a user's identity Processing a user's transactions Credit and models in Loan scoring disbursements and payment collection Obligations of Kiva towards users Compliance with applicable regulations regarding KYC "Know Your Customer", AML "Anti-money laundering", and CFT (Combating the Finance of Terrorism) requirements Promotional communications and marketing services
	Information shared with third parties Duration of data access to third parties	Kiva shares user information with: Its subsidiaries, its parent and other subsidiaries of our parent company ("its group") Anyone acting on behalf of a user From credit bureaus or other financial institutions Business partners in business transfers, disposals, mergers & acquisitions, etc. Third-party service providers including GAFA (Google, Facebook, etc.) and Twitter. The privacy policy states that it shares information with third parties for a reasonable period without explicitly specifying the length of this period.
	Tracking Technologies / Website Cookies	The Kiva Lending Service uses cookies, web beacons, and other automated systems to collect data about user behaviour. The App specifies these elements in its cookie policy. With these tools, Kiva App and its website retrieves information independently and through third-party tools and programs (such as Google Analytics). The data collected include certain technical information (e.g. your path to the website, pages visited, original IP address, device type, browser type, browser language, type of network connection, and the date and time of your visit).

	Storing User Information by the App	Kiva collects and stores all data in the United States. Kiva, affiliates, service providers, its agents and representatives in the United States or elsewhere in the world can view this personal information. Kiva is also committed to respecting its privacy policy, regardless of where your personal information is processed or processed. Kiva's privacy policy also states that it takes reasonable steps to maintain appropriate physical, technical and administrative security to help prevent the loss, misuse and unauthorized access, disclosure or modification of information.

Case study: Building and making available databases on the credit history of Kiva customers.

Kiva's development model facilitates the provision of small loans in more than 80 countries by connecting individuals in need of finance and those with financing capacities. To do this, Kiva makes available databases of beneficiary credit histories as part of an extensive online credit system. These databases, which are freely accessible, result from the collection of personal data (surname, first names, sex, credit history, etc.) of users. This practice is not clearly stated in Kiva's privacy policies and may lead to abuse. Also, the consent given by users when subscribing to Kiva loan offers should not justify the communication of their data to other users. Hence, the Cameroonian State needs to establish regulations and an authority dedicated to protecting personal data.

In addition to the issue of sharing information on the credit history of Kiva users, Cameroonian lawmakers must also address the relationship between Kiva and certain digital giants: Facebook, Google and Apple. Indeed, Kiva's privacy policy states that when users connect to their website via their Facebook account, account information (email address, account photo, list of Facebook friends who also use Kiva) is collected. Through this facility, Facebook can obtain Kiva users' lending activities the user giving explicit consent. This practice also happens with Google and Apple accounts.

Analyzing Data Protection Practices of Digital Loan Applications Vis-À-Vis Laws on the Protection of Consumer Rights in Cameroon.

As Cameroon does not have legislation dedicated to protecting personal data, it is not easy to analyze the practices of digital lending applications in the light of existing texts. The laws on consumer protection and those relating to the security of electronic communications do not serve the purpose of digital law. This deficiency provides a fertile ground for the unlawful processing of personal data and the violation of the digital rights of users of digital

lending applications and all other activities of this kind.

The various aspects of Cameroon's digital credit applications' data processing practices do not comply with international principles and standards for personal data protection. Dedicated legislation and authority are needed to force the data controllers of these applications to adopt more responsible data privacy policies. As soon as a legally backed body is established for this purpose, it should have the material and technical skills required to perform its duties. These resources will enable it to monitor in real-time the volume, quality and quantity of data collected by data controllers of mobile applications and other data processors.

Cape Verde

Country Profile

With an estimated population of 550,000 and a GDP of 4.323 billion as of 2019, Cabo Verde, also called Cape Verde, comprises ten volcanic islands that lie 385 miles (620 km) off the west coast of Africa. Praia, located on Santiago island, is the capital of Cape Verde. Cape Verde consists of nine inhabited islands, one uninhabited island, and various islets. The islands remained a Portuguese colony until 1975[39].

39 Carling, Jørgen, and Luís Batalha. 'Cape Verdean Migration and Diaspora' in Transnational Archipelago: Perspectives on Cape Verdean Migration and Diaspora, Carling Jørgen and Batalha Luís (eds) (Amsterdam University Press, 2008) 13-32.

Data Protection in Cape Verde

Cape Verde provides individuals with several constitutional and statutory rights to personal data protection. The Constitution contains significant provisions for data protection and provides an additional legitimacy layer. Cape Verde has two important laws on data protection: Law 133-V-2001 on the Protection of Personal Data (as amended by Law No. 41/VIII/2013 - General Legal Regime for the Protection of Personal Data of Individuals (only available in Portuguese here) and Law No. 121/IX/2021 of 17 March 2021. In 2001, Cape Verde passed its pinnacle data protection law, Law No. 133.

Since then, the law has gone through several changes. In 2013, the parliament passed Law No. 41 to supplement and update Law No. 133. More recently, in March 2021, the parliament passed Law No. 121 to detail the responsibilities of the Cape Verdean data protection authority, known as the Comissão Nacional de Proteção de Dados Pessoais (CNPD). Cape Verde's data protection legal regime draws inspiration from Europe.[40] The Data Protection Act ('the Act') covers data processing through automated and non-automated means by entities established in Cape Verde or collecting or transmitting personal data through any means in the country.

40 https://dataprotection.africa/cape-verde/ and https://www.dataguidance.com/notes/cape-verde-data-protection-overview > accessed on 2nd August 2021.

Fintech and financial system in Cape Verde

Bank of Cape Verde's first intervention as a payment system regulator was in 2018 when the Bank launched Makeba's money lending mobile application. The reform of the regulatory framework of the Cape Verdean Payment System, Decree-Law No. 7/2018, of 28 November,[41] regulated matters relating to the guiding principles that any payment system operating in the country must observe to ensure efficiency and security. One of the principles listed in Article 10 of the decree-law refers to defining security policies and mechanisms to ensure operational reliability in a payment system, including mobile payments.

On 17 June 2021, the Bank of Cape Verde[42] published a regulation to establish the basic requirements to boost efficiency and security in implementing Mobile Payment Services in Cape Verde.[43] Article 1 states that it seeks to establish the minimum and standard security requirements applicable to the safety of mobile device payments that must be observed by Payment Service Providers (PSPs).

Article 4 refers to security issues and highlights that the design of the Mobile Payment Service should focus on mechanisms that allow the transmission, processing or storage of sensitive information safely and securely. It also defines policies and the adoption of measures to prevent and detect information modification or tampering. It added that Payment Service Providers (PSPs) should implement reliable processes for monitoring transactions and systems to identify abnormal payment profiles and prevent fraudulent acts.

One of the provisions that caught our attention is Article 6 of the same regulation. Bank of Cape Verde states that the mobile payment service provider must ensure robust customer authentication procedures for payment authorisation according to the definition provided in this regulation. The same bank highlights that payment service providers must ensure that the service provided incorporates secure mechanisms for recording transaction data. The instrument should include a reference that allows the identification of the payment operation, the date and time of execution, changes in parameter settings and access to data, allowing traceability of transactions at any time.

Finally, the implemented processes and log files should identify and trace the source that initiates payment (point of sale, internet) and the beneficiary (merchant). We note that it is a measure that gives service providers excessive power in tracing their customers' information.

41 Decree-Law No. 7/2018, of 28 November https://www.bcv.cv/pt/O%20Banco/Sectores/Documents/2018/Bo_28-11-2018_78.pdf > accessed on 29 July 2021.
42 Bank of Cape Verde https://www.bcv.cv/pt/Paginas/Homepage.aspx > accessed on 2nd August 2021.
43 Regulation 3/2021 of 17 of June on Mobile Payment Services https://www.bcv.cv/pt/O%20Banco/Sectores/Documents/2021/Legis%2030.07.2021/Aviso_3-2021.pdf.pdf#search=aplica%C3%A7%C3%B5es%20m%C3%B3veis > accessed on 28 July 2021.

Makeba: The Money Lending Mobile Application

The application arrived on the Cape Verdean financial market in 2018.[44] Users can download the App on either iOS or Android systems.[45] It is an application that allows users to make withdrawals and loans or deposit money at BAI-CV[46] or participating Makeba Merchants. As the application indicates, Makeba works by reading a QR code or biometric data. Still, it does not specify what personal data is accessed, especially since the Agent that manages the application reads the data and not necessarily the customer. In other terms, the user must hand over his mobile phone to the manager to read the data before depositing or lending the money.

During its launch, Makeba CEO Yamandou Alexander explained[47] that the App would bring greater ease and dynamics in business. However, more than two years later, there is little to prove that it is revolutionising the financial market in Cape Verde, as suspicions remain about how the App works. It is unknown how many clients it has and the current monetary balance of transactions since its implementation began in Cape Verde.

Analysis of the lending App

<table>
<tr><td rowspan="2">Makeba[48]</td><td colspan="2">Information Collected and Processed by the App</td></tr>
<tr><td>Permissions sought</td><td>By accepting the contract, BAICV undertakes to provide the user with the MAKEBA service under the conditions and terms outlined in the clauses of the agreement. The user authorises the debit entry to their current account at the Bank. This debit entry reflects the amounts corresponding to the payments they make through the MAKEBA service and the credit or debit entry of the sums related to the bank transfers that they receive or order, respectively, through the MAKEBA service.</td></tr>
</table>

44 https://www.makeba.money/cv-por/howitworks.html > accessed on 1st August 2021.
45 iOS – https://itunes.apple.com/pt/app/makeba-money/id1458893785 and Android – https://play.google.com/store/apps/details?id=money.makeba.makebamoney&hl=pt_cv > accessed on 3 August 2021.
46 https://www.bancobai.cv/particulares/produtos-e-servicos/servico-de-pagamento/makeba > accessed on 3 August 2021.
47 https://expressodasilhas.cv/eitec/2018/12/14/app-que-permite-transferir-dinheiro-e-pagar-online-e-lancada-para-a-semana/61403 > accessed on 28 July 2021.
48 Privacy Policy – https://www.makeba.money/cv-por/terms.html / https://www.makeba.money/app/terms/terms-money-cv-por.html > accessed on 10 August 2021.

	Information collected from the user	Identity Card. National Identity Card, Passport, Residence Permit. Taxpayer Identification Number, country/city of birth, address, town, post office box, telephone, mobile and e-mail The obligation to provide the MAKEBA service will only take effect upon confirmation, by BAICV or by a third party on its behalf and in its name. This confirmation will show that the MAKEBA service has been activated (through communication to the user that the MAKEBA service is active). The BAICV will issue confirmation upon the user's acceptance of the terms and conditions. This is done through the mobile telephone number provided by the user while subscribing to the MAKEBA service For BAICV to provide the MAKEBA service to the user, the user will have to acquire the authorisation of use and install the MAKEBA application on a mobile device with an iOS or Android operating system. The obligation to provide the MAKEBA service is only compelling if and as long as the client cumulatively: a) Keeps the mobile number supplied active on their mobile device. b) Keeps the credentials the client uses to carry out MAKEBA transactions active at the time of each use. c) Ensure that the client receives the push notification requesting confirmation of the MAKEBA transaction on the mobile device the client has installed the MAKEBA application.

	Information collected from the user's device	The user authorises BAICV to process the personal information provided by the User to BAICV. This authorisation is in connection with the execution and maintenance of this contract. It includes information provided during installation and in using the MAKEBA application, directly or indirectly, the purpose of which is to provide the MAKEBA service by BAICV to the user. Personal data are collected using the KYC (Know Your Customer) procedure following the Personal Data Protection Act and other applicable legislation in force in Cape Verde. The processing of personal data provided by the user to the Bank in connection with the conclusion and maintenance is also done under the Personal Data Protection Act in force in Cape Verde. Although the owner of the MAKEBA application does the data processing, it is the latter who defines the purpose and means of the processing, being the entity responsible for it. Users accept that, within legal limits, the records made by the computer system through which the MAKEBA service is provided and which relate to the operations carried out by the user will be used by BAICV for purposes of proof, provision of statistical or aggregate information, or others.
	Information collected from the use of Makeba's website	The website does not ask for cookie authentication.
	Information received from third parties	Financial information (bank account) Tax Identification Number (TIN).

	Use of user's information by the App	Each user is associated with a single cell phone number and a single Tax Identification Number (TIN). In MAKEBA transfers ordered by the user, the latter acknowledges that the recipient will only receive the funds transferred when they are already a user or become a user for this purpose. The user authorises BAICV to transmit their details to the company MAKEBA INC, with registered offices in the United States of America, and the companies of the BAI group. There is a caveat refraining the company from using them for any purpose other than that they were collected and protecting them from unauthorised disclosure or access. It also prevents the Holder access to the details above for their rectification, updating, and elimination under the law terms.
	Information shared with third parties	Users declare that they authorise BAICV to transmit to third parties acting on its behalf their personal information, which is essential for the activation, support, management and maintenance of the MAKEBA service and the development of any activities related to it.
	Duration of third-party access	a) For a minimum of 7 (seven) years from the last transaction or the end of the contractual relationship. b) While there are obligations arising from the contractual relationship. c) While BAICV's rights may be invoked.
	Tracking technologies/ website cookies	The website does not ask for cookie authentication.
	Storage of user information by the App	Financial information Contact information

Makeba is an app with sophisticated communication for its customers. Its website presents a clear tutorial on how customers can join the service, with a detailed step-by-step explanation, from download to use. Although there is a contact section, it does not work since it is unknown whether the platform managers received the message because there is no notification. In one part, the App states that Makeba is intended for use by people and businesses who trust each other. The central requirement to use the application is to verify identification, at least adding the identity card on the platform, clearly showing the transmission of personal data.[49]

49 https://www.makeba.money/cv-por/limits.html > accessed on 29 July 2021.

The FAQ section[50] appears without any highlight, and it states that the user cannot cancel transactions once they have been approved. It notes that it uses the latest encryption technology to protect customers' accounts and ensure that their data is private. If users suspect their account is compromised, they must contact the application managers.

In addition, it is not clear how encrypted technology is applied to protect customers' data, as by accessing the application, you cannot see the information collected. The App states that deposits made on Makeba are kept secure by banking partner Banco BAI Cabo Verde regarding personal data. The App also indicated that customers need to use their NIB to access the Makeba account to transfer their bank money. It is unclear how this NIB is kept and to what extent Banco BAI-CV can manage or access the customer's data, especially as it concerns sensitive information about customers' bank accounts.

One case that gained visibility in the media was related to a fine that the Data Protection Agency (CNPD) imposed on the Central Bank of Cape Verde and a commercial bank called Novo Banco Cabo Verde.[51] This fine was because of disclosure in the press of a list of 50 debtors of the commercial Bank. The penalties were related to the fact that the banks did not take appropriate measures to protect personal data. Both the Central Bank and the commercial Bank have appealed to the court.

When the list was made public, both the Bank of Cape Verde and the Ministry of Finance distanced themselves. The object of the CNPD's investigation was not to find out how the list was made public but whether there were breaches of customer data protection by the Bank.[52] We note that this part shows the weaknesses of using applications like Makeba to protect their customers' data. However, it also indicates some action by the data protection agency.

Considering that Cape Verde is a data protection law pioneer in Africa, we note a clear focus by the Data Protection Agency on monitoring how the finance sector uses its users' data. However, we could not verify how regulators can apply such actions to money lending mobile applications like Makeba. There are no prominent examples of CNPD activities to protect users' data of these applications, which represents a gap. On the other hand, we do not see much action from the Bank of Cape Verde, which in principle should be the lead institution on how these applications are used, especially since there are not so many initiatives other than Makeba.

50 https://www.makeba.money/cv-por/faq.html > accessed on 30 July 2021.
51 It is known that the fine was around $30,000 https://www.voaportugues.com/a/banco-de-cabo-verde-e-novo-banco-multados-violar-lei-proteccao-de-dados/3898368.html > accessed on 29 July 2021.
52 https://www.dn.pt/lusa/banco-central-e-novo-banco-de-cabo-verde-multados-por-falha-na-protecao-de-dados-8563648.html > accessed on 28 July 2021.

Côte d'Ivoire

Country profile

The Republic of Côte d'Ivoire is a French-speaking country in West Africa with over 26 million inhabitants in 2020.[53] This country shares borders with Mali, Burkina Faso, Ghana, Liberia and Guinea, representing 40% of the Economic Union of West African States' (UEMOA) economy. The country GDP estimate is 58.54 billion USD, and it operates as a presidential system of government.

53 Source Ivory Coast Country Sheet produced by the Atlas of the Countries and Populations of the World and available at the following link: https://www.populationdata.net/pays/cote-divoire/

Data Protection in Côte d'Ivoire

Personal data protection in Côte d'Ivoire is covered by Law no 2003-450.[54] This Law applies to any automatic processing or not carried out in the country of Côte d'Ivoire[55]. It is unclear if the rule applies to the data of Ivorians residing outside the country. L'Autorité de Régulation des Télécommunications de Côte d'Ivoire (ARTCI) is the national DPA in Côte d'Ivoire. The ordinance no 2012-293 of June 25, 2013, created the organization but entrusted with regulating personal data processing by Law no 2003-450 of June 16, 2013.[56] It is responsible for ensuring compliance with the legal provisions concerning personal data processing and ensuring that the various processing operations do not interfere with freedoms and privacy[57].

Introduction

With a market share penetration rate of 70.9%, Mobile Money[58] is booming in Côte d'Ivoire. It is carried by the leading mobile telephone operators[59], who share 20,789,662 subscribers.

54 Law n ° 2003-450 of June 16, 2013 on the protection of personal data in Côte d'Ivoire. < https://www.artci.ci/images/stories/pdf/lois/loi_2013_450.pdf> accessed 7 May 2021.
55 Article 3 of Law n ° 2003-450 of June 16, 2013
56 Relevant provision?
57 Article 47 of Law n ° 2003-450.
58 Mobile money is electronic money created by telecom operators and stored in an electronic wallet backed by the telephone plan. This technology allows people to send or receive digitized money through their phone. You just need to know the recipient's phone number to send them money. Thus, the mobile number has become, in a way, a bank account number without having a bank account. However, the costs of mobile money are still much lower than those of a bank account. Hence its popularity and the strong support of the populations for Mobile Money.
59 Orange, MTN and Moov are the 3 mobile telephone operators in Côte d'Ivoire.

Aware of the potential of this market, two (2) of these operators, namely Orange and MTN, have embarked on digital credit, an offer of financial services that allows the Ivorian population to access rapid and short-term loans through mobile applications. This fast access offers and promotes financial inclusion of poorly banked people, helps them fix their current expenses, and presents an opportunity for the population to be a potential source of financial market development in Côte d'Ivoire. Indeed, the first digital credit offer launched on February 16, 2018, by MTN and Bridge Microfinance Côte d'Ivoire attracted 1,900,000 customers in one year.

In July 2020, Orange launched a similar offer. Between July 2020 and May 31, its microcredit service made 44 billion FCFA in loans available to Ivorian customers, including 1.2 million loan requests processed for amounts between 5,000 FCFA and 250,000 FCFA. Or's portfolio stood at 600,000 customers at the end of May 2021, and savings deposits received an interest rate of 3.5%, which came out to 1.5 billion FCFA. For loan recovery and monitoring of savings plans, these operators collect personal data from their customers through mobile applications[60] that serve as a user interface. This practice can infringe on user privacy and should be questioned impartially. This mobile App based loan services ran after adopting the Law on protecting personal data in Côte d'Ivoire[61]. Hence, it is crucial to know whether the data processing practices of these applications, as defined in their policies and conditions of use, consider the regulations on privacy protection.

This study aims to analyze the privacy policies and the terms and conditions of these applications and examine their compliance with the data protection law in Côte d'Ivoire. The first part includes an overview of the data collected by these applications. The second part examines their processing activities under the Law on personal data protection. The last part ends by indicating whether or not these applications comply with the Law on personal data protection.

60 MTN Mobile Money's microloan and micro-savings service called MOMO KASH is based on both a USSD code associated with the phone number and the MyMTN CI mobile application. Both are associated with the customer's MTN Mobile Money account. On the side of Orange Côte d'Ivoire, the micro-loan and micro-savings service called Tik-Tak is also associated with a USSD code and a mobile application: Orange Bank Africa. Both are associated with the customer's Orange Money account.

61 LAct No. 2013-50 of 19 June 2013 on the protection of personal data in Ivory Coast

Overview of the Data Collected by the Digital Loan Applications for the Study

Orange Money Africa[62] Download link : Google Play Store and Apple Store	Information collected and processed by the application	
	Authorizations sought	At startup, Orange Money Africa asks to: · Manage user calls · access a user's SMS: It displays a user's SMS to collect financial information and transaction data to collect information about a user's financial history and determine their creditworthiness · Access user contacts user · Access location, device and usage data: Orange Money App uses GPS technology or other location services to determine the current location of a user
	Information collected from the user	During registration, Orange Money Africa collects the user's information: name, address, email address and phone number, device phone number, SIM card, age, username, password, financial and credit data, descript personal ion and photograph, and other registration

62 Privacy policy for personal data on Orange Money and the General Conditions of Use (T & Cs) of the Orange Bank Savings and Loan services

	information collected from the user's device Information collected while using the Orange Côte d'Ivoire website	Orange Money Africa collects the following information from the user's device: Mobile device model, device IMEI number or serial number, SIM card information, mobile network information, operating system device, browser type, device location and time zone setting Information stored in the device: contact list, call logs, SMS logs, contacts from social media accounts, photos, videos or any relevant digital content Once a user uses the Orange Côte d'Ivoire website on their mobile phone, Orange et Moi[63] collects the following information automatically and stores it in their files Logs: User IP address, browser type, Internet Service Provider (ISP), referring / exit pages, operating system, timestamp and browse media. This information is then combined for analysis or marketing purposes and made available to Orange Bank.
	Information received from third parties	Information was obtained from other entities of the Orange Group: Orange Money Côte d'Ivoire and Orange Côte d'Ivoire, Credit Assessment Offices (BIC), Mobile network providers and collection agencies.
	Use of user information by the App	Orange Money Africa's privacy policy states that it collects user data for the following purposes: · processing a user's transactions · Identity verification of a user · Loan disbursements and collection of payments scoring credit and creation of credit models · analysis of borrower behaviour · Orange Money App's obligations towards users · compliance with · compliance with laws, regulations and rules relating to "know your customer" and anti-money laundering rules · Fraud prevention, · Marketing services

63 Orange et moi is an application from Orange Côte d'Ivoire which serves as a user interface for its customers with android phones.

	Shared information with third parties Duration of data access to third parties	Orange Money shares user information with: · Its members, agents, service providers, the Orange Money Group entities, and the entities that subcontract the data collected. · Anyone acting on behalf of a user of financial institutions, credit bureaus and agencies (BIC) · Business partners in the event of business transfers, divestitures, mergers & acquisitions, etc · Third-party service providers · Law enforcement agencies (the National Telecommunications / ICT Regulatory Authority of Côte d'Ivoire (ARTCI)4), government officials, based on: Formal request or decision Justice Compliance with Law or Reporting Suspected Illegal Activity The policy is silent on how long third parties can access users' personal information and keep it.
	Tracking Technologies / Website Cookies	Orange Money Africa uses mobile tracking technology and website cookies to distinguish App users.
	Storage of User Information by theApp	Orange Money Africa stores users data outside Ivory Coast. Information is also processed by Orange Money Côte d'Ivoire staff, Orange Bank Africa, and its CECOM in Madagascar operating outside Côte d'Ivoire. The App did not provide details on the retention period of data by Orange Côte d'Ivoire.

MyMTN CI[64] Download link : Google Play Store and Apple Store	Information collected and processed by the application	
	Authorizations sought	At startup, MyMTN CI asks to: Manage user calls access a user's SMS: It displays a user's SMS to collect financial and transactional information data to collect information about a user's financial history and determine their creditworthiness Access user contacts user Access location, device and usage data: MyMTN CI uses GPS technology or other location services to determine the current location of a user

64 MyMTN CI Apps privacy policy T & Cs and the General Conditions of Use () for MTN Mobile Money Ivory Coast accounts

	Information collected from the user	During registration, MyMTN CI collects a user's information: the identity of the customer (name, first name, gender, date of birth), these contact details (postal address, email address, telephone numbers), its location (geographical situation) and the interrelation e between these chosen payment methods (check, cash, bank card, mobile money)
	Information collected from the user's device Information collected when using the MTN Côte d'Ivoire website	MyMTN CI collects the information from a user's device: Artificial Intelligence (AI) technique: mobile device model, device IMEI number or serial number, SIM card information, mobile network information, device operating system, browser type, device location and time zone setting Information stored in the device: contact list, call logs, SMS logs, contacts from social media accounts, photos, videos or any relevant digital content Once a user uses the MTN Côte d'Ivoire website, MyMTN CI automatically collects the following information and stores it in its log files: User's IP address r, browser type, internet service provider (ISP), referring / exit pages, operating system, timestamp and browse media. This information is combined for analysis or marketing purposes.
	Information received from third parties	Information obtained from other entities of the MTN Group: MTN Côte d'Ivoire and MTN Mobile Financial Services Côte d'Ivoire, Credit Assessment Offices (BIC), Mobile network providers and collection agencies.
	Use of user information by the App	The privacy policy of MyMTN CI states that it collects user data for the following purposes: · processing a user's transactions · Verifying the identity of the user 'one user · Loan disbursements and payment collection scoring · credit and creation of credit models · analysis of borrower behaviour . Orange Money App's obligations towards users · compliance with · compliance with laws, regulations and rules relating to "know your customer" and anti-money laundering rules · Fraud prevention, · Marketing services

	Shared information with third parties	MyMTN CI shares user information with: Its members, agents, service providers, MTN Group entities and entities that subcontract the data collected. Anyone acting on behalf of a user financial institutions, credit bureaus and agencies (BIC) Business partners in the event of business transfers, divestitures, mergers & acquisitions, etc. Third-party service providers Law enforcement agencies (the National Telecommunications / ICT Regulatory Authority of Côte d'Ivoire (ARTCI)4), government officials, based on: Formal request or decision Justice Compliance with Law or Reporting Suspected Illegal Activity
	Duration of data access to third parties	The policy is silent on how long third parties can access users' personal information and keep it.
	Tracking Technologies / Website Cookies	MyMTN CI uses mobile tracking technology and website cookies to distinguish App users.
	Storing User Information by the App	MTN CI stores user information at a destination outside the Ivory Coast. Information may also be processed by MTN Côte d'Ivoire staff outside of Côte d'Ivoire. The privacy policy of MyMTN CI indicates that the maximum retention period for the data collected is ten years from the end of the contractual relationship and may be extended in the event of legal or administrative proceedings.

Case Study: Orange Money Africa: The question of the duration of storage of user data

The confidentiality policy, the general conditions of use (T & Cs) for Orange Money Côte d'Ivoire accounts and the public compliance policy of Orange Côte d 'Ivoire, associated with the Orange Money Africa Apps do not give any details on the duration of user data storage. An insufficiency that constitutes a law violation relating to data protection in Côte d'Ivoire requires that data be collected for a fixed period[65] .

Analysis of Data Protection Practices of Digital Loan Applications Concerning the Law Relating to the Protection of Personal Data

The Law on the personal data protection in Côte d'Ivoire has clearly defined obligations in privacy laws, applicable to any processing, whether automatic or not[66]. In doing so, the digital applications of subject loans. However, due to their recent development, their risks to protecting privacy are current. This section highlights the relevant provisions of the Law to establish whether these Applications comply with these provisions.

65 Article 16 and 43 of Law No. 2013-50 of June 19, 2013
66 Article 3 of Law No. 2013-50 of June 19, 2013

Right to Privacy

Data protection law requires that data controllers and processors (in this case, digital lending applications) handle personal data in a way that respects the right to privacy.[67] In this case, the Law calls on applications to ensure that the borrowers' right to privacy comes first when processing their data. The applications studied violate this right and process data that is intrusive and unrelated to the purpose of data collection. For example, these applications collect information such as contacts stored on a borrower's device, login information from social media platforms, and accurate real-time location, which is intrusive and excessive concerning data collection.

Legality, fairness and transparency

Data protection law requires that these applications process data lawful, fair, and transparently.[68] All applications must inform their data subjects clearly and concisely on how their data will be processed and that all the parameters of the Law are respected in such processing.[69]

In this case, applications should inform users about why their data is collected, how the company will use their data and, if shared with third parties, with whom the company will share their data and how long they will keep the data. It can be said that the applications studied are transparent as to why they collect user data and with whom they share it. However, they do not indicate how long third parties will access the data and how long they will keep it.

Limitation of Purpose, Relevance and Adequacy

Digital lending applications are required under data protection law to process personal data following data collection.[70] This means that the Apps should only collect data concerning digital lending and not excessive data. Applications should only collect relevant, adequate and limited to data collection.[71]

The applications investigated collect personal information that is not relevant to the purpose of the data collection. They collect borrowers' information such as credit card numbers, financial transactions, social media login account information, social media contacts, phone contacts, photos and videos, etc., irrelevant in digital lending.

Sharing Information with Third Parties

Data protection law states that these applications must notify users of third parties with whom their data will be shared, including details adopted to protect their data before collection.[72] In the specific case of the Orange Money Africa Apps, the lack of a fixed

67 Article 3 of Law No. 2013-50 of June 19, 2013

68 Article 14, 15 and 16 of Law No. 2013-50 of June 19, 2013
69 Article 28 of Law No. 2013-50 of June 19, 2013
70 Article 14 of Law No. 2013-50 of June 19, 2013
71 Article 16 and 43 of Law No. 2013-50 of June 19, 2013
72 Article 16 and 43 of Law No. 2013-50 of June 19, 2013

duration for data processing constitutes a violation of privacy rights[73].
The applications reviewed share user/borrower information with the credit information office (CIO), business partners, professional advisers, government and law enforcement agencies, etc., and do not indicate the safeguards adopted to protect borrower data. The Applications also do not show how long these parties will have access to the data and how long they will retain it.

Transfer of personal data outside Côte d'Ivoire

Provision respected by the various application providers

Confidentiality by design and by default

The Law provides that the data controller must make all arrangements for processing user data[74].
The applications have encryption measures to protect their users' communications and private content—a level of security necessary to protect user data. However, the level of protection included cannot prevent the App provider from collecting excessive information.

Right to access and delete personal data

Users of the applications have the right to access their data held by these applications[75] and have the right to request the deletion or destruction of their data that the applications are no longer authorized to retain. Users also have the right to request deletion of irrelevant, excessive or data obtained illegally[76]. Application providers have set up dedicated services to receive user requests on this subject.

Data portability

The Law gives data subjects the right to receive their data in a structured and machine-readable format.[77] It also gives them the right, where technically possible, to have the data transmitted directly to other data controllers or processors.[78] The applications under review do not provide a means for users to exercise this right.

Data Protection Impact Assessment (DPIA)

The Law requires that a report on the data processing process be produced annually and sent to the ARTCI. In addition, data transfer authorizations have indicated the need for data controllers to perform a Data Protection Impact Assessment (DPIA). However, neither of the data controllers of the two applications have produced or made available their reports.
The data processing practices of digital credit applications in Côte d'Ivoire do not respect the Law of privacy protection principles. Data protection impact assessments (DPIA) must be conducted by those responsible for processing these digital applications to force strict

73 Article 49 of Law No. 2013-50 of June 19, 2013
74 Article 39, 40, 41 and 44 of Law No. 2013-50 of June 19, 2013
75 Article 49 of Law No. 2013-50 of June 19, 2013
76 Article 30, 31, 3 , 33, 34, 35 and 36 of Law No. 2013-50 of June 19, 2013
77 Article 49 of Law No. 2013-50 of June 19, 2013
78 Article 30, 31, 3, 33, 34, 35 and 36 of Law No. 2013-50 of June 19, 2013

compliance with legal obligations in this area. In addition, a revision of Law no. 2013-50 of June 19, 2013, relating to personal data protection must be considered, taking into account the potential risks for privacy. Beyond that, it is also necessary for ARTCI to acquire expertise and technical equipment to monitor in real-time the volume, quality and quantity of data collected by those data managers for processing mobile applications.

Egypt

Country Profile

Located in North-East Africa, Egypt, or the Arab Republic of Egypt, recorded over 106 million inhabitants in 2021. It is located on the southern coast of the Eastern Mediterranean, bordered by Israel, Libya, Sudan and is part of the group of countries of the Middle East and North Africa (MENA). It is Africa's second-largest GDP and was around $ 362 billion in 2019/20. It practices a semi-presidential regime.

Data Protection in Egypt

Privacy protection is governed by Law No. 151 of July 15, 2020, on personal data protection. The Law applies to any processing, whether automatic or not, carried out on the territory or outside of Egypt[79]. The Data Protection Center ('DPC') is an Egyptian DPA. It was created by Law No. 151 of July 15, 2020, and started its activities in April 2021. It is empowered to oversee and enforce the Data Protection Law, including, among other things, issuing required licenses and authorization and certification under the Data Protection Law[80].

Introduction

In 2020, the African continent had 562 million Mobile Money accounts, representing 45% of Mobile Money accounts opened worldwide, i.e. 1.2 billion. Most of these accounts are divided between East Africa (293 million) and West Africa (198 million), and they are used at least for payment transactions of various kinds. We also note a more significant increase in the number of accounts in absolute value over the last five years in North Africa due to new and renewed efforts in this region's sector. Indeed, in North Africa, 14 million mobile money accounts were registered in 2020 for 248 million transactions, equivalent to more than 3 billion US dollars ($), up 24% compared to 2019. One of the leading countries in this ongoing dynamic is Egypt, where four mobile money services have been offered to populations since April 2013. These services concern (i) mobile payments (bill payment, group payments, and merchant payments), transfers (national and international transfers), salary disbursements

79 Article 1 and 2 of Law No. 151 of July 15, 2020
80 Article 19 of Law No. 151 of July 15, 2020

(Paying salaries from a structure to its staff) and banking services (deposit, withdrawal of money, savings account, digital credit, etc.). Thanks to its services, Egypt had about 4.5 million electronic transactions per month, carried out by 13.5 million mobile e-wallets (electronic wallets) active in its territory, according to the latest statistics from the National Authority of Telecommunications Regulation (NTRA), published in June 2020. The leading mobile telephone operators are also e-wallet service providers, fintech. Vodafone Egypt thus remains the leader in this segment, representing 62.7% of total electronic wallets and 86.5% of e-wallet transactions, followed by Orange Egypt (25% of e-wallets and 8.5% of transactions), Etisalat Misr (12% of e-wallets and 4.5% of transactions) and We (0.3% and 0.5%). The services most used by users are money deposits and withdrawals (35% of total transactions by e-wallet), money transfers (33%) and recharging of prepaid mobiles (26%).

Regarding digital credit, it was first introduced in Egypt by the Start-up Kayshat[81] in February 2020 with the agreement of the Financial Regulatory Authority of Egypt. This application allows people to obtain loans between 100 and 1,500 Egyptian pounds (EGP). A boom for a country where nearly 70% of the population is unbanked and, above all, a market for players in the banking and financial sector. Indeed, aware of the potential benefit of this type of service, several offers (Shahry[82], MNT Halan[83] and MoneyFellows[84]) will develop. The multiplication of these offers beyond their beneficial effects for financial inclusion and the improvement of the living conditions of the populations pose challenges in terms of personal data protection in Egypt. Hence, whether the data processing practices of these applications, as defined in their policies and conditions of use, consider the regulations on the protection of privacy?

This study aims to analyze the privacy policies and the terms and conditions of these applications and to examine their compliance with the data protection law in Côte d'Ivoire. The first part includes an overview of the data collected by these applications, and the second part examines their processing activities under the Law on the protection of personal data. The last part ends by indicating whether or not these applications comply with the law protecting personal data.

81 Kashat is the first Nano lending mobile application in Egypt, offering short term loans that start from 100 EGP up to 1500 EGP with a repayment plan up to 61 days.
82 Shahry allowed Egyptians to obtain instant and consumer credits to purchase goods and services in the country.
83 Halan is a multi-service application that enables Egyptians beyond goods delivery and purchase services to obtain instant loans. A digital credit offer that results from a collaboration between the Dutch company MNT Investments BV and the micro-venture capital firm Tasaheel. In particular, it allows traders to obtain funds starting at 3,000 EGP and going up to 200,000 EGP with just a few clicks. It was launched on June 24, 2021.
84 MoneyFellows offers a wide range of money circle options that every user can choose from. Depending on the payment behavior the user can obtain instant credits. Fees start from 8% and gradually decrease depending on your selected niche, until it reaches zero. The selection of the loan niches and the amount granted to the users is done through the user credit evaluation carried out by the MoneyFellows teams.

Overview of Data Collected by Digital Study Loan Application

Kashat[85] Download link: Google Play Store and HUAWEI AppGallery	Information collected and processed by the application	
	Permissions sought	On startup, Kashat App asks to: Manage calls and access users' contacts, find accounts on the device, read your contacts, read call logs, directly call phone numbers and read phone status and identity. · access a user's SMS: It displays a user's SMS and or MMS to collect given financial and transactional information to collect information on a user's financial history and determine their creditworthiness . Access data stored in user's mobile, modify, read or delete the contents of your USB storage access location, device and user usage data: Kashat App uses GPS technology and other location services to determine the current location. . View Wi-Fi connections . Access the schedule for reading calendar events plus confidential information, add or modify calendar events, and send emails to guests without owners' knowledge. . Perform various actions: bind to an accessibility service, receive data from the internet, draw over other apps, read Google service configuration, view network connections, run at startup, full network access and prevent the device from sleeping
	Information collected from the user	When subscribing to the loan service, Kashat App collects user information: name, address, telephone, email address, national identity card, photo of you, username and password., and other registration information: professional status and field, marital status, financial and credit information.

85 Privacy Policy of Kashat App

	Information Collected From User's Device	Kashat App collects the following information from a user's device: device information including mobile type, unique device identifiers (IMEI or serial number), operating system device and device location and time zone mobile network information data stored on your devices such as contact list, call logs, SMS logs and media gallery
	Information CollectedUs-ingWebsite	Current location information provided by GPS technology and other location services Once a user uses the website Kashat Appon their mobile phone, they automatically collect the following information and store it in their log files. Log Data may include information such as the Internet Protocol ("IP") address of the mobile user, Internet Service Provider (ISP), device name, operating system version, browser type, clickstream data, and the time and date of your use of the service. That is to say, statistical data on users' actions and browsing habits, and not allowing them to be formally identified. When used with other information collected, this information provides better analysis and security for users.
	Information received from third parties	Information obtained from other Kashat group entities (subsidiaries), Credit Assessment Bureaus (BIC), Mobile network providers, collection agencies, business partners, etc
	Use of User Information by the App	privacy policy Kashat's states that it collects user data for the following purposes: Verifying the identity of a user Processing of user transactions Credit scoring and creation of credit models Analysis of borrower behaviour Loan disbursements and payment collection obligations Kashat's towards users Compliance with applicable regulations regarding KYC "Know Your Customer", AML "Anti-money laundering", and CFT (Combating the Finance of Terrorism) requirements Promotional communications and marketing services

	Information shared with third parties	Kashat shares user information with: Its subsidiaries, its parent and other subsidiaries of our parent company ("its group") Anyone acting on behalf of a user From mobile wallet providers, insurance companies, credit bureaus or other financial institutions Law enforcement authorities International government agencies to assist in detection, prevention and investigation of criminal activity or fraud. . Business partners in business transfers, disposals, mergers & acquisitions, etc. Third-Party Service Providers
	Duration of data access to third parties	The policy is silent on how long third parties can access users' personal information and keep it.
	Tracking Technologies / Website Cookies	The Lending Service Kashat does not explicitly use these "cookies". However, to provide a better user experience, Kashat uses third-party service providers such as analytics providers or marketing agencies who may choose to use cookies or other mobile tracking technology to distinguish you from other App or website users.
	Storage of User Information by the App	Kashat's data is stored on servers in Egypt, but it may be transferred and stored to a destination outside of Egypt. They can also be processed by staff outside Egypt who work for Kashat or its suppliers. These staff members may be engaged in the fulfilment of user requests. You agree to this transfer, storage, or data processing by submitting your data. Kashat states that it takes all reasonable steps necessary to ensure user data is treated securely and under its privacy policy.

Shahry[86] Download link: Google Play Store and Apple Store	Information collected and processed by the application

86 Privacy Policy of Shahry

	Permissions	Sought On startup, Shahry asks: · Manage calls and access users' contacts, find accounts on the device, read your contacts, call phone numbers and read phone status and identity. Access User Location, Device and Usage Data: Kashat App uses GPS technology from other location services to determine a user's current location. . View Wi-Fi connections . Access the data stored in the user's mobile, modify, read or delete the contents of your USB storage . Perform various actions: receive data from the internet, view network connections, pair with Bluetooth devices, full network access, prevent devices from sleeping and modify system settings.
	Information Collected from the User	When subscribing to the loan service, Shahry collects the user's information: name, date of birth, national identification number, address, occupation, past and present personal educational and financial data.
	Information Collected From User's Device Information Collected UsingWebsite	WhileShahry'sShahry collects the following information from a user's device: device information, including type device, unique device identifiers (IMEI or serial number), device operating system and device location and time zone including IP address. mobile network information stored on your devices such as contact list, call logs, SMS logs and media gallery Current location information provided by GPS technology and other location services Once a user uses Shahry's website on their mobile phone, Shahry App automatically collects the following information and stores it in its log files. Log Data may include information such as the mobile user's Internet Protocol ("IP") address.
	Information received from third parties	Information obtained from other entities of the Shahry Group (subsidiaries), Credit Assessment Bureaus (BIC), Mobile network providers, collection agencies, business partners, etc

	Use of User Information by the App	Shahry's privacy policy states that it collects user data for the following purposes: Verifying the identity of a user Processing a user's transactions credit and creating credit models loan scoring·disbursements and payment collection Shahry's obligations to users Compliance with applicable regulations regarding KYC "Know Your Customer", AML "Anti-money laundering", and CFT (Combating the Finance of Terrorism) requirements Promotional communications and marketing services
	Information shared with third parties Duration of data access to third parties	Shahry shares user information with: Its subsidiaries, parent and other subsidiaries of our parent company ("its group") Anyone acting on behalf of a user From mobile wallet providers, insurance companies, credit bureaus or other financial institutions Law enforcement authorities International or government agencies to assist in detection, prevention and investigation of criminal activity or fraud. . Business partners in business transfers, disposals, mergers & acquisitions, etc. Third-Party Service Providers The policy is silent on how long third parties can access users' personal information and keep it.
	Tracking Technologies / Website Cookies	privacy policy is Shahry Silent on using these "cookies". The website associated with the application does not offer any possibility of choosing cookie preferences.
	Storage of User Information by the App	Personal identification data of users of Shahry are recorded, encrypted and stored on its servers in Egypt and are not accessible to unauthorized entities or persons. This information is not disclosed for rental or other commercials (advertising) purposes.

Halan[87] Download link: Google Play Store and HUAWEI AppGallery	Information collected and processed by the application

87 Politique de confidentialité de Halan

	Permissions sought	On startup, Halan asks to: Handle calls and access directly call phone numbers Access data stored in the user's mobile, modify, read or delete the contents of your USB storage access location, device and user usage data: Kashat App uses GPS technology and other location services to determine the current site. View Wi-Fi connections Perform various actions: receive data from the internet, full network access, prevent the device from sleeping, read Google service configuration, view network connections
	Information collected from the user	When subscribing to the loan service, Halan collects user information: name, email address, mobile phone number, postal address, profile picture, payment method, financial news and credit card.
	Information Collected From User's Device Information CollectedUsingWebsite WhileHalan's	Halan collects the following information from a user's device: device information, including type device, unique device identifiers (IMEI or serial number), device operating system and device location and time zone mobile network information stored on your device such as contact list, call logs, SMS logs, multimedia gallery, SMS data and transaction data, current location information provided by GPS technology and other location services Once a user visits the Halan website, Halan App automatically collects the following information and stores it in its log files. Log Data may include information such as the Internet Protocol ("IP") address of the mobile user, Internet Service Provider (ISP), device name, operating system version, browser type, clickstream data, and the time and date of your use of the service. That is to say, statistical data on users' actions and browsing habits, and not allowing them to be formally identified. When used with other information collected, this information provides better analysis and security for users.
	Information received from third parties	Information obtained from other Halan Group entities (subsidiaries), Credit Assessment Bureaus (BIC), Mobile network providers, collection agencies, business partners, etc

	Use of User Information by the App	Halan's privacy policy states that it collects user data for the following purposes: Verifying the identity of a user Processing of user transactions Credit scoring and creation of credit models Analysis of borrower behaviour Loan disbursements and payment collection Halan's obligations towards users Compliance with applicable regulations regarding KYC "Know Your Customer", AML "Anti-money laundering", and CFT (Combating the Finance of Terrorism) requirements Promotional communications and marketing services
	Information shared with third parties Duration of data access to third parties	Halan shares user information with: Its subsidiaries, parent and other subsidiaries of our parent company ("its group") Anyone acting on behalf of a user From mobile wallet providers, insurance companies, credit bureaus or other financial institutions Law enforcement authorities International or government agencies to assist in detection, prevention and investigation of criminal activity or fraud. . Business partners in business transfers, disposals, mergers & acquisitions, etc. Third-Party Service Providers The policy is silent on how long third parties can access users' personal information and keep it.
	Tracking Technologies/ website cookies	website Halan's uses cookies to distinguish itself from others. They make it possible to offer an excellent experience to the user when he browses his site and also makes it possible to improve and develop the services offered. These cookies can be accepted or refused by users.
	Storage of User Information by the App	Halan's data is stored on servers in Egypt, but it may be transferred and stored to a destination outside of Egypt. They can also be processed by staff outside Egypt who works for Kashat. or one of its suppliers. These staff members may be engaged in the fulfilment of user requests. You agree to this transfer, storage, or data processing by submitting your data. Kashat states that it takes all reasonable steps necessary to ensure user data is treated securely and under its privacy policy.

MoneyFellows Trusted and Convenient Money Circles[88] Download link: Google Play Store and Apple Store	Information collected and processed by the App	
	Permissions sought	On startup, MoneyFellowsHandle asks to: calls and access users' contacts, find accounts on the device, read your contacts, directly call phone numbers and read phone status and identity. Access a user's SMS: It displays a user's SMS and or MMS to collect given financial and transactional information to collect information on a user's financial history and determine their creditworthiness Access data stored in the user's mobile, modify, read or delete the contents of your USB storage Access user's location, device and usage data: MoneyFellows App uses GPS technology and other location services to determine the current location. Perform various other actions: receive data from the internet, pair with Bluetooth devices, run at startup, view network connections, full network access, vibration control, use accounts on the device, prevent the device from sleeping.
	Information Collected from the User	When subscribing to the loan service, MoneyFellows App collects the user's information: name, address, telephone, email address, national identity card, photo of you, name of user and password., and other registration information: professional status and field, marital status, financial and credit information.

88 Privacy Policy of MoneyFellows

	Information Collected From User's Device	Kashat App collects the following information from a user's device: Identity Data includes [first name, maiden name, last name, username or similar identifier, marital status, title, date of birth and gender]. Contact Data includes billing address, delivery address, email address and telephone numbers. Financial Data includes [bank account and payment card details. Transaction data includes details about payments to and from you and other information about the products and services you have purchased from us.
	Information Collected While UsingWebsite Money Fellows	Technical data includes Internet Protocol (IP) address, connection data, browser type and version, time zone setting and location, browser plug-in types and versions, system operating and platform and other technologies on the devices used to access this website. Profile Data includes your username and password and your website activities, interests, preferences, comments, and survey responses. Usage Data includes information about how you use our website, products and services. Marketing and Communications Data includes your preferences for receiving marketing from our third parties and us and your communications preferences. When users use the website of MoneyFellows, etc., the technical data of the user's terminal navigation data are automatically collected. This data is collected using cookies and other similar technologies. Further technical data about users is also collected when the user visits other websites that use cookies.
	Information received from third parties	The Personal data are also received from various third [and public sources] as shown below.Technical data of the following parties: analysis suppliers, advertising networks, and researching information providers. Contact, financial and transaction data of technical, payment and delivery service providers

	Use of user information by the App	privacy MoneyFellowspolicy indicates that it collects user data for the following purposes: Verifying the identity of a user Processing of user transactions Credit scoring and creation of credit models Analysis of borrower behaviour Loan disbursements and payment collection Obligations of MoneyFellows towards users Compliance with applicable regulations regarding KYC "Know Your Customer", AML "Anti-money laundering", and CFT (Combating the Finance of Terrorism) requirements Promotional communications and marketing services
	Information shared with third parties Duration of data access to third parties	MoneyFellows shares user information with: Its subsidiaries, parent and other subsidiaries of our parent company ("its group") Anyone acting on behalf of a user Mobile wallet providers, insurance, credit bureaus or other financial institutions Law enforcement authorities, International or government agencies assist in detecting, preventing, and investigating criminal activity or fraud. Business Partners and Third-Party Service Providers The policy is silent on how long third parties can access users' personal information and keep it.
	Tracking Technologies / Website Cookies	The Lending Money Fellows Service uses"cookies" to better user experience. Kashat uses third-party service providers such as analytics providers or marketing agencies who may choose to use cookies or other mobile tracking technology to distinguish you from other App or website users.
	Storage of user information by the App	Personal data of Money Fellows are stored on servers in Egypt, but they can be transferred and stored to a destination outside of Egypt. It may also be processed by staff outside Egypt who works for MoneyFellows or one of its suppliers. These staff members may be engaged in the fulfilment of user requests. You agree to this transfer, storage, or data processing by submitting your data. MoneyFellows indicates taking all reasonable steps necessary to ensure user data is treated securely and under its privacy policy. The primary user information (including contact details, identity, financial and trading) are retained for five (5) years after they have ceased to be clients for tax purposes.

Case Study: The Halan App and the question of data processing of multiservice applications.

With its slogan "One App For All Your Needs", Halan App brings together five services: E-Commerce & BNPL, Bill Micro Finance, Payments, Delivery & Groceries and Wallet & Card. In addition to their sub-components, services assume a large mass of data collected

from users globally without necessarily considering the service researched by the user. In doing so, Halan's privacy policy does not differentiate between the data collected by a user seeking a loan and another who is waiting for groceries to be delivered. A situation that requires for theData Protection Center ('DPC') in Egypt to have a real-time tool for monitoring the processing of data collected by Halan Apps.

Analysis of Data Protection Practices of Digital Lending Applications Against Personal Data Protection Law

Egypt's Personal Data Protection Law has clearly defined legal obligations in privacy protection matters applicable to any processing, whether automatic or not[89]. In doing so, digital loan applications are subject to it. However, analysis of the latter's data processing system shows that the provisions concerning privacy protection are not strictly observed. This section highlights the relevant provisions of the Law to establish whether these Applications comply with these provisions.

Right to Privacy

Data protection law requires that data controllers and processors (in this case, digital lending applications) handle personal data in a way that respects the right to privacy of the person concerned.[90] In this case, the Law calls on applications to ensure that the borrowers' right to privacy comes first when processing their data. The applications studied violate this right and process data that is intrusive and unrelated to the purpose of data collection. For example, these applications collect information such as contacts stored on a borrower's device, login information from social media platforms, and accurate real-time location, which is intrusive and excessive about data collection.

Legality, fairness and transparency

Data protection law requires these apps to process data legitimately and lawfully.[91] The applications must ensure that data subjects are informed clearly and concisely of how their data is processed and that all the parameters of the Law are respected in such processing.[92]

In this case, applications should inform users why their data is collected, how their data will be used and, if shared with third parties, with whom the data will be shared and how long they will keep the data. The applications studied can be transparent as to why they collect user data and with whom they share it. However, they do not indicate how long third parties have access to the data and how long they will keep it[93].

Limitation of purpose, relevance and adequacy

Digital loan applications are required under data protection law to process personal data

89 Article 1 and 2 chapter I of Law n ° 151 of July 15, 2020
90 Article 1 chapitre I of Law n ° 151 of July 15, 2020

91 Article 6 of Chapter II of Law No. 151 of July 15, 2020
92 Article 2 and 3 of Chapter II of Law No. 151 of July 15, 2020
93 Article 5 of Chapitre II Chapter II of Law No. 151 of July 15, 2020

following data collection.[94] This means that they should only collect data within the limits of digital lending and not excessive data. Applications are also required to collect only relevant, adequate, and limited to what is necessary for data collection.[95]
The applications examined collect personal information that is irrelevant and contrary to the purpose of the data collection. They collect information about borrowers, such as their professional associations, credit card numbers, social media login account information, social media contacts, phone contacts, photos and videos, which are irrelevant in digital lending.

Sharing information with third parties

Data protection law states that companies must inform users of the third parties with whom their data will be shared, including details adopted to protect their data before collecting it.[96]
The reviewed applications share user/borrower information with several third parties (business partners, professional advisers, government and law enforcement agencies) and do not indicate the safeguards adopted to protect borrower data. The Applications also do not show how long these parts will have access to the data and how long they will retain it.

Confidentiality by design and by default

The Law provides that the controller must make all arrangements for processing user data[97]. The applications have encryption measures to protect their users' communications and private content. A level of security is necessary to protect user data. However, the level of protection included cannot prevent the App provider from collecting excessive information.

Right to access and delete personal data

Users of the borrowing applications have the right to access their data held by these applications[98] and request the deletion or destruction of their data that applications are no longer authorized to retain, or are irrelevant, excessive or obtained illegally[99]. Application providers have set up dedicated services to receive user requests on this subject.

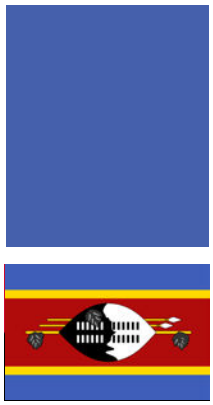
Data portability

The Law gives data subjects the right to receive their data in a structured and machine-readable format.[100] It also gives them the right, where technically possible, to have the data transmitted directly to other data controllers or processors.[101] The applications under study have incorporated these relevant provisions into their privacy policies, but there is nothing to ensure that users can recover all of the data collected on them.
The data handling practices of digital credit applications in Egypt in various aspects do

94 Article 5 of Chapter II of Law No. 151 of July 15, 2020
95 Article 5 and 6 of Chapter II of Law No. 151 of July 15, 2020
96 Article 4,5 and 6 of Chapter II of Law No. 151 of July 15, 2020
97 Article 4, and 6 of Chapter II of Law No. 151 of July 15, 2020
98 Article 2 and 5 of Chapter II of Law No. 151 of July 15, 2020
99 Article 6 of Chapter II of Law No. 151 of July 15, 2020
100 Article 2 of Chapter II of Law No. 151 of July 15, 2020
101 Article 2 et 6 of Chapter II of Law No. 151 of July 15, 2020

not comply with the applicable Law on privacy protection. To force those responsible for processing these applications to strictly comply with legal obligations in this area, they must conduct data protection impact assessments (DPIA). Beyond that, it is also necessary for the Data Protection Center ('DPC') to acquire the material and technical means, allowing it to monitor in real-time the volume, quality and quantity of data collected by data processors of the mobile applications.

Eswatini



Country Profile

Located in Southern Africa, Eswatini or Swaziland (long form: Kingdom of Swaziland) recorded 1,104,479 inhabitants in 2020. It shares a border with South Africa and Mozambique and has no access to the sea. Its GDP is estimated at 4.472 billion USD (2019) and practices an absolute monarchy[102].

102 The executive, legislative and judicial powers are concentrated in the hands of the king (the Ngwenyama) who is assisted by a council of ministers and a parliament (with two chambers: the House of Assembly (lower house) and the Senate (upper house))).

Data Protection in Eswatini

There is currently no single law enacted in Eswatini that collects and deals specifically with protecting the privacy and personal data. However, two bills, namely: the Computer Crime and Cybercrime Bill 2020 and the Data Protection Bill 2020 ("the 2020 Bill"), are supposed to deal in depth with data protection and data subjects. The Data Protection Bill No. 21/2017 ("the Data Protection Bill") aims to bring together all existing data protection laws, but it has not yet been enacted into law. Pending the promulgation of its various texts and under most modern jurisdictions, Eswatini recognizes and protects the right of data subject to their personal information[103]. Therefore, the processing (collection, use and disclosure) of information concerning a legal person, whether utilizing computer processing or other processing, can only be carried out with the data subject's express consent. The unauthorized collection and processing of personal data and their disclosure to third parties is prohibited and may only be carried out in specific cases.

Introduction

Without context, mobile money is experiencing a colossal boom in Sub-Saharan Africa;

103 Regulation 14 of the Consumer Protection Regulation provides that any digital service provider must respect the privacy of a consumer when collecting and processing personal data. A supplier may only collect, collate, process or disclose personal data concerning a consumer if: the consumer consents thereto; it is necessary for the conclusion or performance of a contract to which the consumer is a party; the provider is required by law to collect, collate, process or disclose personal data; it protects a legitimate interest of the consumer; it is necessary for the proper performance of a public law obligation towards a public body; or it is necessary for the pursuit of the legitimate interest of the provider of a third party to which the information is provided. A provider in lawful possession of a data subject's personal information is required to keep that data in a secure manner, as long as the personal data is used and for a period of at least one year thereafter.

however, Sub-Saharan Africa is experiencing slower development in other geographic areas. Indeed, sufficiently banked and provided with liquidity, Southern Africa remains little interested in transfers and payment by mobile telephony. This sub-region has only three million (3) active users, against 102 million in East Africa, 56 million in West Africa and 20 million in Central Africa in 2020, according to the GSMA report.

Of these three million (3) active users, a large part is located in South Africa, Mozambique and Eswatini (Swaziland). Specifically, in Eswatini, the access and use of mobile money have evolved Eswatini over the past few years. According to the consumer FinScope 2018 Survey, the rate of mobile money uses increased by 42% (from 28% to 70%) between 2014 and 2018. This increase in mobile money is driven by digitization from classic mobile banking services traditional mobile money to mobile phone companies and fintechs. These various services make it possible to transfer mobile money and subscribe to loan offers. The loan offers consist of mobile digital credit services in vogue in East Africa.

The first digital credit offer was launched in Eswanti by Old Mutual Limited and Swazi MTN in October 2017 through the recommendation of Likhandlela Insurance[104]. An offer allows MTN subscribers to obtain funeral assistance for the user's family who has subscribed to the offer. As an extension of this offer, MTN Eswatini, in partnership with Letshego, launched a new loan offer on January 26, 2021, through its Momo Quick Loans service[105]. In addition to this offer, several others (E-Mali[106] by Eswatini Mobile, Instant Pay Day Loans[107] by Standard Bank, and Nifty Credit[108] by GetBucks and Nifty Credit) are offered to populations through mobile applications. The objective is to attract a potential market in a country where only 52% of the population have access to financial services (FinScope Swaziland 2018). An increase in the number of offers that require significant customer profiling by companies

The latter collects personal data from their customers through mobile applications that serve as user interfaces. This practice can infringe on users' privacy; therefore, it must be questioned impartially. This type of loan service is based on mobile applications with complete freedom in Eswatini, where there is no specific law on personal data protection so abuses may exist.

Do the data processing practices of these applications, as defined in their policies and conditions of use, consider the regulations on protecting privacy? This study aims to analyze the privacy policies and the terms and conditions of these applications and examine the potential risks in Eswatini. The first part includes an overview of the data collected by

104 Ikhandlela insurance coverage amounts range from SZL 500 to SZL 2000 (the acronym for the currency of Swaziland: Lilangeni). Claimable coverage for up to 12 months.
105 This offer offers loans between 50 and 200 SZL through the MTN Eswatini Mobile Money (MoMo) service.
106 Eswatini Mobile's E-Mali offer allows people to obtain short-term loans between 50 and 800 SZL repayable in 30 days *
107 The offer Instant Payday Loans from Standard Bank allows an Estwanian get less than 33% of the monthly salary to provide him with financial assistance in an emergency. This interest free loan is designed to meet the needs of clients who require short term financing. The loaned amount is between 500 and 5000 SZL with a flat rate of 8% min 40 SZL. In addition, the customer can access the facility monthly depending on the conduct of the account. It is accessible on the Standard Bank App mobile application.
108 Nifty Credit is a digital credit application offered by GetBucks that allows people in Eswatini to obtain flexible loans up to R8000. Loans granted on the basis of the client's profile and his ability to repay.

these applications, and the second part examines their processing activities under the law on the protection of personal data. The last part ends by indicating whether or not these applications comply with the law protecting personal data.

Overview of Data Collected by Applications Ready Digital Study

MTN MoMo[109] Download Link: Google Play Store and Apple Store	information collected and processed by the application	
	sought Permissions	When starting the application, MTN MoMo asks. Access the user's contacts . Access the calendar to add or edit calendar events and send emails to invitees without the owners' knowledge . Access the precise location (GPS and network) of the user . Access Photos / Media / Files to play USB storage content, edit or delete USB storage content and other contents . Access the Camera to take photos and videos . Access information about the Wi-Fi connection and view the Wi-Fi connections . Manage other items, receive data from the internet, view network connections, control flashlight, full network access, control vibration, and prevent the device from going to sleep.
	Information collected from the user	During registration, MTN MoMo collects information allowing the user's identification: name, postal address, email address, telephone numbers and credit card number.
	Information Collected From User's Device Information Collected While Using MTN Eswatini	Orange Website MTN MoMo collects the following information from a user's device: Information stored in the device: contact list, call logs, contacts from social media accounts, photos, videos or any relevant digital content. Once a user uses the MTN Eswatini website on their mobile phone, MTN MoMo automatically collects the user's personal identification information: contact list, call logs, contacts from social media accounts, photos, videos or any relevant digital content.
	Information received from third parties	Information obtained from other entities of MTN Eswatini and the MTN Group (parent company and subsidiary) and third parties; Commercial Partners.

109 Privacy Policy of MTN Momo

	Use of User Information by the App	privacy MTN MoMo'spolicy states that it collects user data for the following purposes: · processing a user's transactions · Verifying the identity of the user 'one user · Loan disbursements and payment collection . Analysis of borrower behaviour and profiling . Bonds MTNMoMo to users · Compliance · Compliance with laws, regulations and rules relating to the "know your customer" rules and the fight against money laundering · Marketing services
	shared information with third parties access time data to third parties	MTN MoMo shares user information with: Its members, agents, MTN Eswatini and MTN Eswatini Group entities Anyone acting on behalf of a user Business partners Third-party service providers The policy is silent on how long third parties can access users' personal information and keep it. MTN, therefore, indicates that it is not responsible for the actions or policies of data processing of third parties who are not members of the MTN group.
	website tracking technologies/cookies	MTN MoMo does not provide any information about its use of cookies on its website
	Storage of user information by the App	The App does not give details regarding the storage and retention period of data collected by MTN MoMo.

e-Mali[110] Download link : Google Play Store	Information collected and processed by the application	
	sought Permissions	When starting the application, email Asos. . Access Photos / Media / Files to play USB storage content, edit or delete USB storage content and other contents . Manage other items, download files without notification, receive data from the internet, view network connections, full network access, run on startup, control vibration, and prevent the device from going to sleep.
	Information Collected From User	Information not available
	Information Collected From User's Device Information Collected While Using Eswatini Mobile Website	Information not available Information not available

110 e-Mali does not have a Privacy Policy

	Information received from third parties	Information not available
	Use of user information by the App	Information not available
	Information shared with third parties Duration of data access to third parties	Information not available Information not available
	Technologies tracking / website cookies	Information not available
	Storage of user information by the App	Information not available

Instant PayDay Loans by Standard Bank[111] (Standard Bank App) Download link : Google Play Store and Apple Store	information collected and processed by the application

111 Privacy Policy of Standard Bank App

	Sought Permissions	When starting the application, Standard Bank asks. Access the user's contacts to read the user's contacts, phone status and identity Access device ID and call information Access Photos / Multimedia / Files and Storage, edit or delete the contents of your USB storage and play the contents of your USB storage Access the Camera to take photos and videos Access the user's location to know his approximate location (based on the mobile network used), the precise location (GPS and network) Go to information about the Wi-Fi connection and view the Wi-Fi connections Manage other accesses such as: receive data from the internet, view network connections, run on startup, read the configuration of the Google service, deactivate the screen lock, prevent the device from going to sleep, control the flashlight, control vibration, create accounts and set passwords, send persistent broadcast, full network access and control near field communication
	Information collected from the user	Upon registration, Standard Bank App collects information about an identifiable natural person and / or, where applicable, a legal person, including, but not limited to, information on race, sex, sex, pregnancy, marital status , nationality, ethnic or social origin, color, sexual orientation, age; physical or mental health; well-being; disability; religion; consciousness; belief; culture; Tongue; birth; education; medical, financial; criminal or work history; any identification number, symbol, email, postal or physical address, telephone number; site; any online identifier; any other assignment specific to the person; biometric information; personal opinions; the views or preferences of the person or the views or opinions of another individual about the person; correspondence sent by the person which is implicitly or explicitly of a private or confidential nature; or any other correspondence which would reveal the contents of the original post; and the individual's name if it appears with additional personal information about them or if the disclosure of the word itself would reveal information about the individual.

	Information collected from the user's device Information collected when using the Standard Bank website	Orange Standard Bank App contains the relevant information allowing the user's identification from his terminal (see the previous section). Once a user uses the Standard Bank website on their mobile phone, Standard Bank App collects the relevant information allowing the user's identification (see the previous section).
	Information received from third parties	Information obtained from other entities of Standard Bank and the Standard Bank Group (parent company and subsidiary) and third parties; Commercial Partners
	Use of User Information by the App	privacy policy Standard Bank's states that it collects user data for the following purposes: Processing a user's transactions Verifying the identity of 'one user Loan disbursements and payment collection Analysis of borrower behaviour and profiling obligations Standard Bank's towards users compliance with laws, regulations and rules relating to "know your customer" and anti-money laundering rules Marketing services
	Information shared with third parties Duration of access data to third parties	MTN MoMo shares user information with: Its members, agents, Standard Bank and Standard Bank Group entities Anyone acting on behalf of a user Business partners Third-party service providers The policy is silent on how long third parties can access users' personal information and keep it. Also, Standard Bank indicates that it is not responsible for the actions or policies of data processing of third parties who are not members of the Standard Bank group.
	website tracking technologies/cookies	Standard Bank does not provide any information about its use of cookies on its website
	Storage of user information by the App	No details are given concerning the storage and retention period of data collected by Standard Bank.

Nifty Credit[112] by GetBucks and Nifty Credit Co Download link : Google Play Store and Apple Store	information collected and processed by the application	
	sought Permissions	On startup, Nifty Credit asks. Access Photos / Media / Files to play USB storage content, edit or delete USB storage content and other contents . Access the precise location (GPS and network) of the user . Access the Camera to take photos and videos . Access information about the Wi-Fi connection and view the Wi-Fi connections . Manage other items, receive data from the internet, view network connections, control flashlight, full network access, control vibration, and prevent the device from going to sleep.
	Information collected from a user	Information not available
	Information collected from the user's device Information collected while using a website	Information not available Information not available
	Information received from third parties	Information not available
	Use of information used by App	information not available
	information shared with third time data access to the third party	information not available information not available
	tracking technologies/website cookies	information not available
	Storing user information by The App	Information not available

Case Study: The absence of an actual privacy policy for personal data on the mobile applications of the MTN Group

As in Côte d'Ivoire with the application MyMTN, MTN Eswatini's MTN MOMO application does not have a privacy policy. The privacy policy associated with its applications is general

112 Privacy policy not found

policies that do not deal with the specifics and nature of the data collected. This situation reflects the Group's unwillingness to work in favour of compliance with regulations relating to personal data protection.

Concerning Eswatini in particular, the absence of a framework law on privacy protection does not exempt MTN from its obligations. Its presence in more than 22 countries in Africa and the Middle East and its economic and financial weight should enable it to combine its mobile applications with legal confidentiality policies adapted to different national contexts.

Analysis of Data Protection Practices of Digital Loan Applications Versus the Law Relating to the Protection of Personal Data

The absence of a framework law on protecting privacy in Eswatini is a risk for its residents. However, data controllers of companies providing digital lending applications remain subject to consumer protection law. In its rule 14, this law has made provisions regarding privacy protection pending the new law and the establishment of the 'Communication Eswatini Commission ("ECC")[113]. Also, the Data Protection Bill, 2020 (Draft) provided for legal obligations in terms of privacy protection, applicable to any automated processing or not[114]. Digital loan applications will have to fall under the said law to minimize the risks on the topical protection of privacy.

Regarding the relevant provisions concerning the respect of privacy in Eswatini, it is good to note that the applications under study are in total violation of the basic principles. These violations concern the right to privacy, equality, fairness and transparency, sharing information with third parties, confidentiality by design and by default, the right to access and deletion of personal data, and data portability. In addition, some of them do not have privacy policies for the data they process.

The data handling practices of digital credit applications in Eswatini are essential for protecting privacy. Faced with the expected dynamics of this type of service development, the country's political and administrative authorities must work to establish a Data Protection Authority. As soon as it is set up, the latter will have to carry out compliance audits of the activities of the processing responsibilities and will have to be provided with the material means allowing it to monitor the data collected by the mobile Apps.

113 The statutory body was created and supposed to be responsible for the publication of the data guidelines.
114 Section 3 of the Data Protection Bill, 2020

Ethiopia

Country Profile

Located in North-East Africa (i.e., the Horn of Africa)[115], Ethiopia, also known as the Federal Democratic of Ethiopia, shares a border with Eritrea, Djibouti, Somalia, Kenya, South Sudan, and Sudan.[116] It covers an area of 1,112,000 km2 and has a population of about 110.14 million.[117] It comprises about 80 ethnic groups, most of which are Amhara and Oromo.[118] Its capital city is Addis Ababa which is also its largest city.[119]

115 About Ethiopia https://ethiopianembassy.org/overview-about-ethiopia/
116 Ethiopia https://www.britannica.com/place/Ethiopia
117 About Ethiopia https://ethiopianembassy.org/overview-about-ethiopia/
118 Ibid
119 Ethiopia https://www.britannica.com/place/Ethiopia

Data Protection in Ethiopia

Lending apps in Ethiopia currently lack a legal framework regulating them. The country also does not have a data protection law to control the lending practices of these apps.[120] However, provisions on privacy and data protection can be found in other legislation in the country, key among them being the Constitution of the Federal Democratic Republic of Ethiopia 1995[121]. The Constitution guarantees the right to privacy and gives public officials a duty of respecting and protecting this right.[122]

Ethiopia's Data Protection Proclamation is still in its draft stages. This study will examine the privacy policies of (selected) lending apps in Ethiopia to establish whether they safeguard the right to privacy of users of the apps.

Overview of Data Collected by the Lending Apps

120 Ethiopia-Data Protection Overview Privacy and personal data protection in Africa: A rights-based survey of legislation in eight countries (May 2021) pg. 27
121 Ethiopia-Data Protection Overview
122 Section 26, Constitution of the Federal Democratic Republic of Ethiopia https://www.refworld.org/docid/3ae6b5a84.html

Dashen Amole App[5]	Information Collected and Processed by the App[1]	
	Permissions sought	Requests to access to: email, text message (SMS), social media platforms or mobile applications. Where a user no longer wants the app to access this information, they can contact customer service to stop the use of the app's service
	Information collected from the user	The app collects the user's name, address, email address and phone number upon registration
	Information collected from the user's device	
	Use of user's information	Performance of obligations to the user Following user's instructions Opening and maintenance of user's account, facilitating transactions, managing claims and risks Statistical and analytical purposes Marketing Compliance with applicable regulations
	Information received from third parties	Collects information from the following third parties: Credit reporting Government agencies Shares information with: Individuals offering support services Its subsidiaries and affiliates
	Disclosure of personal information Duration of third party access	Discloses user information under the following circumstances: When required by the law When requested by the NBE Under its public duty to disclose the information When the user or the company's legitimate interest requires disclosure of the information When the user consents to it When ordered by a court Not indicated
	Tracking technologies/ website cookies	Types of cookies used: Session cookies: Temporary and exist only when a user browses the site Persistent cookies: Permanent and stored in user's device until expiry or deletion by a user First party cookies: Owned and created by Dashen Third-party cookies: Owned and designed by Dashen's service providers

	Storage of user information	

HelloCash App[6]	Information Collected and Processed by the App	
	Permissions sought	
	Data Collected from the user	Contact information Phone number among others
	Data collected from the user's device	Internet Protocol (IP) address, device name, operating system, the configuration of the app, time and date of the user's use of the services
	Use of user's information	No explicit details on the use of the information given The policy only states that user information will be shared with third parties to help in the identification of users
	Information received from third parties	Users identity: The app uses third-party services to help in the identification of users
	Third-party use of Information/ Disclosure of information Duration of third party access	Shares information with third parties for the following purposes: Facilitation of HelloCash's services Provision of HelloCash's services on its behalf Analysis of HelloCash's services The third parties are obligated not to disclose or use user's info for any other purpose Not indicated
	Tracking technologies/ website cookies	The policy indicates that the app does not use cookies (this should be confirmed) The policy also states that the app uses third party cookies
	Storage	It does not guarantee users security of their data
Commercial Bank of Ethiopia Lending app[7]	Information Collected and Processed by the App	
	Permissions sought	Requests access to: mobile device's contacts, and other features (policy does not specify the features
	Information collected from a user	

	Information collected from the user's device	The app collects information regarding the user's mobile device (policy does not specify which information this is)
	Use of user information	The policy does not indicate how user information is used
	Information received from third parties	Not indicated
	Third-party use of information/ disclosure of information Duration of third party access	Shares user information under the following circumstances: Where user's consent has been obtained For achievement of its legitimate interest For the performance of the contract with the user Fulfilment of legal obligations - i.e., compliance with laws, government requests, judicial proceedings, court orders, legal processes For investigation and prevention of fraud or illegal activities Not indicates
	Tracking technologies/ website cookies	Not indicated
	Storage of user information by the app	Not indicated
TeleBirr by EthioTelecom[9]	Information Collected and Processed by the App	
	Permissions sought	
	Information collected from the user	Collects the following information from users: Data contained in users comments made on the site, including user's IP address and browser
	Information collected from the user's device	
	Information received from third parties	Not indicated
	Use of user's information by the app	Not indicated

	Information shared with third parties	Not indicated
	Tracking technologies/ website cookies	When making comments on the site, users can save their information in the website cookies, i.e., their name, email address e.t.c Temporary cookies: discarded when a user closes the browser Cookies that save user login information when logging in on the site Cookies saved in the user's browser when editing or publishing articles on the site
	Storage of user information	It was not indicated.

Analysis of Data Protection Practices of These Apps

Ethiopia does not have a one-piece privacy and data protection law to assess the apps' compliance under this study. However, the country has the right to privacy provided under the Constitution, where everyone is guaranteed the right not to be subjected to searches of his home, person, or property. The Constitution also guarantees individuals the right to privacy of their communications made by either telephone or telecommunications on electronic devices. It gives public officials a duty of respecting and protect this right.[123] This research will look at the data processing practices of these apps vis a viz the required standards of safeguarding privacy and protection of personal data.

Clarity of Privacy Policies

The privacy policies under study lack sufficient detail on their data processing practices. They do not provide a user with adequate information on what data is being collected, how it is being collected, and the intended use. It also does not specify which third parties will have access to the data and how long it will be granted. It is important to note that there is no mention of the safeguard measures put up to protect data shared with third parties, the duration of the retention of that data, and the security measures put in place to protect data in their possession. At the very least, a privacy policy should provide information around these critical issues. It should enable a user to know how the company (the lending app entity) intends to handle and use their data and their rights to access and correct their data.[124]

The privacy policies of the apps studied in this research can create fear among users due to a lack of certainty on how they use and store their data. They do not provide sufficient information to enable users to make informed decisions regarding their app use.

123 Section 26, Constitution of the Federal Democratic Republic of Ethiopia https://www.refworld.org/docid/3ae6b5a84.html

124 Center of Financial Inclusion pg.1

User Control

Entities owning lending apps should allow users to control their data. They should give them room to opt-out of marketing messages and enable them to access and request for correction and deletion of their data. Access to personal data is critical because data subjects have rights over their data. However, examining these apps indicates that most do not enable users to control their data. For example, the Commercial Bank of Ethiopia lending app and HelloCash app provide no rights in their policies. Only Ethio Telecom and DashenBank enable users to access their data and request deletion and correction of their data. DashenBank goes further to allow users to opt out of marketing messages.

Security

Data security is crucial, mainly where large amounts of personal data are processed. Digital lending apps, for example, are data-heavy, and access to their services is pegged on user data. They must put robust security measures to prevent breaches and access to user data by malicious parties. Some do not have security clauses indicating the safeguards they intend to put in place.

Third-Party Access

These apps do not indicate which third parties have access to user data, which information they access, how long they are granted access, and what measures these apps have put in place to ensure the security of data accessed by the third parties.DashenBank app is the only app indicating the third parties that access users' personal information.

Data Retention

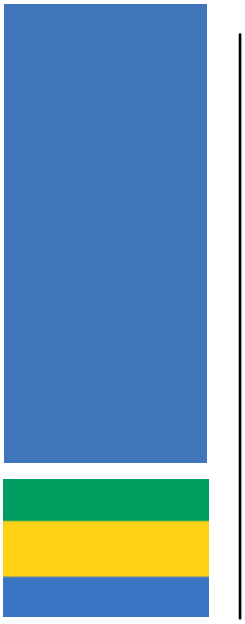
The study apps do not indicate how long they intend to retain user data and what criteria they use to determine such retention. They leave users uncertain on how long these entities will keep their data and whether such retention will continue even after uninstalling the apps.

Purpose of Data Collection

A party that processes the personal data of a data subject should expressly indicate the type of data collected and the purpose of data collection. The privacy policies of the apps in this study do not show the purpose of data collection to users. The only app that provides this information is the Dashen Bank app, which lists the information collected uses.[125]

125 Dashen Bank Privacy Policy: Collection Clause https://dashenbanksc.com/privacy-and-security/

Gabon



Country Profile

In the Gabonese Republic, Gabon is a French-speaking country located in Central Africa with 2,172,579 inhabitants[126]. It is crossed by the equator and borders the Republic of Congo, Equatorial Guinea and Cameroon. A member country of the Economic and Monetary Community of Central African States (CEMAC)[127] has a GDP of 16.87 billion USD (2019)[128] and is governed by a semi-presidential system[129].

126 https://fr.countryeconomy.com/pays/gabon
127 The Economic and Monetary Community of Central African States (CEMAC) is an international organization bringing together several countries of Central Africa, created to take over from the Customs and Economic Union of Central Africa (UDEAC). Its headquarters are in Bangui, Central African Republic. It brings together the following countries: Cameroon, the Central African Republic, Congo-Brazzaville, Gabon, Equatorial Guinea and Chad.
128 https://www.google.com/search?client = avast-a-1 & q = le + GDP + du + gabon & oq = le + PIB + du + gabon & aqs = avast..69i57j0l6.9968j0j4 & ie = UTF-8 (Source World Bank)
129 http://archive.ipu.org/parline-f/reports/CtrlParlementaire/1115_F.htm

Data Protection in Gabon

The protection of personal data in Gabon is governed by law 001/2011 of September 25, 2011[130]. The law applies to any automatic processing or not carried out on the territory of Gabon[131]. The National Commission for the Protection of Personal Data (CNPDCP)[132] is the DPA of Gabon. It was created by law 001/2011 of September 25, 2011, and is responsible for ensuring that the processing of personal data respects individual freedoms[133]. At the same time, electronic transactions are governed by Ordinance No. 00000014 / PR / 2018 of February 23, 2018.

Introduction

According to the joint report "Stimulating Electronic Commerce in Central Africa: Role of Mobile Services and Policy Implications" of the Global Grouping of Mobile Telephone Operators (GSM Association) and the Economic Commission for Africa (ECA), the countries of Central Africa lags behind those of other African regions in terms of mobile internet

130 https://www.afapdp.org/wp-content/uploads/2012/01/Gabon-Loi-relative-%c3%a0-la-protection-des-donn%c3%a9es-personnelles-du-4-mai -2011.pdf
131 Article 2 and 4 of Law 001/2011 of September 25, 2011
132 For more information: https://www.cnpdcp.ga/presentation/
133 Article 11 of Law 001/2011 of September 25, 2011

access. Indeed, data from GSMA Intelligence indicates that the penetration rate of mobile internet within the Economic Community of Central African States (ECCAS) reached 23% in 2019, against 43% in North Africa., 29% in the Economic Community of West African States (ECOWAS), 26% in the Southern African community and 21% in East Africa. In addition, the sub-region still faces significant challenges such as a shortage of ICT skills and weak institutional capacity to support innovative businesses. All things that do not facilitate the development of Mobile Money. However, within ECCAS, Gabon ranks first in terms of internet penetration, with a rate of 38%. Also, the penetration of mobile money was extreme in Gabon (43% of the population over 15 years old had an account in 2017 against 6.7% in 2017) but remained higher than in other countries. of said region 15% in Cameroon and Chad, and 6% in Congo and lower than in Kenya 73%.

Beyond that, mobile money in Central Africa and Gabon remains confined to simple services such as cash deposits and withdrawals on mobile phones. Mobile telephone companies carry out these activities: Airtel Mobile Gabon, Moov Africa Gabon, certain banks (BGFI Bank, Ecobank Gabon, etc.) offering digital services to their traditional customers and FinTechs (E-Doley Finance, Fedha Finance, etc.) with various e-money solutions. Thanks to these companies, mobile money services allow you to remotely pay your subscription to television service, your water and electricity bills, your school and university fees, but also your property taxes, etc.

Despite these possibilities offered to populations, digital lending and credit activities are not yet widely developed in Gabon as in East Africa. Only two digital credit offers are provided in Gabon by companies domiciled outside the said country. Viva PS offers the first through its Open Loans Gabon offer[134]. This offer lets one obtain unsecured personal loans directly and put borrowers and lenders domiciled in Gabon in touch. Its objective is to create an efficient, operational and instant loan market between the populations in Gabon. Loans are subject to an interest rate of between 12 and 15%, a minimum repayment and a repayment period of 90 days and 365 days, respectively. Offers are also available in African countries like Ghana, Kenya, Nigeria, and Tanzania. Spectro Coin offers the second part of the crypto-currency movement through Crypto Loans on its Bitcoin Wallet by a SpectroCoin application. This offer, launched in 2013, allows cryptocurrency account holders (Bitcoin, Ethereum etc.) in Gabon to obtain and guarantee convertible loans in different currencies such as the Euro (€) or the dollar ($). These loans range from 25 to over 15,000 (€) (16,000 FCFA to over 9,000,000 FCFA). With the gradual adoption of crypto-currencies worldwide, this type of offer will become more and more widespread. Though they elevate access to finance for citizens and especially for private borrowers, these differences enable the suppliers to collect data on their customers to follow-up the transactions and recover the funds. This practice can infringe on users' privacy and must be questioned impartially. This type of loan service based on mobile applications took root after the data protection law entered into force in Gabon's[135]. Does the data processing practices of these applications,

134 Open Loans Gabon a été lancé en Janvier 2018
135 Loi n°001/2011 du 25 septembre 2011 relative à la protection des données à caractère personnel au Gabon.

as defined in their policies and conditions of use, consider the regulations on the protection of privacy?

This study aims to analyze the privacy policies and the terms and conditions of these applications and examine their compliance with the data protection law in Gabon. The first part includes an overview of the data collected by these applications. The second part examines their processing activities under the law on protecting personal data. The last part ends by indicating whether or not these applications comply with the law protecting personal data.

Overview of Data Collected by Digital Loan Study Application

Open Loans Gabon [136] Download link : Google Play Store[137]	Information collected and processed by the application	
	Authorizations sought	At start-up, Open Loans Gabon App asks to: · Manage user calls · access a user's SMS: It displays a user's SMS to collect financial information and transactional data to collect information about a user's financial history and determine their creditworthiness Access user contacts user Access location, device and usage data: Open Loans Gabon App uses GPS technology or other location services to determine a user's current location . Access User Calendar, Open Loans Gabon App read calendar events plus confidential information, add or modify calendar events and send email to guests without owners' knowledge. . Access Photos / Multimedia / Files, Open Loans Gabon App read the contents of your USB storage modify or delete the contents of your USB storage, can read the contents of your USB storage, modify or delete the contents of your USB storage . Open Loans Gabon App can also receive data from the internet, view network connections, full network access, run at start-up, draw over other apps, control vibration, prevent devices from sleeping and set the alarm.
	Information collected from the user	During registration, Open Loans Gabon collects the user's information: email address, name and telephone number, financial and payment information, authentication, contacts actively provided by the user, credit references and country of residence.

136 Loans and Credit Privacy Policy
137 https://play.google.com/store/apps/details?id=com.viva.openloansglobal

	Information Collected From User's Device Information Collected While Using	Open Loans Gabon website collects the following information from a user's device: Artificial Intelligence (AI) technique: mobile device model, device IMEI number or serial number, SIM card information, mobile network information, device operating system, browser type, device location and setting the time zone Information stored in the device: contact list, call logs, SMS logs, contacts from social media accounts, photos, videos or any relevant digital content Once a user connects to the internet, the data applications are transmitted over HTTPS. This information is then combined for analysis or marketing purposes and made available to Orange Bank.
	Information received from third parties	Open Loans Gabon receives registers from lenders in each country where similar applications are used: Kenya, Ghana, Nigeria and Tanzania to give borrowers as wide a choice of opportunities as possible when seeking financing.
	Use of user information by the App	Open Loans Gabon's privacy policy states that it collects user data for the following purposes: · processing a user's transactions · Identity verification of a user · Loan disbursements and payment collection scoring · Credit and creation of credit models · analysis of borrower behaviour · compliance with · compliance with laws, regulations and rules relating to "know your customer" and anti-money laundering rules · Fraud prevention, · Marketing services . Obligations of Open Loans Gabon App towards users Personal and sensitive user data collected by the application with the user's consent and protected by this policy is limited to personally identifiable information, financial information and payment, authentication information, actively provided contacts by the user, credit references, and country. of residence.

	Information shared with third parties Duration of data access to third parties	Open Loans Gabon shares user information with third-party lenders to analyze credit risk and make lending decisions. Information about non-personally identifiable visitors may be provided to other parties for marketing, advertising or other purposes. These parties agree to keep this information confidential and may not disclose it. The policy is silent on how long third parties can access users' personal information and keep it. Said third parties are not authorized to track user behaviour.
	website tracking technologies/cookies	Open Loans Gabon indicates that it does not use cookies for tracking purposes. For connections on computers, the user warns when a cookie is sent. The user, therefore, has the choice of choosing or deactivating all cookies.
	Storage of user information by the App	Users' personal information is contained in secure networks. It is only accessible to a limited number of people who have special access rights to these systems and must keep the information confidential. In addition, all sensitive / credit information provided is encrypted using Secure Socket Layer (SSL) technology. All transactions are processed through a gateway provider and are neither stored nor processed on Open Loans Gabon servers. In addition, various security measures are implemented when a user enters, submits, or access their information to maintain their data security.

Bitcoin Wallet by SpectroCoin[138] Download link : Google Play Store and Apple Store	Information Collected and Processed by the Application

138 Politique de confidentialité de Bitcoin Wallet Apps

	Permissions Sought	On start-up, Bitcoin Wallet asks: · Manage user identity information, find accounts on the device and add or remove accounts. . Access the user's contacts . Access the user's Photos / Multimedia / Files and other contents, read the contents of your USB storage and modify or delete the contents of your USB storage. . Access the camera to take pictures and videos and the microphone for recording audio. Access User Location, Device, and Usage Data: Bitcoin Wallet uses GPS technology or other location services to determine a user's current location . It can also view network connections, create accounts and set passwords, full network access, change user's audio settings and prevent devices from sleeping. . Features can be automatically added within each group in the event of an update of the Bitcoin Wallet by SpectroCoin app
	Information Collected from User	During registration, Bitcoin Wallet collects the following information about users: (i) General identification data: first name, middle name, former name, aliases, surname, gender, date of birth, residential address, email, phone number, selfie (with the identity document), real-time video; (ii) Identity document data: ID Type (Passport / Identity Card / Residence permit), its copy, MRZ, document number, date of issue, date of expiry; (iii) Other Customer's profile information: profile type, member ID, referral code, login status, email confirmed status, phone confirmed status, secret questions information; (iv) Social network data: social sign in type, social network profile photo, name, surname, your comments, emotions and other actions expressed via our social network account, other your social network profile information provided by you; and (v) Information about Customer's occupation and income sources: specific occupation, main sectors of Customer's occupation, source of wealth and funds in Customer's account, source of fixed income, information on the percentage of turnover in aforementioned Customer's activity handled in cash.

	Information Collected From User's Device Information Collected While Using the https://spectrocoin.com website	Bitcoin Wallet collects the following information from a user's device: Artificial Intelligence (AI) technique: mobile device model, device IMEI number or serial number, SIM card information, mobile network information, device operating system, browser type, device location and time zone setting Information stored in the device: contact list, call logs, SMS logs, contacts social media accounts, photos, videos or any relevant digital content Once a user uses the Spectro Coin website, Bitcoin Wallet automatically collects the following information and stores it in its log files: User's IP address, browser type, internet service provider (ISP), referring / exit pages, operating system, timestamp and browse media. This information is then combined for analysis or marketing purposes.
	Information received from third parties	The Company collects your data directly from you or third parties when: you use or consult the Platform; you register on the Platform; you use our Services; you request assistance from the Services; we perform client due diligence or ongoing due diligence; we monitor your transactions; we check if you are not linked to fraudulent activity; we receive requests, orders, decisions, etc. of third parties concerning you. The Company may also collect your data from other SpectroCoin companies, as defined in the Terms and Conditions of the Platform when changing the Spectro Coin company as your service provider.

	The use of user information by the App	Bitcoin Wallet's privacy policy states that it collects user data to.Opening of the user account; . The performance of the Services (such as sale and purchase, withdrawal, deposit, exchange transactions); . Prevention of money laundering and terrorist financing (implementation of the "Know Your Customer" principle); . Prevention of crime; . The respect and implementation of international sanctions; . Assistance services; . Quality assurance; . Registration on the waiting list for the provision of the Services; . Direct marketing and use of the Company's social media accounts; . The correct and secure functioning of the Bitcoin Wallet Platform.
	Information Shared with Third Parties Duration of Data Access to Third Parties	Bitcoin Wallet shares user information with the other entities of the Spectrocoin group in 40 countries to promote customer follow-up with the international authorities in charge of the fight against cybercrime, money laundering, personal data protection, credit bureaus, etc Depending on the category of personal data and the purpose for which they are processed, your data retention period is applied within the Company, as required by law or commercial practice, to ensure the proper delivery of the Services
	Tracking Technologies / Website Cookies	Bitcoin Wallet uses mobile tracking technology and website cookies to distinguish App users. The Cookie Policy (starting now the "Cookie Policy") applies to access to the website (https://spectrocoin.com) and other domains/subdomains of ours such as https://spectrocoin.com/crypto-loans/app, https://exchange.spectrocoin.com or any other website, page, feature or content and explains the types of cookies.

	Storage of user information by the App	Bitcoin Wallet processes personal data to achieve the purposes indicated in this policy. To set the retention periods for the data collected, the Company referred to legal acts and public recommendations such as compliance with legitimate limitation periods and current commercial practice. The Company uses various technologies and procedures ensuring security to protect your data against unauthorized or illegal processing, accidental loss, misuse, unauthorized access, unlawful use, destruction, disclosure, damage, etc. This includes legal, organizational, technical and physical security measures, such as the latest security systems, passwords, ability to detect cybersecurity attacks and other threats to the integrity of the Platform, working only with suppliers' trustworthy services, etc. However, no transmission of information by email or other telecommunications channels or your access to the Platform or the Services via the internet could be completely secure. Therefore, you should exercise caution when accessing the Platform or using the Services via the internet or sharing confidential information by email or other telecommunications channels.

Case Study: The question of whether automatic processing of data carried out outside the territory of Gabon and the domiciliation of data controllers

The Law of September 25, 2011, on the protection of personal data in its articles 2, 3 and 4 stipulates that it applies to all automatic processing or not of personal data on the territory of Gabon. In the case of these two applications, even if the companies offering them are domiciled outside Gabon, the said law applies to them. However, the privacy policies provided by these two companies do not stipulate any relationship with the National Commission for the Protection of Personal Data (CNPDCP). This situation raises the question of monitoring the data processing process that companies domiciled outside the country or the data collected.

Analysis of Data Protection Practices of Digital Loan Applications Concerning the Law Relating to the Protection of Personal Data

Gabon's law on protecting personal data has clearly defined the legal obligations regarding privacy protection, applicable to any processing, whether automatic or not[139]. In doing so, digital loan applications are subject to it. However, due to their recent development, their risks to protecting privacy are current. This section highlights the relevant provisions of the law to establish whether these Applications comply with these provisions.

139 Articles 2 and 4 of Law 001/2011 of 25 September 2011

Right to Privacy

Data protection law requires that data controllers and processors (in this case, digital lending applications) handle personal data in a way that respects the right to privacy of the person concerned.[140] In this case, the law calls on the companies that provide these applications to ensure that the borrowers' right to privacy comes first when processing their data. The applications studied violate this right and process data that is intrusive and unrelated to the purpose of data collection. For example, these applications collect information such as contacts stored on a borrower's device, login information from social media platforms, accurate real-time location, Photos/Media/Files of users, .etc. Behaviour that results in the violation of the regulations on protecting personal data and the objectives assigned to their collection.

Legality, fairness, and transparency

Data protection law requires applications to collect and process data fairly and lawfully.[141] Following this provision, companies must have the consent of users.[142], Data subjects must be informed clearly and concisely of how their data will be used and ensure that all the law parameters are respected in such processing.[143]

In this case, applications should inform users why their data is collected, how their data will be used and, if shared with third parties, with whom the data will be shared and how long they will keep the data. It can be said that the applications studied are transparent as to why they collect user data and with whom they share it. However, they do not indicate how long third parties will access the data and how long they will keep it.

Limitation of Purpose, Relevance and Adequacy

Digital lending applications are required under data protection law to process personal data following data collection.[144] This means that they should only collect data within the limits of digital lending and not excessive data. Applications are also required to collect only relevant, adequate, and limited to what is necessary for data collection.[145]

The applications examined collect personal information that is irrelevant and contrary to the purpose of the data collection. They collect information about borrowers such as their social media profiles, phone contacts, photos and videos, which are irrelevant in digital lending.

Sharing Information with Third Parties

Data protection law states that these applications must notify users of third parties[146] with whom their data will be shared, including details adopted to protect their data before

140 Articles 2,3 and 4 of Law 001/2011 of 25 September 2011

141 Article 45 of Law 001/2011 of 25 September 2011
142 Article 46 of Law 001/2011 of 25 September 2011
143 Article 8, 66, 68, and 69 of Law 001/2011 of 25 September 2011
144 Article 45 of Law 001/2011 of 25 September 2011
145 Article 45 of Law 001/2011 of 25 September 2011
146 Article 13 of Law 001/2011 of 25 September 2011

collecting it.[147] The absence of a fixed period of data processing and storage constitutes a violation of the right to privacy.

In anti-money laundering and protection, the reviewed applications share user/borrower information with third parties such as affiliates, business partners, and government and law enforcement agencies. Personal data, etc., do not indicate the safeguards adopted to protect borrower data. The Applications also do not show how long these parties will have access to the data and how long they will retain it. In addition, the confidentiality rules of the two applications do not refer to their specific relationship with the DPA of Gabon.

Confidentiality by design and by default

The law provides that the controller must make all arrangements to process user data[148]. The applications have encryption measures to protect their users' communications and private content—a level of security necessary to protect user data. However, the level of protection included cannot prevent the App provider from collecting excessive information.

Right to access and delete personal data

Users of the applications have the right to access their data held by these applications and request the deletion or destruction of their data that the applications are no longer authorized to keep, or are not relevant, excessive or obtained illegally[149]. Application providers have set up dedicated services to receive user requests on this subject.

Data portability

The law gives data subjects the right to receive their data in a structured and machine-readable format. It also gives them the right, where technically possible, to have the data transmitted directly to other data controllers or processors.[150] The applications under review do not provide a means for users to exercise this right.

The formalities before the implementation of the processing of personal data

The law provides that automated processing of personal data must be declared to the National Commission for the Protection of Personal Data (CNPDCP)[151]. The law provided for the appointment of a data protection correspondent. This provision is primarily because of the domiciliation of the providers of the applications under study[152]. A documentary review of recommendations from the CNPDCP does not indicate that the companies in this study obtained these authorizations.

The data processing practices of digital credit applications in Gabon are regulated by different aspects of the law in force on privacy protection. Data protection impact assessments (DPIA) must be carried out by those responsible for processing digital credit

147 Article 14, 48, 60 and 66 of Law 001/2011 of 25 September 2011
148 Article 66, 68, 69, et 70 of Law 001/2011 of 25 September 2011
149 Article 7, 8, 9, 10, 11, 12, 13 and 14 of Law 001/2011 of 25 September 2011
150 Article 14 of Law 001/2011 of 25 September 2011
151 Article 51 of Law 001/2011 of 25 September 2011
152 Article 51 of Law 001/2011 of 25 September 2011

applications. This assessment will enable strict compliance with legal obligations. In addition, a revision of Law No. 2013-50 of June 19, 2013, relating to the protection of personal data must be considered, considering the new privacy risks. Beyond that, it is also necessary for the CNPDCP to acquire the material and technical means to monitor the volume, quality, and quantity of data collected by those responsible for processing mobile applications. Without forgetting the need for the CNPDCP to ensure a permanent technological watch on the appearance of new entities whose primary activity requires collecting and processing personal data.

Ghana

Country Profile

Ghana, also known as the Republic of Ghana, is located in Western Africa.[153] It stretches across the Gulf of Guinea and the Atlantic Ocean to its south. Ghana shares a border with Ivory Coast, Burkina Faso, and Togo[154] and has a beautiful terrain that includes low plains traversed by hills, rivers and Lake Volta, known as the largest artificial lake in the world.[155] The country covers an area of 238,533km2[156] and has a population of over 31 million[157]. Its capital city is Accra, and English is one of the most spoken languages, followed by Akan and other native languages.[158]

153 Ghana https://www.britannica.com/place/Ghana
154 Ghana https://www.nationsonline.org/oneworld/ghana.htm
155 Ghana https://www.nationsonline.org/oneworld/ghana.htm
156 Ghana Country Profile https://www.bbc.com/news/world-africa-13433790
157 Worldometer https://www.worldometers.info/world-population/ghana-population/
158 About Ghana https://www.nationsonline.org/oneworld/ghana.htm

Data Protection in Ghana

Digital lending in Ghana has a diverse regulatory framework. The lending platforms are regulated by several bodies established under various laws that govern them. Key among them is the Payment System and Services Act, 2019, which gives the Bank of Ghana the mandate to supervise and regulate them.[159] Under this law, the platforms must apply for registration with the Bank of Ghana[160], responsible for issuing out licenses[161]. Failure to apply for registration amounts to an offence and makes the platform liable upon conviction to a fine or imprisonment for a defined period.[162]

Due to their data intensity, the lending platforms are also regulated by the Data Protection Commission established under the Data Protection Act, 2012.[163] The Act establishes the Commission to protect the privacy of individuals and ensure the protection of

159 Section 3 (1), Payment Systems and Services Act, 2019
160 Section 8 (1), Payment Systems and Services Act, 2019
161 Section 3 (2)(l), Payment Systems and Services Act, 2019
162 Section 9, Payment Systems and Services Act, 2019
163 Section 2, Data Protection Act, 2012

personal data.[164] Under the Act, digital lenders must register with the Commission[165] , which mandates regulating their processing of personal information[166]. The Act makes it mandatory for the platforms to register failure to which they will be liable upon conviction to a fine or imprisonment for a defined period.

Thirdly, due to the threats posed by computer systems, the platforms also fall under the regulation of the Cyber Security Authority established under the CyberSecurity Act, 2020.[167] The Authority regulates cybersecurity activities in the country and responds to cybersecurity threats and incidents.[168] Essential among its objectives is holding accountable owners of critical information infrastructure in terms of cybersecurity activities, cyber security service providers, and practitioners in Ghana.[169]

Fourthly, the platforms are subject to the Anti-Money Laundering Act, 2020, prohibiting them from carrying out money laundering activities. The Act establishes the Financial Intelligence Center, which effectively identifies the proceeds of unlawful activities and combats money laundering and financing terrorist activities.[170]

Lastly, platforms are subject to the Electronic Transactions Act, which aims to remove and prevent barriers to electronic commerce and develop a safe, secure, and effective environment for consumers, businesses, and the Government to conduct and use electronic transactions.[171] The Act aims at creating a climate for lending platforms that is safe and secure.[172]

This study narrows its focus on regulating these platforms in terms of their data processing activities. It looks at the regulatory framework around these platforms regarding data protection. It begins by examining the nature of data processed by these platforms and subsequently analyses whether their processing activities align with the Data Protection Act. The research focuses on four key lending platforms in Ghana, i.e., Airtel Money Bosea, MTN Qwik Loan, FIDO Micro Finance, and Eco Bank Mobile Money.

164 Section 2, Data Protection Act, 2012
165 Section 27 (1), Data Protection Act, 2012
166 Section 2 (a) Data Protection Act, 2012
167 Section 2, Cyber Security Act, 2020 (Act 1038)
168 Section 3 (a)&(b), Cyber Security At, 2020 (Act 1038)
169 Section 3 (c) Cyber Security Act, 2020 (Act 1038)
170 Section 7 (a)(b)(i)(ii), Cyber Security Act, 2020 (Act 1038)
171 Section 1, Electronic Transactions Act, 2008 (Act 772)
172 Law and Practice: Fintech Market (2.2 Regulatory Regime) https://practiceguides.chambers.com/practice-guides/comparison/626/6478/10265-10267-10280-10284-10289-10292-10295-10305-10310-10314-10317-10320-10329

Overview of Data Collected by the Digital Lending Apps in this Study.

Airtel Money Bosea -Terms and Conditions not available -Privacy policy not available	Information Collected and Processed by the App	
	Permissions sought	
	Information collected from the user	
	Information collected from the user's device and	
	Information received from third parties	.
	Use of user's information by the App	
	Information shared with third parties Duration of third party access	
	Storage of user information by the App	

MTN Qwik Loan	Information Collected and Processed by the App	
	Permissions sought	The Privacy Policy for MTN Qwik Loan is not available. The only Policy available is the General MTN Group Privacy Policy[173]
	Information collected from the user	
	Information collected from the user's device	
	Information received from third parties	
	Use of user's information by the App	
	Information shared with third parties Duration of third party access	
	Storage of user information by the App	
	Tracking and Cookies	.
FIDO Micro Credit[174]	Information Collected and Processed by the App	

173 MTN Group Privacy Policy https://www.mtn.com/privacy-policy/
174 FIDO Micro Credit Privacy Policy https://www.fidocredit.com/privacy.html

	Permissions sought	Seeks permission to access: User social network account
	Information collected from the user	FIDO collects the following user information from its App and website: Personal information: registration information, billing and collection information, the information generated from user communication. Device information is collected automatically through App and website: log data, product usage data, installed applications (on the user device), SMS logs, contact list, email address, third party account, and device phone number. Third parties (sharing info with FIDO): Credit reference bureaus and identification registries, social network accounts, and third-party data providers
	Information collected from the user's device	Device information collected through App and website: log data, product usage data, installed applications, SMS logs, contact list, email address, third party account, and device phone number.
	Information received from third parties	FIDO receives information from the following third parties: Credit reference bureaus and identification registries, social network accounts, and third-party data providers.
	Use of user's information by the App	Improvement of FIDO's lending products and services and user experience Research and development Billing and collection Contacting user Marketing Provision of customer support Credit analysis Verification of user identity Compliance with legal requirements or requests by authorities Prosecution or defence of FIDO's rights in legal proceedings Provision of information to authorised third parties

	Information shared with third parties Duration of Third Party Access	Shares information with the following third parties: FIDO's associates, i.e., directors, officers, employees, and shareholders FIDO's vendors, contractors, suppliers, agents, service, and payment providers Persons acting on users behalf such as payment recipients, beneficiaries, account nominees, intermediaries, correspondents, and agent banks FIDOs referrals Business partners in cases of sale, mergers, transfer, or acquisition Credit reference bureaus Law enforcement agencies, courts, or government officials Not indicated
	Storage of user information by the App Cookies and tracking technologies	A secure layer socket protects user personal information transmitted through the App
EcoBank Mobile App[175]	Information Collected and Processed by the App	
	Permissions sought	
	Information collected from the user	Collects the following information from users upon registration: Name Email address Phone number Date of birth Gender Residential address ID number Device ID Device location
	Information collected from a user device	IP address Cookie information Mobile device and advertising identifiers Browser version Type of operating system and version Mobile network information Device settings, and Software data Also collects user information from third parties to verify user's account and device

175 EcoBank Mobile App Privacy Notice https://www.ecobank.com/privacy-centre/personal-banking-privacy-notice/mobile-app

	Information received from third parties	
	Use of user's information by the App	Authentication and authorisation of user's access to services in the App Communication to the user, i.e., through emails, SMS, phone calls, e.t.c., Serving users with advertisements Marketing its products Investigation and resolving customer complaints Investigation of fraud and violation of privacy policy
	Information shared with third parties/ Sharing of personal information	EcoBank may share user information with the following third parties: Its affiliates or partners Its technology and security subsidiaries Its service providers and marketing partners
	Storage of user information by the App Cookies and tracking technologies	Information is retained for as long as the user's account is active or needed to provide ExpressPay services, comply with legal obligations, resolve disputes, and enforce the agreement.

Analysis of the Data Protection Practices of Digital Lending Apps Vis-A-Vis the Data Protection Act, 2012

The Data Protection Act of Ghana contains key provisions, from Sections 18 to 24, central to the data protection practices of digital lending Apps operating in Ghana. The Act lays down the principles that should be observed by these Apps and their obligations concerning privacy and protection of personal information of borrowers. This section highlights relevant provisions of the Act to establish whether the Apps comply with these provisions.

Lack (Unavailability) of Privacy Policies

Privacy policies are crucial for digital lending platforms due to the intensity of their data. They provide essential information to users on the data being processed by the platforms, the intended use of the data, the third parties having access to the data, the retention period of the data, the storage of the data, and whether the data will be transferred outside the user's jurisdiction. They enable users to know how the lending platforms intend to handle their data and whether they exercise control over their data, i.e., right to access, correct, delete, or transfer personal data.[176]

Two key lending platforms under this study, i.e., Airtel Money Bosea and MTN Qwik Loan, lack privacy policies. This defect is contrary to their obligation under the Data Protection Act, 2012, which requires them to inform users of the following.

176 Center of Financial Inclusion pg.1

the nature of data being processed,
the name and address of the lending platform,
the purpose of the data collection, whether such collection is discretionary or mandatory,
the consequences of failure to provide data,
the recipients of the data, and the data subject's right to access and,
request rectification of the data before collection.[177]

User Control

Lending platforms should allow users to exercise control over their data by giving them room to access, correct, and transfer data to other providers.[178] This right should be prioritised as users are the custodians of their data. The Data Protection Act lays out this requirement and provides comprehensive guidance on how such platforms can facilitate the right of access to users.[179]

Lending platforms such as Airtel Money Bosea and MTN Qwik Loan deny users control over their data due to their lack of privacy policies, enabling users to know how such rights can be exercised. FIDO and EcoBank Mobile Money provide channels for users to exercise these rights. EcoBank Mobile Money does not allow users to request the portability of their personal information.

Purpose Of Data Collection

Online lending platforms should limit themselves to collecting and using users' data to be compatible with lending services.[180] They should consider the user's privacy[181] and ensure that the personal data processing is necessary, relevant, and not excessive[182]. The collection of a user's information such as log data, installed applications, SMS logs, contact lists, and news from social media accounts is contrary to the purpose of online lending.[183] Such information is intrusive and invades a user's privacy. There have been concerns that users' data, such as information obtained from their social media platforms for credit scoring, maybe improperly used or sold without their consent.[184] Lenders should ensure that data is used in a customer's best interest and not in a manner that harms them.[185]

Automated Decision Making

Digital lending platforms employ alternative credit scoring models that rely on AI to determine a user's creditworthiness. The AI systems access content stored in a user's device such as the camera, contacts, storage, among others, to create the user's credit score.[186] The scores created by these systems based on assessing a user's data may

177 Section 27, Data Protection Act, 2012
178 [Focus on Making Data Work for the Poor] pg. 2
179 Section 32-35, Data Protection Act, 2012.
180 [Focus on Making Data Work for the Poor] pg.10
181 Section 17 (c) Data Protection Act, 2012
182 Section 19, Data Protection Act, 2012.
183 FIDO Privacy Policy - 'Information We Collect' https://www.fidocredit.com/privacy.html
184 John Owens, Responsible Digital Credit: What Does Responsible Digital Credit Look Like? (July 2018) pg 25
https://content.centerforfinancialinclusion.org/wp-content/uploads/sites/2/1970/01/Responsible_Digital_Credit_FINAL_2018.07.18.pdf
185 [Focus on Making Data Work for the Poor] pg.2
186 Will AI Risk Analysis Really Expand Access to Credit in Africa?
https://www.theafricareport.com/107432/will-ai-risk-analysis-really-expand-access-to-credit-in-africa/

sometimes be unfair. They may further promote inequality for these lending entities should design these systems to ensure fairness and free from bias.[187] In doing this, the entities should employ personnel that constantly monitor and evaluate the decisions made by the AI systems to ensure that the systems do not cause financial inequality.[188]

Security Measures

Under the Data Protection Act, digital lending platforms are required to take necessary steps to ensure the security of data in their possession by adopting appropriate, reasonable, technical, and organisational measures.[189] This protection is needed to protect data from loss, unlawful access and processing.[190] In doing this, the apps must first identify any reasonably foreseeable risk to personal data. Secondly, they must establish and maintain appropriate safeguards against the identified risks and regularly verify that the securities are effectively implemented. Finally, they are required to ensure that the safeguards are continually updated in response to new threats.[191]

Due to the intensive amount of data processed by digital lending platforms, strict adherence to this provision is required to ensure data security. The apps understudy raise a lot of concern concerning their security measures. Some, particularly Airtel Money Bosea and MTN Qwik Loan, lack privacy policies which are vital in this case in indicating to users the security measures being adopted by the platforms. Others, such as FIDO Microcredit, do not have clauses on security measures, thus leaving users with no information on how the platform will store their data.

Processing of Data from Credit Bureaus

Digital lending apps access data from third parties such as credit reference bureaus for purposes of assessing a borrower's creditworthiness. The apps, if not restricted, can access excessive personal data contrary to the purpose of digital lending. The Act, in this case, limits the scope of data that these apps can access from credit reference bureaus to prevent the breach. It indicates that the data accessed by these apps from credit bureaus should be limited to a data subject's financial standing and history for the period that precedes 12 months after the loan was taken.[192]

187 [Focus on Making Data Work for the Poor] pg.2
188 [Focus on Making Data Work for the Poor] pg.3
189 Section 28 (1), Data Protection Act, 2012
190 Section 28 (1), Data Protection Act, 2012
191 Section 28 (2), Data Protection Act, 2012
192 Section 36 (2), Data Protection Act, 2012

Kenya

Country Profile

Kenya is a country located in the East African region.[193] It has a square foot of 580,000 Km2[194] and borders Somalia, Ethiopia, and Sudan on its Northern side and Uganda and Tanzania on its western and southern side.[195] Its capital city is Nairobi, which is the most developed County. According to the 2019 National Census report, Kenya has a population of 47,000,000 million.[196]

193 About Kenya https://www.britannica.com/place/Kenya
194 https://www.nationsonline.org/oneworld/kenya.htm
195 https://www.un.int/kenya/kenya/general-information-about-kenya
196 2019 Kenya Population and Housing Census Volume I: Population by County and Sub-County
https://www.knbs.or.ke/?wpdmpro=2019-kenya-population-and-housing-census-volume-i-population-by-county-and-sub-county

Data Protection in Kenya

Digital lending apps have provided a convenient way of accessing fast and short term loans to Kenyans. They make loans easily accessible to individuals who otherwise lack bank accounts and traditional sources of income required to borrow from financial institutions.[197] Their convenience has enabled them to gain popularity in Kenya. A study conducted by FSD Kenya indicates that more than 6 million Kenyans have accessed loans from these apps over the past years.[198]

However, these apps remain primarily unregulated, giving them room to charge high-interest rates and implement practices that violate users' rights. The Government is trying to cure this through the Central Bank of Kenya (Amendment) Bill, 2021, which is currently in Parliament.[199] This Bill, when passed, will effectively make lending apps subject to the Central Bank of Kenya (CBK) and will require them to be licensed by the Bank.[200] The Bill will make the CBK oversee the activities of these apps[201] and will, among other things, give the CBK powers to make Regulations on: the registration of the apps, their management, permitted

197 Kenya is Preparing to Crack Down on a Flood of High-Interest Loan Apps
< https://qz.com/africa/1975202/kenya-prepares-to-crack-down-on-high-interest-loan-apps/ > Accessed on 26/7/2021
198 Fsd Kenya, Digital Credit Audit Report: Evaluating the Conduct and Practices of Digital Lending Apps in Kenya (September 2019) pg iv
http://www.fsdkenya.org/wp-content/uploads/2019/11/19-09-10-Regulation-Digital-credit-audit.pdf
199 The Central Bank of Kenya (Amendment) Bill 2021
http://kenyalaw.org/kl/fileadmin/pdfdownloads/bills/2021/TheCentralBankofKenya_Amendment_Bill_2021.pdf
200 Section 33 (S) (1), Central Bank of Kenya (Amendment) Bill 2021
201 Section 3 (da), Central Bank of Kenya (Amendment) Bill 2021

and prohibited activities, their information sharing with credit reference bureaus, their data protection activities, consumer protection, and their reporting requirements.[202]

It is worth noting that once the Bill is passed, the apps will share and receive information from credit reference bureaus. This was not the case last year when the Government effectively locked them out from credit bureaus reference systems in the advent of the COVID-19 pandemic.[203]

Currently, the apps are amassing a lot of personal information when furnishing these loans. The amount of data collected by most of them is excessive compared to the purpose of processing, leading to violation of users privacy. The Data Protection Act, 2019 lays out key provisions that are crucial to the processing activities of these apps.

This study seeks to analyse the privacy policies and the terms and conditions of these apps and examine their compliance with the Data Protection Act. The first part includes an overview of the data collected by these apps. The second part examines their processing activities vis-a-vis the Data Protection Act. The final part concludes by indicating whether these apps comply with the Data Protection Act or not.

Overview of Data Collected by the Digital Lending Apps in this Study

202 Section 6 (3), Central Bank of Kenya (Amendment) Bill 2021
203 624 Digital Loan Firms Barred from Sharing Client Data with CRBs
https://www.businessdailyafrica.com/bd/markets/market-news/624-digital-loan-from-sharing-client-data-with-crbs-3416546

Tala[204]	Information Collected and Processed by the App	
	Permissions sought	Managing user's calls Accessing user SMSs Accessing user's contacts Accessing user's location (using GPS technology) and user's data
	Information collected from the user	User's name, address, email address and phone number, device phone number, SIM card, age, user name, password, financial and credit information, personal description and photograph, and other registration information
	Information collected from the user's device Information collected from the use of Tala's website	Technical data: Model of mobile device, device IMEI or serial number, SIM card information, mobile network information, the device's operating system, type of browser, devices' location and time zone setting Information stored in device: contact list, call logs, SMS logs, contacts from social media accounts, photos, videos or any relevant digital content User IP address, browser type, internet service provider (ISP), referring/ exit pages, operating system, time/date stamp, and clickstream media. This information is stored in Tala's log files and used for analysis or marketing
	Information received from third parties	Receives information from credit reference bureaus, mobile network providers, and collection agencies
	Use of user's information by the App	Processing transactions Verification Loan disbursement Credit scoring Borrower behaviour analysis Fulfilment of lender obligations Compliance with KYC (Know Your Customer Requirements) and anti-money laundering rules Prevention of fraud Marketing

204 Tala Privacy Policy https://tala.co.ke/privacy-policy-ke/

	Information shared with third parties	Shares user information with the following: Its members, agents, service providers, and any person subcontracted by it Persons acting on a user's behalf Financial Institutions, credit reference bureaus Business partners in cases of business transfer, disposal, mergers & acquisitions, etc Third-party service providers Law enforcement agencies government officials, on the grounds of: Formal request or court order Compliance with the law or reporting suspected illegal activity
	Duration of third party access	Not indicated
	Tracking technologies/ website cookies	Mobile tracking technology and website cookies are used to distinguish users of the App
	Storage of user information	User information outside Kenya and processed by staff operating outside Kenya.

Branch[205]	Information Collected and Processed by the App	
	Permissions sought	Access to: Contacts SMS Phone calls Location data: Using GPS technology
	Information collected from a user	name, address, email address and phone number, SIM card details, age, username, password, financial and credit information and other registration information.
	Information collected from the user's device	Technical Information: Model of mobile device, device IMEI or serial number, SIM card information, mobile network information, the device's operating system, the type of browser used by a user, the devices' location and time zone setting Information stored in device: contact list, call logs, SMS logs, contacts from social media accounts, photos, videos or any relevant digital content Data from any third-party application used by a user on the device
	Information received from third parties	Information is received from third parties such as credit reference bureaus, mobile network providers, and collection agencies.
	Use of user's information by the App	Determination of creditworthiness Its policy also indicates that it shares user information only in compliance with a court order, Arbitral Panel, Tribunal, Regulatory Directive or Order, or any other legal or regulatory obligation.

205 Branch' Privacy Policy https://branch.co.ke/pp

	Information shared with third parties Duration of third party access	Shares user information with the following: Credit reference bureaus Its members, i.e., subsidiaries, affiliates, holding companies Business partners during the sale of business or assets Authorities in compliance with legal or regulatory obligations Not indicated
	Storage of user information	It stores user information outside Kenya, where its staff is processed outside the country.
	Tracking and Cookies	Mobile tracking technologies/ website cookies are used to distinguish users of the App.
LionCash[206]	Information Collected and Processed by the App	
	Permissions sought	Access to: SMSs Location data: Uses precise real-time location information Phone: To read phone status and identity Contacts
	Information collected from the user	User's name, job title, company name, address, email address, phone number, gender, age, date of birth, nationality, professional associations and registration numbers, information about users use of LionCash products, mobile money statements, banking or account information, login information of users social media accounts, phone contacts in user's device.
	Information collected from the user's device	Technical Information: Type of mobile device, IP address, the device's operating system, and device identifier. This information is collected automatically from a user's device and web browsers through cookies User's usage of the App and consumption of digital advertisement Location data: Collects precise real-time location from a user's device
	Information received from third parties	Receives information from its business partners such as; user's name, company name, job title, address, email address, and phone number for verification purposes May also collect publicly or commercially available information from other third parties.
	Use of user's information by the App	Delivery of services Provision of information on products and services Improving site, App, products and services Marketing Defending legal suits, compliance with laws and court orders, and prevention for fraud

206 LionCash Privacy Policy http://lioncash.co/privacy-policy/

	Information shared with third parties Duration of third party access	Shares user information with: Service providers Business partners assist them with providing products and services to users Authorities, in compliance with laws, regulations, and court orders, and prevention of fraud Business partners in mergers, liquidation, dissolution, e.t.c., Not indicated
	Storage of user information	Stores user information in databases and servers outside Kenya
Timiza[207]	Information Collected and Processed by the App	
	Permissions sought	Requests access to: Location data - accesses real-time location information Phone - to read phone status and identity Contacts
	Information collected from a user	
	Information collected from the user's device	
	Information received from third parties	Obtains information from the following: Safaricom: Including user's phone number, name, date of birth, ID/ passport number, and any other relevant information Accesses information on user's use of MPESA services and Safaricom services Government's IPRS system. Credit reference bureaus and shares user credit info with the bureaus
	Use of user's information by the App	Delivery of services Marketing purposes Improvement of site, App, products and services Defending legal claims, compliance with the law and court orders, and preventing fraud
	Information shared with third parties/ Sharing of personal information	Shares user information with: Its service providers, dealers, and agents Its professional advisors, including lawyers and auditors Safaricom relating to MPESA services Local and international law enforcement agencies and government agencies in the prevention of fraud and prosecution of criminal activities
	Storage of user information by the App	

207 Absa Timiza Account Terms and Conditions https://www.absabank.co.ke/content/dam/kenya/absa/pdf/Terms-of-use/timiza-account-terms-and-conditions.pdf

O-Kash[208]	Information Collected and Processed by the App	
	Permissions sought	Requests access to: · Photos and media on user's device · Device' location
	Information collected from the user	MPESA number, phone number, borrower's name, age, email address, and other contact information. Contacts of emergency contacts may be used to verify user's identity
	Information is collected from the user's	device make and model, operating system, software applications, and a unique user identifier. Email and phone book contacts, call logs, SMSs, and GPS location information.
	Information received from third parties	Collects information from credit reference bureaus and financial institutions.
	Use of user's information	Verification and credit scoring
	Information shared with third parties	Shares user information with: Credit reference bureaus Collection agencies Government and law enforcement agencies Professional advisers Business partners during mergers, acquisitions, and insolvencies
	Storage of user information by the App	Transfers user data to other countries, including countries that do not have data protection laws

Case Study: O-Kash: Debt Shaming

O-Kash has been notorious for debt shaming borrowers on its platform. The App relies on contacts on a borrower's device and the contact information of the borrower's emergency contact/ referee.[209] The App, upon installation, requests access to a borrower's contacts and requires the provision of an emergency contact once the borrower asks for a loan.[210] Its terms and conditions provide that a borrower offers express consent to contact the borrower's referee when the borrower defaults in paying the debt.[211] Based on this, the App has been aggressively calling borrowers referees and contacts and, in some instances issuing threats to make them pay.[212]

Such acts amount to violations of the borrower's privacy. They are contrary to the provisions of the Data Protection Act, which requires the personal data of data subjects to be processed under their right to privacy.[213]

Analysis of the Data Protection Practices of Digital Lending Apps Vis-A-Vis the Data

208 O-Kash Privacy Policy https://ke.o-kash.com/kenya/en/privacy-policy/
209 O-Kash Privacy Policy https://ke.o-kash.com/kenya/en/privacy-policy/
210 O-Kash Privacy Policy https://ke.o-kash.com/kenya/en/privacy-policy/
211 Clause 8, O-Kash Terms and Conditions https://ke.o-kash.com/kenya/en/Terms-for-Kenya/
212 This Lending App Publicly Shames You When You Are Late on Loan Payment https://restofworld.org/2020/okash-microlending-public-shaming/
213 Section 25 (a) Data Protection Act, 2019

Protection Act, 2019

The Data Protection Act of Kenya contains critical provisions central to the data protection practices of digital lending Apps operating in Kenya. The Act lays down the principles that should be observed by these Apps and their obligations concerning privacy and protection of personal information of borrowers. This section highlights relevant provisions of the Act to establish whether the Apps comply with these provisions.

Right to Privacy

The Data Protection Act requires that data controllers and processors (in this case, the digital lending Apps) process personal data in a manner that respects the right to privacy of the data subject.[214] In this case, the Act requires the Apps to prioritise the right to privacy of borrowers when processing their data.

The Apps in the study violate this right and process data that is intrusive and irrelevant to data collection. For example, these apps collect information such as contacts stored in a borrower's device, social media platforms' login information, precise real-time location, among others, which are intrusive and excessive concerning the purpose of data collection. An App such as O-Kash has been notorious for debt shaming borrowers by calling and harassing their guarantors and contacting persons stored in their devices to make them pay the debt.[215] Such acts invade the privacy of borrowers.

Lawfulness, Fairness and Transparency

The Data Protection Act requires these apps to process data lawful, fair, and transparently.[216] This entails the Apps ensuring that data subjects are informed clearly and concisely how their data will be used and ensuring that all the law parameters are met in such processing.[217] The Act further requires the Apps to ensure that the borrowers' consent has been obtained before processing their data.[218]

In this case, the Apps should inform users why their data is being collected, how their data will be used, and in cases of third party sharing, who the data will be shared with and how long they will retain the data. The Apps understudy can be transparent about collecting user data and sharing it. However, they fail to indicate how long the third parties will access the data and how long they will retain it.

Purpose Limitation, Relevance and Adequacy

Digital lending Apps are required under the Data Protection Act to process personal data in line with data collection, which means that they should only collect data within the limits of digital lending and not excessive data. The Apps are also required to collect relevant, adequate, and limited to what is necessary for data collection.[219]

---

214 Section 25 (a) Data Protection Act, 2019
215 Debt of Shame: How Rogue Digital Lenders Use Unorthodox Tactics to Recover Loans https://www.instagram.com/p/CRgoT7OM-8hy/
216 Section 25 (b) Data Protection Act, 2019
217 Privacy International Guide to Data Protection
218 Section 30 (1), Data Protection Act 2019
219 Section 25 (d), Data Protection Act, 2019

The apps under review collect irrelevant and intrusive information such as; borrowers' contacts, credit card numbers, social media login details and contacts, photos, and videos.

Sharing Information with Third Parties

The Data Protection Act stipulates that these Apps should inform users of the third parties with whom their data will be shared, including details adopted to safeguard their data before collecting it.[220]

The Apps under review share user/borrower information with credit reference bureaus, business partners, professional advisors, telecom companies like Safaricom, government and law enforcement agencies, etc., and fail to indicate the safeguard measures adopted to protect borrowers' data. The Apps also fail to mean how long these parties will be given access to the data and how long they will retain it.

Transfer of Personal Data Outside Kenya

The Data Protection Act provides that these Apps shall ensure that personal data is not transferred outside Kenya unless adequate safeguards for data protection have been put in place and consent of the data subject has been obtained.[221] It also states that these Apps shall only transfer data to other countries where they have given proof to the data commissioner on the appropriate safeguards concerning the security and protection of personal data.[222] The Act further states that the Apps may only transfer personal data to other countries where they have given proof to the Data Commissioner of the appropriate security safeguards and protection of personal data and the appropriate safeguards, including jurisdictions with commensurate data protection laws.[223]

Most of the companies that own the Apps under review are established outside Kenya and have databases and servers storing borrowers' personal information outside Kenya. This creates a security risk for the borrowers regarding their data. For example, Tala, Branch, and O-Kash have their headquarters outside the country and store borrowers' personal information in servers located outside the country.[224] Some Apps store data in countries that lack commensurate data protection laws like Kenya. O-Kash, for example, transfers personal data to countries that do not have the same level of data protection as Kenya.[225]

Privacy by Design and by Default

The Data Protection Act requires these Apps to implement appropriate technical and organisational measures designed to effectively implement the data protection principles and integrate the necessary safeguards for processing.[226]

---

220 Section 29 (d), Data Protection Act 2019
221 Section 25 (h), Data Protection Act 2019
222 Section 48 (a) Data Protection Act, 2019
223 Section 48 (b), Data Protection Act 2019
224 Tala Privacy Policy: https://tala.co.ke/privacy-policy-ke/; Branch Privacy Policy: https://branch.co.ke/pp; O-Kash Privacy Policy: https://ke.o-kash.com/kenya/en/privacy-policy/
225 O-Kash Privacy Policy, Clause C
226 Section 41 (a) & (b), Data Protection Act, 2019

The Act further provides that these apps should implement technical and organisational measures that ensure, by default, only personal data that is necessary is processed.[227] The Act states that the Act should consider the amount of personal data collected, the extent of the processing, the storage period, the accessibility of the data, and the cost of processing the data and technologies used.[228]

The apps understudy should have been designed to prevent them from collecting excessive information and should have been restricted to collecting only what is necessary for purposes of digital lending.

Right of Access and Deletion of Personal Data

Borrowers are provided with the right to access their data held by these Apps[229] and the right to request for deletion or destruction of their data that the Apps are no longer allowed to retain, or are irrelevant, excessive or obtained unlawfully[230].
The Apps, however, do not create a room where borrowers can exercise these rights. Tala, for example, keeps user information even after the user has uninstalled the App.[231]

Data Portability

The Act gives data subjects the right to receive their data in a structured and machine-readable format.[232] It also gives them the right, where technically possible, to have the data directly transmitted to other data controllers or processors.[233] The apps under study do not provide an avenue to users where this right can be exercised.

Data Protection Impact Assessment (DPIA)

The Act requires that a Data Protection Impact Assessment (DPIA) be conducted where the processing of personal data is likely to result in a high risk to the rights and freedoms of the data subject.[234] None of the apps understudied has conducted a DPIA despite the massive amount of data.
Digital lending apps in Kenya may be processing data contrary to the Data Protection Act, 2019. Their practices, as a result, are violating the privacy of users and their rights to have their data protected. The Government should mandate these apps to revise their privacy policies to align with the Data Protection Act.

227 Section 41 (3), Data Protection Act, 2019
228 Ibid
229 Section 26 (b), Data Protection Act, 2019
230 Section 40 (1) (b), Data Protection Act, 2019
231 Tala Privacy Policy https://tala.co.ke/privacy-policy-ke/
232 Section 38 (1), Data Protection Act, 2019
233 Section 38 (3), Data Protection Act, 2019
234 Section 31 (1), Data Protection Act, 2019

Mali

Country profile

A landlocked francophone country in West Africa, the Republic of Mali borders Mauritania, Algeria, Niger, Burkina-Faso, Côte d'Ivoire, Guinea and Senegal. With more than 19 million inhabitants, it has a 17.28 billion USD (2019) GDP and is supported by a semi-presidential regime[235]. In May 2013, the Malian government enacted Law no. 2013-015 on protecting personal data in the Republic of Mali[236]. The law applies to automated or non-automated processing carried out in whole or in part on the territory of Mali[237]. The Autorité de Protection des Données à Caractère Personnelles (APDP) is Mali's DPA[238]. Its primary mission is to protect personal data and regulate the Republic of Mali's digital sector.

235 Reading Mali's February 25, 1992 constitution indicates that it relies on a semi-presidential regime. Indeed, the said constitution enshrines the separation of powers and the responsibility of the Government before the National Assembly (Article 54, 78 et 79). Cf: https://mjp.univ-perp.fr/constit/ml1992.htm#3

236 Loi no 2013-015 du 21 mai 2013 relative à la protection des données personnelles (Law No. 2013-015 of 21 May 2013 on the protection of personal data) <https://apdp.ml//wp-content/uploads/pdf/Loi-sur-la-protection-des-donnees-personnelles-du-21-mai-2013.pdf > 2 May 2021.

237 Article 4 of Law no. 2013-015

238 Website: https://apdp.ml/

Data Protection in Mali

Mobile-to-mobile and transactional data development has opened up new, hitherto untapped services. One of these new services is digital credit, part of second-generation digital financial services. It makes it possible to provide people with instant loans for their particular needs—an alternative to traditional credit that is very successful in English-speaking countries in Africa.

In French-speaking countries, particularly West Africa, the first digital credit experiments began in 2018 with the 'Momo Kash' offer from MTN & Bridge Bank in Côte d'Ivoire and Mali with Singa Ni Mara[239] from the First Microfinance Agency (PAMF-M) and Orange in Mali.

239 SINGA NI MARA is a savings and pico / micro-credit offer to individuals, in partnership with the microfinance institution PAMF (Première Agence de Microfinance) launched on Wednesday, June 13, 2018. It allows people to instantly benefit from credit and savings products, helping them quickly and easily manage unforeseen expenses or save. It is accessible using a USSD code for Orange Money customers of Orange Mali and passes through its Orange Mali Sugu mobile application.

Aware of the potential flexibility of this type of offer, another microinsurance service will develop between the start-up OKO[240][241] and Orange Mali. This offer is based on satellite data and mobile money transfer services to design automated insurance products for farmers. As with the Singa Ni Mara offer, the Oko offer is accessible on the mobile phones of populations using a USSD code and on the mobile application Orange Money Mali: Orange Mali Sugu. A mobile application which in addition to the data collected with Orange Money Mali accounts also associated with those of the Oko and Singa Ni Mara, offers; a large volume of data, the processing of which may entail potential risks to the respect for the privacy of these users and which must be analyzed. Above all, this type of data processing based on mobile applications began after adopting the law on protecting personal data in Mali. Therefore, it is essential to know whether the data processing practices of the Orange Mali Sugu mobile application, as defined in its policy and conditions of use, take into account the regulations on the protection of privacy.

This study aims to analyze the privacy policies and the terms and conditions of these applications and examine their compliance with the data protection law in Mali. The first part includes an overview of the data collected by these applications. The second part examines their processing activities under the law on personal data protection. The last part ends by indicating whether or not these applications comply with the law on personal data protection.

Overview of the Data Collected by Orange Mali Sugu

240 https://fr.oko.finance/mali
241 The OKO agricultural insurance offer was launched on Tuesday, January 21, 2020

Orange Mali Sugu[242] Download link : Google Play Store and Apple Store	Information collected and processed by the application	
	Authorizations sought	At start-up, Orange Mali Sugu asks: · Manage user calls · access a user's SMS: It displays a user's SMS to collect financial information and transaction data to collect information about a user's financial history and determine their creditworthiness Access user contacts user Access location, device and usage data: Orange Mali Sugu uses GPS technology or other location services to determine the current location of a user
	Information collected from the user	During registration, Orange Mali Sugu collects the user's information: name, address, email address and phone number, device phone number, SIM card, age, username, password, financial and credit data, descript personal ion and photograph, and other registration
	information Information collected from the user's device Information collected while using the Orange Mali website	Orange Mali Sugu collects the following information from the '' user's device: Artificial Intelligence (AI) technique: mobile device model, device IMEI number or serial number, SIM card information, mobile network information, operating system device, browser type, device location and time zone setting Information stored in the device: contact list, call logs, SMS logs, contacts from social media accounts, photos, videos or any relevant digital content Once a user uses the Orange Mali website on their mobile phone, Orange Mali Sugu collects the following information automatically and stores it in their files Logs: User IP address, browser type, Internet Service Provider (ISP), referring / exit pages, operating system, timestamp and browse media. This information is then combined for analysis or marketing purposes and made available to Orange Money Mali, Oko Israel and PAMF.
	Information received from third parties	Information was obtained from other entities of the Orange Group: Orange Money Mali and Orange Finances Mobile Mali, Credit Assessment Offices (BIC), Mobile network providers and collection agencies.

242 The Orange Money Sugu application does not have a Personal Data Privacy Policy. And only available, the conditions of use Orange Money Mali which deals in point 12 with the issue of data processing.

	Use of user information by the App	The conditions of use Orange indicate indication That It collects user data for the Following Purposes: · processing a user's transactions · Identity verification of a user · Loan Disbursements and collection of payments scoring · Credit And Creation of credit models · analysis of borrower behaviour . Orange Mali Sugu App's obligations towards users · compliance with · compliance with laws, regulations and rules relating to "know your customer" and anti-money laundering rules · Fraud prevention, · Marketing services
	Shared information with third parties Duration of data access to third parties	Orange Mali Sugu shares user information with: Its members, agents, service providers, the Orange Money Group entities, and the entities that subcontract the data collected. · Anyone acting on behalf of a user · financial institutions, credit bureaus and agencies (BIC) · Business partners in the event of business transfers, divestitures, mergers & acquisitions, etc. Third-party service providers Law enforcement agencies (The Authority for the Protection of Personal Data (APDP)), government officials, based on: Formal request or decision Justice Compliance with Law or Reporting Suspected Illegal Activity The policy is silent on how long third parties can access users' personal information and keep it.
	Tracking Technologies / Website Cookies	Orange Mali Sugu uses mobile tracking technology and website cookies to distinguish App users.
	Storage of User Information by the App	Orange Mali Sugu stores user information at a destination outside Mali. Data may also be processed by Orange Money Mali, Orange Mali staff. No details are also given concerning the retention period of data by Orange Mali.

Case Study: Orange Mali Sugu (The question of the duration of storage of user data)

The conditions of use of Orange Money Mali accounts associated with the Orange Mali Sugu Apps do not detail the duration of user data storage. This insufficiency constitutes a violation of law relating to data protection in Mali, which requires that data be collected for a fixed period.[243] In addition, the Orange Mali Sugu application does not have a specific privacy policy.

243 Article 15 of Law no. 2013-015

Analysis of Data Protection Practices of Digital Loan Applications Concerning the Law Relating to the Protection of Personal Data

Mali's law on personal data protection has clearly defined obligations in privacy laws, applicable to any processing, whether automatic or not[244]. In doing so, the digital applications of subject loans. However, due to their recent development, their risks to protecting privacy are current. This section highlights the relevant provisions of the law to establish whether these Applications comply with these provisions.

Right to Privacy

Data protection law requires that data controllers and processors (in this case, digital lending applications) handle personal data in a way that respects the right to privacy.[245] In this case, the law calls on applications to ensure that the borrowers' privacy rights come first when processing their data. The applications studied violate this right and process data that is intrusive and unrelated to the purpose of data collection. For example, these applications collect information such as contacts stored on a borrower's device, login information from social media platforms, and accurate real-time location, which is intrusive and excessive concerning data collection.

Legality, fairness and transparency

Data protection law requires that these applications process data lawful, fair, and transparently.[246] This implies that applications ensure that data subjects are informed clearly and concisely of how their data will be used and that all the law parameters are respected in such processing.[247]

In this case, applications should inform users about why their data is collected, how their data will be used and, if shared with third parties, with whom the data will be shared and how long they will keep the data. It can be said that the applications studied are transparent as to why they collect user data and with whom they share it. However, they do not indicate how long third parties will access the data and how long they will keep it.

Limitation of Purpose, Relevance and Adequacy

Digital lending applications are required under data protection law to process personal data following data collection.[248] This means that they should only collect data that only concerns digital lending and not excessive data. Applications should only collect relevant, adequate and limited to data collection.[249]

Orange Mali Sugu collects personal information that is not relevant to the purpose of the

244 Article 5 and 6 of Law no. 2013-015
245 Article 8 of Law no. 2013-015

246 Article 7 of Law no. 2013-015
247 Article 15 of Law no. 2013-015
248 Article 15 of Law no. 2013-015
249 Article 15 of Law no. 2013-015

data collection. It contains borrowers' information such as credit card numbers, financial transactions, social media login account information, social media contacts, phone contacts, photos and videos, etc., irrelevant in digital lending.

Sharing Information with Third

Parties data protection law states that these applications must notify users of third parties with whom their data will be shared, including details adopted to protect their data before collection.[250] In the specific case of the Orange Mali Sugu Apps, the lack of a fixed duration for data processing constitutes a violation of privacy rights[251].

Orange Mali Sugu App's reviews share user/borrower information with the credit information office (CIO), business partners, professional advisers, government and law enforcement agencies, etc. They do not indicate the safeguards adopted to protect borrower data. Orange Mali Sugu App's also does not mean how long these parts will have access to the data and how long they will retain it.

Transfer of personal data outside Mali

Provision respected by the various application providers

Confidentiality by design and by default

The law provides that the data controller must make all arrangements for processing user data[252]. Orange Mali Sugu App's have encryption measures to protect its users' communications and private content. A level of security is necessary to protect user data. However, the level of protection included cannot prevent the App provider from collecting excessive information.

Right to access and delete personal data

Users of the Orange Mali Sugu App's have the right to access their data held by these applications[253] and have the right to request the deletion or destruction of their data that the applications are no longer authorized to retain. Users also have the right to request deletion of irrelevant, excessive or data obtained[254]illegally.

Data portability

The law gives data subjects the right to receive their data in a structured and machine-readable format.[255] It also gives them the right, where technically possible, to have the data transmitted directly to other data controllers or processors.[256] Orange Mali Sugu App's under review do not provide a means for users to exercise this right.

Data Protection Impact Assessment (DPIA)

250 Article 11 and 15 of Law no. 2013-015
251 Article 8 of Law no. 2013-015
252 Article 8 of Law no. 2013-015
253 Article 12,13,14,18 and 18 of Law no. 2013-015
254 Article 12,13,14,18 and 18 of Law no. 2013-015
255 Article 12 of Law no. 2013-015
256 Article 12 of Law no. 2013-015

The law requires that a report on the data processing process be produced annually and sent to the Personal Data Protection Authority (APDP). In addition, data transfer authorizations have indicated the need for data controllers to perform a Data Protection Impact Assessment (DPIA). However, Orange Mali Sugu has not produced or made available their reports.

Conclusion

The data processing practices of digital credit applications in Mali do not respect the basic principles of privacy protection law. Data protection impact assessments (DPIA) must be required to force those responsible for processing these applications to comply with legal obligations in this area strictly. In addition, a revision of law no. 2013-015 of May 21, 2013, relating to personal data protection must be considered, considering the potential risks for privacy. Beyond that, it is also necessary for the APDP Mali to acquire expertise and technical equipment to monitor in real-time the volume, quality and quantity of data collected by those data managers for processing mobile applications.

Morocco

Country Profile

The Kingdom of Morocco is located in northwest Africa and has a population of more than 37 million[257] with an estimated GDP of 117 USD Billion in 2021.[258] The country practices a unitary monarchical system of government with an elected parliament. According to the African Development Bank (2018), the Moroccan economy is considered the most robust in Africa. The service sector dominates the Moroccan economy, contributing around 55% of GDP.[259]

257 Atlas monde https://www.atlas-monde.net/afrique/maroc/ > accessed on 23 August 2021.
258 Trading economics https://tradingeconomics.com/morocco/gdp > accessed on 25 August 2021.
259 https://thefintechtimes.com/fintech-africa-morocco/ > accessed on 25 August 2021.

Data Protection in Morocco

According to Freedom House (2020), Internet freedom in Morocco is characterised by tenuous as a crackdown on online journalists covering protests continue, and pro-government news websites publish false information about activists and journalists. While internet access increases overall, the government maintains sophisticated surveillance systems.[260]

Morocco's law on data protection was enacted on 18 February 2009.[261] The rule applies to the processing of personal data wholly or partly by automatic means and the non-automatic processing of personal data contained or intended to be contained in manual files.[262] The country as a Data Protection Agency – the DPA – the National Commission for the Supervision Protection of Personal Data (CNPD)[263] was established by Decree on 21 May 2009.

260 Freedom House 2020 https://freedomhouse.org/country/morocco/freedom-net/2020 > accessed on 25 August 2021.
261 Law 09-08 of 18 February 2009 https://www.cndp.ma/images/lois/Loi-09-08-Fr.pdf > accessed on 10 May 2021.
262 Law 09-08 of 18 February 2009, chapter I, section 1, art.2.
263 https://www.cndp.ma/fr/ > accessed on 24 August 2021.

Financial System and Fintech in Morocco

Banks, monitored by the Central Bank of Morocco (Bank Al Maghreb – BAM),[264] account for nearly half of the country's financial system.[265] Of the 19 banks, the top three are responsible for over two-thirds of all bank assets and deposits. Since 2007, BAM has made discernible e orts to improve financial inclusion.[266]

In 2014, was developed a new framework (No. 103-12) published in the Journal Officiel in March 2017 (Banking Law).[267] It applies to institutions (including participating Islamic Banks): receiving funds from the public, conducting credit operations, making available to the customers of any means of payment or management.

The law creates two categories of financial providers, thereby increasing competition within the payment services arena. A new type, loosely translated as 'participative banking', allows non-banks to o er payment services enabling cash transfers and withdrawals from payment accounts.

According to Fintechnews Middle East (April 2021),[268] Morocco is the third largest fintech hub in the Arab world, hosting 13% of all 400 active fintech solutions, or about 40 fintech solutions. It is noted that the total banking penetration in Morocco stood at just 28.6% in 2017, and the economy remains cash-based mainly, with around 80% of transactions made using cash.

A high level of mobile coverage reportedly supports Morocco's Fintech ecosystem. Fintech News Middle East first reported that out of the 40 active fintech solutions in Morocco, payment, remittance, and point-of-sale (POS) systems are the most developed segment.[269] Some other forms of Fintech growing in popularity are crowdfunding, personal financial services, lending platforms, and advanced data analytics. For example, Cotizi[270] is reportedly the first crowdfunding platform in the country.

Wafacash/Jibi: The Money Lending Mobile Application

Jibi[271] is a 24/7 mobile money application that allows customers to make transactions from the internet or user's mobile. With Jibi, customers can: pay for purchases using their mobile phone from an extensive network of merchants; deposit and withdraw money whenever and wherever they want through our vast network of Wafacash branches and retail agents throughout Morocco.

264 https://www.bkam.ma/ > accessed on 24 August 2021.
265 https://thefintechtimes.com/fintech-africa-morocco/ > accessed on 22 August 2021.
266 Idem
267 Law No. 103-12 – On Credit Institutions and Similar Bodies (Banking Law) https://dfsobservatory.com/sites/default/files/Parliament%20of%20Morocco%20-%20Law%20No.%20103-12%20-%20On%20Credit%20Institutions%20and%20Similar%20Business%20%28Banking%20Law%29.pdf > accessed on 22 August 2021.
268 News report https://www.moroccoworldnews.com/2021/01/331921/cmi-chief-moroccos-2020-e-commerce-transactions-rose-43/ > accessed on 22 August 2021.
269 News report https://www.crowdfundinsider.com/2021/04/174365-morocco-is-now-home-to-many-fintech-services-crowdfunding-lending-advanced-data-analytics-platforms-report/ > accessed on 22 August 2021.
270 http://www.cotizi.com/ > accessed on 22 August 2021.
271 Available on Google Play – https://play.google.com/store/apps/details?id=com.b3g.wafacash.jibi&hl=fr&gl=US and iOs – https://apps.apple.com/fr/app/jibi-pro/id1371478054

It also sends money from their phone to a Jibi mobile account, bank account or Wafacash branch. One can also receive a money transfer from one of the Wafacash branches, pay bills or make purchases online without giving out bank details or top up their mobile phone.

In partnership with Wafasalaf, Wafacash offers a consumer credit that allows for short-term financing of any project or expense. Wafacash provides solutions to meet the needs of its customers, ranging from credit to microcredit in collaboration with Wafasalaf and Al Amana Micro Finances – it acts as a lending application.[272]

Analysis of the lending App

Wafacash/Jibi[273]	Information Collected and Processed by the App[274]	
	Permissions sought	Find accounts on the device Find accounts on the device Take pictures and videos View Wi-Fi connections Read phone status and identity Read the contents of client USB storage Modify or delete the contents of client USB storage
	Information collected from the user	Personal data: title, surname, first name Telephone number Telephone operator Email address
	Information collected from the user's device	Approximate location (network-based) Precise location (GPS and network-based) Read phone status and identity The customer's responsibility is to adequately protect their mobile device, back up their data and equipment, and take reasonable and appropriate precautions to detect viruses and other destructive elements. Wafacash shall not be liable for any losses the customer may suffer because of the above events. All operations carried out by the customer via the ''Jibi Mobile Application'' and the ''Jibi Website'', which has been authenticated, are considered carried out by the customer. The customer expressly accepts and undertakes not to contest.

272 https://www.wafacash.com/cr%C3%A9dit-micro-cr%C3%A9dit / https://www.alamana.org.ma/fr/alamana/tout-savoir-sur-le-micro-credit > accessed on 23 August 2021.
273 https://www.wafacash.com/mentions-legales > accessed on 22 August 2021.
274 Terms & Conditions (adopted on 4 July 2018) https://www.jibi.co.ma/DocReadme/CG_JIBI_VF_04072018_Valide.pdf / Privacy Policy https://www.jibi.co.ma/DocReadme/PROPRIETE%20INTELLECTUELLE%20JIBI.pdf > accessed on 25 August 2021.

	Information collected from the use of Jibi's website	Access to the website www.wafacash.com is unlimited and open to all. Wafacash reserves the right, because of the permanent evolution of the internet and the products and tariffs, to modify or delete, at any time and without prior notice, the proposed conditions of use and the information present on the www.wafacash.com website. Following law 09-08 on the protection of individuals about the processing of personal data, it is brought to the user's attention that by accepting the general conditions, the site user acknowledges that their data will be subject to computer processing. In any case, wafacash only collects personal information relating to the user for certain services offered by the www.wafacash.com website. The user provides this information with full knowledge of the facts when they enter it.
	Information received from third parties	The information collected is subject to computer processing. It is intended for Wafacash, its group and their respective subsidiaries, which, by express agreement, are authorised to proceed with their automated or non-automated processing, to communicate them to the legal entities of their group, partners, and service providers. Wafacash, its group and their respective subsidiaries undertake to use the information collected solely to meet legal and regulatory obligations. It may also be used to keep the customer informed of new offers, events, actions, or publications that may interest him.
	Use of user's information by the App	Receive data from the internet Mock location sources for testing View network connections Full network access Prevent device from sleeping Read Google service configuration
	Information shared with third parties	The personal information collected is intended for use by the Wafacash departments responsible for responding to customer requests to manage HR applications, complaints and appeals, and partnership applications. It is used by Wafacash, the Attijariwafa Bank Group[275] and their partners and may be communicated to any administrative or judicial authority having the right to transmit.

275 https://www.attijariwafabank.com/fr > accessed on 25 August 2021.

	Duration of third-party access	The general terms and conditions are concluded for an indefinite period. They come into force from when the client signs the account agreement. Wafacash reserves the right to modify the general terms and conditions, add or delete them, better respond to customer satisfaction, and legislative, regulatory, and technical developments.
	Tracking technologies/ website cookies	The use of the functionalities of the www.wafacash.com website may require the setting of cookies. The www.wafacash.com website uses cookies to memorise the preferences chosen by a user when visiting the site and for statistical and audience measurement purposes.

Conclusion

Morocco is one of the countries that has seen a quick expansion of digital platforms in the financial and transaction sector. Our research notes that the context indicates that the country has an adequately organised legal framework with clarity on how these digital services/applications should operate. In fact, since 2007, the Central Bank of Morocco (Bank Al Maghreb – BAM) has been making discernible e orts to improve financial inclusion. In 2014, it developed a new framework (No. 103-12), published in March 2017 (Banking Law).

One of the main conclusions is related to the existence of digital applications that, in their majority, are not initially regulated in Morocco, as foreign companies do their creation. On the other hand, we note the absence of concrete cases. The Data Protection Agency has already acted to safeguard users' rights, even after announcing instances of customer data theft on the Internet in July this year.[276]

276 News report https://www.zdnet.fr/actualites/un-pirate-accuse-de-fraude-bancaire-arrete-au-maroc-39925899.htm > accessed on 25 August 2021.

Mozambique

Country Profile

Maputo is the capital of Mozambique. The country has more than 30 million inhabitants, and Portuguese is the official language.[277] Mozambique is located in Southern Africa, and Eswatini binds it to the south.[278] According to Trading Economics global macro models and analysts ' expectations, by the end of 2021, GDP is expected to reach 14.30 USD Billion.[279]

277 http://www.ine.gov.mz/iv-rgph-2017/mocambique/censo-2017-brochura-dos-resulta-dos-definitivos-do-iv-rgph-nacional.pdf/view > accessed on 15 July 2021.
278 https://www.britannica.com/place/Mozambique > accessed on 17 July 2021.
279 https://tradingeconomics.com/mozambique/gdp > accessed on 17 July 2021.

Data Protection in Mozambique

The preamble to Mozambique's 2004 Constitution, as amended, emphasises the need for pluralism of opinion and the respect and guarantees of fundamental human rights.[280] Article 48 provides for the right to freedom of expression, the press, and the right to access information that shall not be censored. The Inclusive Internet Index 2020[281], which assesses internet availability, affordability, relevance, and readiness, ranks Mozambique 94th out of 100 countries. According to the Index, Mozambique's low scores across the four assessment criteria is linked to low literacy levels, inadequate electricity supply and network infrastructure.[282]

Mozambique is currently ranked 45th out of 61 countries in internet affordability.[283] There is still no specific legislation on data protection and privacy. Guiding principles are provided by the constitution, the civil code and several pieces of sectoral legislation which regulate data protection in specific sectors. In 2020, new amendments[284] to the Mozambican Penal Code[285] were introduced to protect privacy. The Media Institute of Southern Africa (MISA) Mozambique met with the Mozambican government to discuss collaborative cybersecurity

280 https://cdn.accf-francophonie.org/2019/03/mozambique_const-en.pdf > accessed on 19 July 2021.
281 https://theinclusiveinternet.eiu.com/ > accessed on 22 July 2021
282 https://theinclusiveinternet.eiu.com/explore/countries/MZ/?category=affordability > accessed on 24 July 2021.
283 https://a4ai.org/affordability-report/report/2019/#annexes > accessed on 25 July 2021.
284 https://advox.globalvoices.org/2020/01/17/new-privacy-law-in-mozambique-threatens-freedom-of-expression-activists-say/ > accessed on 26 July 2021.
285 https://acjr.org.za/news/mozambique-promulgates-new-penal-code > accessed on 27 July 2021.

and data protection efforts during that period.[286]

On 26 June 2018, Mozambique signed the African Union Convention on Cyber Security and Personal Data Protection[287] ('the AU Convention'). Mozambique has yet to ratify the AU Convention, and this could indicate a general direction for how a data protection framework may develop in the jurisdiction.[288]

Financial System and Fintech in Mozambique

The financial sector in Mozambique is regulated by the Central Bank (Banco de Moçambique).[289]The Law No. 14/2013 of 12 August establishes[290] the legal regime for the prevention and repression of the use of the financial system for the practice of acts of money laundering, goods, products or rights derived from criminal activities defined under that law, and this applies to Money Leading Mobile Applications. Article 17 of the Law states that financial institutions and financial entities covered by the law are obliged to keep identification and transaction documents for 15 years from the date of closure of the accounts of the respective clients or the termination of the contract.

The same law is regulated by Decree 66/2014, 29 October.[291] In its article 2, the Decree stipulates that all financial institutions, banks, or mobile application entities, shall require at least the identification of the customers, which is evidenced by the identity card or an equivalent document in Mozambique. In 2020, Mozambique adopted Law No. 20/2020 of 31 December, which establishes Credit Institutions and Financial Companies.[292] The Electronic Transactions Law (Law No. 03/2017, of 9 January), for instance, provides requirements related to e-commerce.[293]

M-Pesa: The Money Lending Mobile Application

M-Pesa[294] is the largest mobile financial service in Mozambique that allows customers to transfer and withdraw money, buy credit, pay for electricity, and complete transactions for services through mobile phones.[295] Vodafone M-Pesa SA created this service.[296] It was established on 16 January 2013 and is subject to regulation by the Bank of Mozambique. It is unclear how many customers use the application. Recently, M-Pesa launched a service called "Txuna", which will focus on our research. Txuna M-Pesa is a financial service – a

286 Media report https://www.misa.org.mz/index.php/destaques/noticias/85-government-and-misa-mozambique-explore-synergies-for-cyber-security > accessed on 27 July 2021.
287 https://platform.dataguidance.com/legal-research/african-union-convention-cyber-security-and-personal-data-protection-27-june-2014-0 > accessed on 25 July 2021.
288 https://www.dataguidance.com/jurisdiction/mozambique > accessed on 26 July 2021.
289 https://www.salcaldeira.com/index.php/pt/component/docman/cat_view/32-legislacao/77-bancario > accessed on 24 July 2021.
290 http://www.minec.gov.mz/index.php/documentos/legislacao/131-lei-14-2013-lei-de-branqueamento-de-capitais/file > accessed on 24 July 2021.
291 Decree 66/2014, of 29 October https://www.standardbank.co.mz/en/content/download/94383/2328657/file/Decreto%20n%C2%BA66-2014%20-%20Regulamento%20da%20Lei%2014-2014%20-%20Branqueamento%20de%20Capitais.pdf > accessed on 20 July 2021.
292 https://www.salcaldeira.com/index.php/pt/publicacoes/artigoss/doc_download/1205-lei-n-20-2020-de-31-de-dezembro-de-2020-lei-das-instituicoes-de-credito-e-sociedades-financeiras-e-revoga-as-leis-n-15-99-de-1-de-novembro-e-n-9-2004-de-21-de-julho > accessed on 23 July 2021.
293 http://www.oam.org.mz/wp-content/uploads/2017/07/Lei-das-Transac%C3%A7%C3%B5es-eletr%C3%B3nicas.pdf > accessed on 23 July 2021.
294 https://www.vm.co.mz/M-Pesa2 > accessed on 23 July 2021.
295 iOS Download https://apps.apple.com/pt/app/meu-m-pesa-mo%C3%A7ambique/id1442121355 ; Google Play Download https://play.google.com/store/apps/details?id=com.vodafone.mpesa.mozambique&hl=en_US&gl=US > accessed on 20 July 2021.
296 https://www.vm.co.mz/ > accessed on 23 July 2021.

money lending mobile application that allows the customers to borrow money from the Bank and receive mobile money through M-Pesa without needing a bank account. The service is offered to all Vodacom customers who have had an active M-Pesa account for three months.

To request a loan, the customer must access the M-Pesa menu using *150# or choose the "Txuna M-Pesa" option through the App and then follow the steps. Loans can be paid back in 7 days (with 10% service charge), 14 days (with 12% service charge) and 30 days (with 15% service charge). The service works with two Mozambican banks, ABC[297] (African Banking Corporation) and MozaBanco.[298]

Analysis of the lending App

297 https://www.bancabc.co.mz/en/index.html > accessed on 23 July 2021.
298 https://www.mozabanco.co.mz/ > accessed on 23 July 2021.

Txuna M-Pesa[299]	Information Collected and Processed by the App	
	Permissions sought	The terms and conditions (T&C) state that the contract defines the rules and responsibilities between the Client, M-Pesa, MozaBanco and BancABC during the loan term. There is no date of the last update of the terms and conditions with the two banks. By accepting such T&C, the client authorises BancABC to access the data of his Vodacom number and the M-Pesa account to define the eligibility level.
	Information collected from the user	Txuna M-Pesa is committed to collecting essential personal information authorised and limited. They may obtain the client's personal information when: Purchase or acquire a product or service from M-Pesa (including purchasing products online, by telephone or in a Vodacom shop or another establishment). Register for a product or service (including when the client registers their name and address details or create an email address account with Vodacom). Subscribe to newsletters, alerts or other services from Vodacom. Request further information about any product or service, or contact Vodacom with any queries or complaints. Participate in any contest, lottery or survey. Use M-Pesa's products and services. Upon your permission or consent and as permitted by law, we may also collect information from you from other entities or third parties if appropriate and allowed by law. This includes fraud prevention, anti-fraud agencies, business directories, credit reference agencies, and other companies.
	Access and correction of personal information	Under the terms provided by law, the client has the right to access, correct, amend, delete their personal information or refuse to have it processed. Upon receiving the written request, and sufficient information to enable M-Pesa to identify the personal information, they will disclose all information M-Pesa holds about the users. They may charge the client, as permitted by applicable law.

299 Privacy Policy – https://www.vm.co.mz/M-Pesa2/Termos-e-Condicoes/Politica-de-Privacidade > accessed on 4 August 2021. It was interesting to note that on the website M-Pesa has an e-mail to Feedback and Complaints: M-PESA.Privacy@vm.co.mz.

	Information collected from the user's device	The company's information about the users depends on the M-Pesa products and services the clients use and subscribe to. This includes (but is not limited to) the following: The client's name, date of birth, identification document type and number, place of birth and nationality, parentage, marital status and marital regime, address, subscriber account information and email address and nature of income. Client's preferences for particular products, services or activities reported by the client – or when Vodacom assume what they are, depending on how the client use our products and services. Client's communications with M-Pesa – such as any notes or recordings of calls the client has made with one of Vodacom contact centres, email or letter sent to Vodacom, or any other records of contact the client have made with Vodacom. The client's account information includes users' telephone numbers, dates of transfers and payments made or received, or any other related information. Shopping Financial information Contact information Contacts Password Identifiers Usage data Diagnostics
	Information collected from the use of M-Pesa's website	First party cookies originate from the same domain as the website you're currently visiting (in this case, vodafone.com). Third-party cookies originate from a domain different from the website being visited. For example, when clients visit M-Pesa's website, they may link to another company's website – like their Facebook or Twitter account or a video from their YouTube page. So, when the client 'Like' or 'Tweet' an item from M-Pesa's website, these sites may sometimes put cookies on the user's computer. M-Pesa states that they don't control their cookies, so suggest that users check their website to see how they're using them and how to manage them.
	Information received from third parties	Affiliates of the Vodafone Group with a different domain name may also place cookies on their website to show the users adverts or pages of other Vodafone Group companies that may be of interest to you. Details of these affiliates – and how to opt-out – are included on the website.

	Use of user's information by the App	Financial information ID – personal documents (passport or local document) Contacts
	Information shared with third parties	Financial information ID (the Bank obliges customers to provide a copy of their documents) Information may be shared with: Vodacom group companies (Vodafone Group Plc and any other company in which Vodafone Group Plc owns more than 15% of the share capital) Partners or agents involved in providing services you have requested or used Partners or agents who conduct customer satisfaction surveys on products and services provided to you Companies engaged in the provision of services on behalf of Vodacom (Pty) Ltd, including Vodafone Limited or other Vodafone Group companies Where applicable, credit reference agencies, fraud prevention, business assessment agencies, or other credit assessment agencies. Debt collection companies or other debt recovery companies If required or permitted by law, law and order authorities, regulators, courts, or other public authorities. Emergency services (if the client make an emergency call) The company discloses information within the limits of what is reasonable for the protection against fraud, to defend the rights or property of M-Pesa or to protect the interests of our customers. If Vodafone M-Pesa is reorganised or acquired by another company or group, we may transfer any personal information we hold about you to that company or group.
	Duration of third-party access	It is not clear how this data is used and the durability of use in case of termination of the contract between the Bank, M-Pesa Txuna and the client.
	Tracking technologies/ website cookies	M-Pesa Txuna states that their cookies don't hold personal information such as the name. M-Pesa lets the users find information once they are logged in or help link their browsing information to their data when the clients choose to register for a service, white paper or newsletter.
	Storage of user information by the App	Financial information Contact information

Loans can start from 70 Meticais (MT) to 3,500 MT (approximately $1 – $60). The amounts can change according to the client's eligibility level and historical records. Bank ABC's terms and conditions are written[300] in an unprofessional style. It does not appear to be a contract document between two entities. The document defines what is meant by customer data,

300 http://www.vm.co.mz/content/download/106232/706643/version/1/file/Termos+e+Condicoes+Txuna+M-Pesa+BancABC.pdf > accessed on 23 July 2021.

which is the information provided by M-Pesa to the Bank and NANO (Global Holdings Limited) to enable Customer profiling and the provision of this service.

The same document states that NANO is the technology company that provides the technical platform to profile Customers' eligibility to use the service. It is said that if the terms and conditions are accepted, the customer: a) confirms that all information (including any documents) provided to Vodafone M-Pesa SA is correct, complete, and not misleading; and b) authorises Vodafone M-Pesa SA to disclose, verify and exchange any of identity and transaction information with the financial institution responsible for providing the loan service and third parties providing technical infrastructure and regulatory authorities.

We note that between the two banks, ABC and MozaBanco, there is some difference in how the terms and conditions are explained. For example, MozaBanco[301] uses a different data management system, FICO, a partner company/entity that deals with credit/financial services, analysis, criteria and associated services. However, the authorisation system for personal data/information is the same between the two banks.

We also noted that the Frequently Asked Questions – Q&A document[302] available on the website did not clarify when its last update was made. The same document does not mention anything on data protection or the use of information. The questions that are asked primarily benefit the money lending mobile application to promote its service and not necessarily the customers. However, one of the positive aspects we could find is that M-Pesa publishes[303] its annual financial reports, and the last one was in December 2020. On 7 March 2019, We found that Vodafone M-Pesa, S.A. was fined[304] an amount of MT 10 million (approximately $157,240) by the Central Bank of Mozambique, following a violation of the anti-money laundering regulations – article 77 of Law 14/2013. The offence was due to a system limitation that has now been resolved. It is unclear[305] what the system error was. Still, it is understood that it was a breach that left user data vulnerable to third parties who could have access to personal data and commit financial fraud through the application.

Case Study: Two M-Pesa Users

Gilberto Manhiça[306] has been using M-Pesa since 2017. First, he gave his data (identification/personal ID) to the mobile phone company when he registered his account and updated his personal information to increase the amount allowed on the account. Regarding data privacy, he notes that Txuna became secure in 2020 when M-Pesa changed the rules to hide the customer's name during the transfer process. As a Txuna customer, he is not clear about the security of his data. Still, even if he knew about his data, he does not doubt that

301 http://www.vm.co.mz/content/download/106233/706647/version/1/file/Termos+e+Condicoes+Txuna+M-Pesa+Moza+Banco.pdf > accessed on 25 July 2021.
302 http://www.vm.co.mz/content/download/106095/705913/version/1/file/Perguntas+Frequentes+Txuna+M-Pesa.pdf > accessed on 24 July 2021.
303 https://www.vm.co.mz/M-Pesa2/Relatorios-Financeiros > accessed on 24 July 2021.
304 Report http://www.vm.co.mz/content/download/103501/690546/version/1/file/M-Pesa+-+Relat%C3%B3rio+Disciplina+de+Mercado_Junho_2019.pdf > accessed on 24 July 2021.
305 http://www.vm.co.mz/content/download/103501/690546/version/1/file/M-Pesa+-+Relat%C3%B3rio+Disciplina+de+Mercado_Junho_2019.pdf > accessed on 24 July 2021.
306 Interview 22 July 2021, Maputo (Mozambique, via zoom).

if the justice entities (police) want his information, they will always have access to it from the mobile phone company. Gilberto has never read the terms and conditions but remembers a contract with ABC Bank that allows Vodacom and Txuna M-Pesa to share his data with the Bank. He considers some security but noted that he "trusts the bank, more than Vodacom."

We also talked to Justino Mabuiango[307], who started using M-Pesa in 2016. For him, the M-Pesa application is safe because his "data is not exposed to anyone". Like Gilberto, he mentioned that the substantial change happened in 2020 when M-Pesa adopted a system that, in case of transfer, the application only shows the client's initials. The client said he does not use Txuna regularly because it "is not good to have debts." Everything he knows about personal data was due to his own experience as a user and noted that he never read any document to join the service there is a security guarantee.

Conclusion

The M-Pesa Txuna application reveals that although the service has been in Mozambique for more than five years, its expansion to other banks is still limited when we consider that Mozambique has more than ten commercial banks. It only works with two banks may raise some questions that need further analysis. In addition, despite making available the terms and conditions of use of the platform, the lack of update of these documents remains an unanswered question. The privacy policy is not published visibly to customers, which makes there are cases of omission, as was found throughout the interviews where a user mentioned using the service without ever having read any document before. In conclusion, there is some omission on how M-Pesa works with the Central Bank to request customer personal data.

307 Interview 27 July 2021, Maputo (Mozambique, via zoom).

Namibia

Country Profile

Located on the southwestern coast of Africa, Namibia shares a border with Angola to the north and South Africa to the south. After 106 years of German and South African rule, Namibia became independent on March 21, 1990, under a democratic multiparty constitution.[308] The capital of the country is Windhoek. It has an estimated population of around 2 million people[309] with an estimated GDP of 10.56 billion as of 2020.[310]

308 https://www.britannica.com/place/Namibia > accessed on 6 September 2021.
309 https://www.worldometers.info/world-population/namibia-population/ > accessed on 5 September 2021.
310 https://www.statista.com/statistics/510122/gross-domestic-product-gdp-in-namibia/ > accessed on 5 September 2021.

Data Protection in Namibia

Namibia has not enacted data privacy legislation.[311] The country recognises privacy as a fundamental human right under Article 13 of the Namibian Constitution.[312] It states that no persons shall be subject to interference with the privacy of their homes, correspondence, or communications. The law makes an exception for interference under the statute, in the interests of national security, public safety or the country's economic well-being, for the protection of health or morals, for the prevention of disorder or crime, or the protection of the rights or freedoms of others.

Namibia has ratified the International Covenant on Civil and Political Rights ('ICCPR').[313] This reinforces Article 12 of the UDHR, which provides that "no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation".

Financial System and Fintech in Namibia

The legal framework for the National Payment System was derived from the Payment System Management Act, 2003 (Act No.18 of 2003)[314] and the bylaws issued under the

311 https://www.dlapiperdataprotection.com/index.html?t=law&c=NA > accessed on 6 September 2021.
312 http://www.kas.de/upload/auslandshomepages/namibia/constitution/const_en_contents.pdf > accessed on 5 September 2021.
313 https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx > accessed on 5 September 2021.
314 https://www.bon.com.na/Bank/Payments-and-Settlements/Legal-Framework/Payment-System-Management-Act.aspx > accessed on 3 September 2021.

Payment System Management Act, as amended.[315] Bank of Namibia has five Authorised Electronic Money Issuers: Magnet Payment Solutions; Nam-mic Payment Solutions; NamPost; Virtual Technology Services, and Vivo Energy Namibia.[316]

In February 2021, it was reported[317] that in 2020 alone, over N$40 billion[318] was moved through e-money platforms such as eWallet, easyWallet and Blue Wallet and other similar banking services. A year before 2019, this value was just N$14,8 billion[319], which has grown by 177%, more than the growth in value pushed by bank cards and electronic transfers.

Last April, the Bank of Namibia (BON) called on the banking sector to consider financial technology to improve access and financial inclusion.[320] In its annual report,[321] the central bank said the more options to access banking products and services, and the more clients would be reached. It is reported that Namibia still has many individuals and businesses not registered with banks and prefer to transact cash.

Mobile transactions have also increased dramatically, from less than 10 million in 2015 to over 65 million in 2020.[322] The BON also launched the Namibia National Payment System Vision and Strategy 2021-2025, which includes plans on making cross-platform payments more user-friendly.[323]

In addition to that, the Bank of Namibia (BON) is on course to complete its study[324] into cryptocurrencies by April 2022, the central bank governor, Johannes Gawaxab, recently confirmed.[325] However, the governor reiterated that cryptocurrencies are not legal tender as there is currently no provision for digital currency use in the country's laws.

PayToday: The Money Lending Mobile Application

PayToday[326] is a Namibian mobile money application that makes payments and loans through bank accounts for individuals and businesses. The customers must download the PayToday App from the Apple App Store or Google Play Store and complete the registration process to use the application. The clients must submit their card and bank details as part of the registration process. Their card details are used to make payments.
First, the application was launched as StayToday, by Chris (Chartered Accountant) and Naude (Electric/Electronic Engineer) in 2013.[327] In 2017 it was introduced in Namibia. The

315 https://www.bon.com.na/Bank/Payments-and-Settlements/Legal-Framework/Payment-System-Management-Amended-Act.aspx > accessed on 3 September 2021.
316 E-Money Institutions https://www.bon.com.na/Bank/Payments-and-Settlements/E-Money-Institutions.aspx > accessed on 6 September 2021.
317 News report https://allafrica.com/stories/202102240567.html > accessed on 3 September 2021.
318 Approx. $ 2 800 581 200
319 Approx. $ 1 050 217 950
320 News report https://afcacia.com/2021/04/17/namibian-banks-urged-to-embrace-fintech/ > accessed on 3 September 2021.
321 https://www.bon.com.na/getattachment/7923760d-1805-4265-906a-b424abafdef8/.aspx > accessed on 3 September 2021.
322 Idem.
323 https://www.bon.com.na/getattachment/2183fe04-8b8f-44d0-add9-4629d7ec86a5/19-02-2021-Namibia-National-Payment-System-Vision.aspx > accessed on 3 September 2021.
324 Namibia Cryptocurrency Laws https://freemanlaw.com/cryptocurrency-blockchain/namibia/ > accessed on 6 September 2021
325 News report https://news.bitcoin.com/namibia-central-bank-to-complete-crypto-study-by-april-2022-governor-says-current-laws-do-not-permit-use-of-digital-assets/ > accessed on 4 September 2021.
326 https://site.paytoday.com.na > accessed on 4 September 2021.
327 https://www.offerzen.com/companies/paytoday > accessed on 4 September 2021.

solution is made possible through a partnership with Nedbank Namibia. Most debit or credit cards from any Namibian Bank can be used to pay for fuel on PayToday.[328]

Analysis of the lending App

PayToday[329]	Information Collected and Processed by the App	
	Permissions sought	The App allows three different types of Privacy settings and permissions[330]: Participants only (Strict privacy setting): Only the people users request money from or send money to will be aware of the transaction. Friends only (Moderate privacy setting): Transactions will only be shared with users' friends. All clients' contacts in their phone book define users' friends' friends. Everyone (Lenient privacy setting): Transactions (peer to peer and purchases) will be shared on the Namibian and Friends Feed and visible to everyone.
	Information collected from the user	Name; Phone number; E-mail address; Credit/Debit card number and expiration date; Bank Details; ID numbers; Login names; Passwords; Device information;
	Access and correction of personal information	Read the contents of clients' USB storage Modify or delete the contents of clients' USB storage All clients' personal information which the App collect and maintain can be viewed and edited by users at any given time.
	Information collected from the user's device	Location information (only once the client has explicitly provided the authorisation); Clients' contact details in your phone book (only once the client has explicitly provided the authorisation) PayToday matches contacts data to the registered user database to transact with other registered users. Their contact data is stored on the App in an internal database for caching but not on the back end server. All information related to each transaction (the message content, the time, date, recipient and amount for each transaction); Non-Personal Identifiable Information ("NPPI") – this is information that may correspond to a particular person or account but, on its own, is not sufficient to identify, contact or locate a specific person.

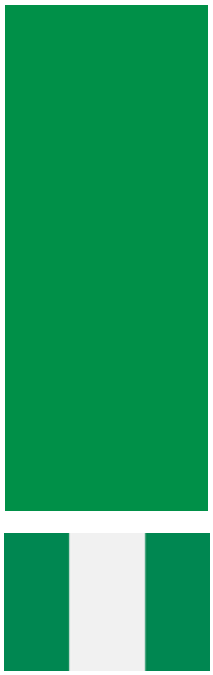
328 https://www.namibian.com.na/169678/archive-read/PayToday-introduces-mobile-fuel-payments > accessed on 4 September 2021.
329 Frequent Asked Questions https://site.paytoday.com.na/need-help/#FAQs > accessed on 4 September 2021.
330 https://www.today.com.na/paytoday-privacy-policy > accessed on 3 September 2021.

	Information collected from the use of PayToday's website	When the user's login to the PayToday App or access the Today website, they may transfer small data files called "cookies" to their computer or login device. Today websites use these "cookies" to improve users' experience, and the users are free to decline these "cookies".
	Information received from third parties	No information
	Use of user's information by the App	PayToday or related entities or their respective assets could be acquired by another business entity or merged into such an entity. Should such a merger or acquisition occur, the client should expect PayToday to share some or all users' personally identifiable information.
	Information shared with third parties	As part of sending and requesting money from other Pay-Today users, the following personal information will be shared with the other users that the clients transact with: details of the transaction (amount, time, date, other participants, client profile picture and username).

Conclusion

It seems that the application details the necessary information to the users on its website. However, the absence of a data protection law does not allow a consistent analysis that guarantees personal data protection. For example, in the policy privacy terms, there is no mention of the intervention of regulatory bodies for cases where App holders violate the privacy rights of their customers. We also note that it does not mention the relationship between the App and its partners (commercial banks) in sharing information with third parties. The explanation is vague and only focuses on the App itself and not on other entities.

Nigeria



Country Profile

Located in West Africa,[331] Nigeria, also known as the Federal Republic of Nigeria, shares a border with Niger, Chad, Cameroon, and the Gulf of Guinea.[332] It covers an area of 923,768 km2[333] with a climate ranging from arid to humid equatorial.[334] It has diverse ethnic groups of around 250, with Hausa, Igbo, and Yoruba being the most popular languages.[335] Nigeria is the most populated country in Africa, with over 211 million people.[336] Its capital city is Abuja though Lagos remains the largest city with economic activities.[337]

331 Nigeria https://www.nationsonline.org/oneworld/nigeria.htm
332 Nigeria https://www.britannica.com/place/Nigeria
333 (n1)
334 (n2)
335 13 Things you Need to Know About Nigeria https://artsandculture.google.com/story/13-things-you-need-to-know-about-nigeria/_AJCyGgURLk8KA
336 World Population Dashboard Nigeria https://www.unfpa.org/data/world-population/NG
337 (n1)

Data Protection in Nigeria

The use of digital lending apps in Nigeria has been chiefly resorted to by individuals and SMEs due to their simplified and fast lending process, unlike banks where obtaining a loan has proven to be arduous.[338] These apps have increased their use, particularly in the advent of the coronavirus pandemic, which significantly impacted the global economy.[339] Unlike banks, these apps provide a convenient way of accessing loans within a short period without requiring security. However, they rely strongly on a user's data to assess the credit risk.

The entities that own these apps must be registered and obtain a licence from the Central Bank of Nigeria (CBN) under the Banks and Other Financial Institutions Act 2020 (BOFIA).[340] The Act places these apps under the supervision of the CBN and classifies them as "businesses of other financial institutions", which include financial businesses conducted

338 The Intrusiveness of Mobile Lending Apps in Nigeria https://aanoip.org/the-intrusiveness-of-money-lending-apps-in-nigeria/
339 Ibid
340 Section 57 (1), Banks and Other Financial Institutions Act 2020 (BOFIA) https://www.cbn.gov.ng/Out/2021/CCD/BOFIA%202020.pdf

digitally, virtually, or electronically.[341] It is worth noting that these entities (lenders) also can register themselves within the laws of the Nigerian states. However, this option can limit the lender's activities. This limitation is because the lender will only be allowed to operate within the confines of the state where registration has taken place. They will also be limited in terms of interest rates they can charge.[342]

The data processing activities of these apps are governed by the Nigeria Data Protection Regulations (NDPR), which require these apps to safeguard users' right to privacy.[343] The Regulations lay out a framework that data controllers should follow to ensure the security of data subjects' data (in this case, borrowers).

This study focuses on examining the compliance of these apps with the provisions of the NDPR. It begins by assessing the data collected by these apps and subsequently analysing whether such processing complies with the NDPR.

Overview of Data Collected by The Digital Lending Apps in this Study

341 Section 57 (2)(j)(ix), Banks and Other Financial Institutions Act, 2020
342 ICLG, Nigeria Fintech Law Regulation 2021 https://iclg.com/practice-areas/fintech-laws-and-regulations/nigeria
343 Nigeria Data Protection Regulation 2019 https://ndpr.nitda.gov.ng/Content/Doc/NigeriaDataProtectionRegulation.pdf

Carbon[344]	Information Collected and Processed by the App	
	Permissions sought	Seeks permission to access: SMSs Contacts Installed applications Browser history Calendar Location- Precise location information The App may also collect this information in the background when the user is not using it.
	Information collected from the user	User information requested; name, address, email address, phone number, social media login information, financial/ credit card information, personal description, current and previous employment, education, names of colleagues, contacts and friends, photographs, and list of family members
	Information collected from the user's device/ Use of the website	Technical information: IP address, login information, type of browser and version, time zone setting, plug-in types of browsers and versions, operating system and platform User's visit: URL links when navigating the site; products viewed or searched; page response times, download errors, length of visits to site pages, page interaction information (scrolling, clicks, mouse movers); methods used to browse; phone number used to call customer service number Repayment data
	How is user info collected	When filling forms in the site (i.e., registration and loan application in the App) When granting access to social media platforms Through correspondence i.e., email, phone e.t.c.,
	Information received from third parties	Receives information from: Other websites operated by Carbon, used by the user Social media platforms logged in via Carbon by a user Third parties such as; business contractors, sub-contractors, payment and delivery services, social media sites, advertising networks, credit bureaus, credit providers, among others
	Use of user's information by the App	Performance of contractual obligations with the user Credit rating Provision of information about Carbon's goods and services Marketing Notification of changes on Carbon's services Further processing for scientific, statistic or historical research purposes in line with the public interest,

344 Carbon Policy https://getcarbon.co.ke/privacy-policy.html

	Information shared with third parties/ Disclosure of Information	Shares information with the following third parties: Its Subsidiaries, holding company Business partners, suppliers and subcontractors Advertisers and advertising networks Analytics and search engine providers Other parties comply with a legal obligation or enforce its terms of use. Receives user information from: Switching companies Mobile network providers Electricity companies Aggregators Credit reference bureaus eCommerce platforms, and Other financial institutions
	Duration of third party access	Not indicated
	Tracking technologies/ website cookies	Users consent to the placement of cookies in their browsers and HTML based emails upon visiting the site
	International data transfers	Data may be transferred/ shared between countries in which Carbon operates
	Storage of user information by the App	Stores data on its servers using JWT

PalmCredit[345]	Information Collected and Processed by the App	
	Permissions sought	Seeks permission to access: Contact list Call logs SMS logs Facebook contacts Contact lists from other social media accounts Photos, videos or other digital content The App calls contacts from a user's contact list, SMSs, or call list to verify the identity of the user
	Information collected from the user	Personal data: name, age, email address, phone number, physical contact info, personal description, photograph, username, password, financial information-credit card, bank account numbers Transactional data: user's activities on the App Correspondence: data collected through correspondence with the user Additional information for verification purposes
	Information collected from the user's device	Device ID Device type Unique device identifiers; geo-location information, computer, operating system, and connection information IP address Standard web log information

345 PalmCredit Privacy Policy http://web.palmcredit.loans/policy.html

	How is user information collected	Filling in forms on the App Corresponding with PalmCredit Registering to use the App Subscribing to PalmCredit services Sharing data via the Apps social media functions Promotion, competition or survey Reporting issues to do with the App
	Information received from third parties	Demographic and navigation data, Credit check information, and Information from a credit bureau
	Use of user's information by the App	Calculation of credit limit Provision of access to Carbon App Resolution of disputes Prevention of crime and enforcement of the Apps terms and conditions Customisation of content, advertisement, and services Provision of information about the Apps services Targeted marketing Verification with third parties Contacting user
	Information shared with third parties Duration of third party access	-The App discloses user information to: Its business partners during mergers and acquisitions Its business partners when selling or buying a business or assets Law enforcement and governmental agencies Its subsidiaries, holding companies, e.t.c., Third parties when enforcing its terms and conditions or publishing the Apps usage statistics Credit reference bureaus Third parties when complying with legal or regulatory orders or enforcing its policies Not indicated
	Tracking technologies/ website cookies	The App has: Session cookies that are deleted from a user's hard drive once a user is done with a session on the App Third-party cookies that are mainly from its service providers Cookies from third parties (not belonging to the App) that a user encounters when visiting a different web page on the App

	International data transfers/ Cross border data transfer	Where user data is to be transferred to a country that is not White-Listed, the App will only transfer data under the following circumstances: Where user's consent has been obtained Where a transfer is required for the performance of a contract between the user and the App Where a transfer is required for the conclusion of a contract between the App and a third party in the interest of the user Where a transfer is necessary for public interest Where a transfer is required for the establishment or defence of legal claims
	Storage of user information by the App	User data may be stored or transferred outside Nigeria. It may also be handled by staff operating outside Nigeria

Branch	Information Collected and Processed by the App	
	Permissions sought	
	Information collected from the user	Name, date of birth, phone number, email address, nationality, tax identity (ID) number, bank details, bank verification number, ID number, location, photograph, IP address, MAC address, IMEI number, IMSI number.[346]
	Information collected from the user's device	
	How Branch collects the information	Through in-app forms during application for a loan Through the user's device Through correspondence with user's, i.e., emails
	Information received from third parties	
	Use of user's information	Credit risk assessment Conduction of due diligence Compliance with Regulations Marketing purposes
	Information shared with third parties Duration of third party access	
	Tracking technologies/ website cookies	
	International data transfers	

346 Branch Data Protection Policy, pg 5 https://branch.co/documents/BranchDataProtectionPolicy-NG.pdf

	Storage of user information by the App	

Quick-Check[347]	Information Collected and Processed by the App	
	Permissions sought	
	Information collected from the user How information is collected from users	Name, address (including past address), email, phone number, social media information, financial information, personal status information, employment information, level of education details, family contacts and knowledge, applications, messages, IP address, type of browser.[348] When filling in forms in the App/ site When granting access to social media accounts Through correspondence, i.e., through phone or email Through comments made by users on the site
	Information collected from the user's device	
	Information received from third parties	
	Use of user's information by the App	Personalisation of content Provision of products and services Credit scoring Notification of changes in products and services Correspondence, i.e., through email or phone
	Retention of user's data	Indefinite retention of user comments on the site "Users can see, edit or delete their data at any time". However, "they cannot change their username".
	Information shared with third parties Duration of third party access	
	Tracking technologies/ website cookies	Type of cookies: Temporary cookie- determines the acceptance of cookies by the user's browser during login Login cookies- Save user's login information Cookies are saved in users browsers when they publish or edit articles on the site -Cookies are used for tracking purposes.
	International data transfers	

347 QuickCheck Privacy Policy https://quickcheck.ng/privacy-policy/
348 QuickCheck Privacy Policy-'What Personal Data we Collect' Clause

	Storage of user information by the App	"User personal information is contained behind secured networks and is only accessible by a limited number of persons who have special access rights to such systems and are required to keep the information confidential. In addition, all sensitive/credit information users supply is encrypted via Secure Socket Layer (SSL) technology...All transactions are processed through a gateway provider and are not stored or processed on our servers."[349]

Aella credit[350]	Information Collected and Processed by the App	
	Permissions sought	
	Information collected from the user	Name, address, email address, phone number, IMEI, SIM card details, age, username, password, financial and credit information (including user's mobile money account details, bank account details, bank verification number), personal description and photograph[351]
	Information collected from the user's device/ Use of the website	Technical information: type of mobile device, unique identifiers (IMEI or serial number), SIM card use, mobile network, operating system, type of browser, device location and time zone setting, information stored on a device (contacts, call logs, SMSs, photos, video or other digital content), third party App use information on a device, details of the use of aella App (including traffic and location data, login information).[352] Location information through GPS technology
	Information received from third parties	Receives information from: Credit reference bureaus Mobile network providers
	Use of user's information	Account opening Compliance with Know Your Customer (KYC) requirements Assessment of user's creditworthiness
	How user information is collected	Filling in forms during loan application on the App or the site Correspondence with aella credit Registration for the use of the aella site The download of the App Subscription to aella services During a search of an App or service Logging in/ sharing information through aella credit's social media functions Joining App's competitions During promotions or surveys When submitting complaints regarding the App, services or site

349 QuickCheck Privacy Policy- 'How we protect your data' Clause
350 Aella credit Privacy Policy https://aellaapp.com/privacy-policy
351 Aella credit Privacy Policy- 'Required Information" Clause https://aellaapp.com/privacy-policy
352 Aella Credit Privacy Policy- Clause 3.2 Collected Information

	Information shared with third parties/ Disclosure of Information	Aella credit shares information with: Service providers Business affiliates, i.e., its parent company, subsidiaries, e.t.c., Companies contracted by them to market their products Other companies during mergers, acquisitions, sale of assets, liquidation or bankruptcy proceedings Authorities for purposes of preventing harm Relevant bodies in compliance with court orders, or for purposes of defending legal claims, or complying with the law Credit reference bureaus when reporting defaulters or for publishing statistics on usage of the App
	Duration of third party access	Not indicated
	Tracking technologies/ website cookies	Uses cookies and tracking technologies
	International data transfers	
	Storage of user information by the App	User data may be stored and transferred outside Nigeria and processed by staff operating outside Nigeria.

Analysis of the Data Protection Practices of the Apps

Purpose Limitation

The lending apps are required under the Nigeria Data Protection Regulations (NDPR) to process personal data for specific, legitimate, and lawful purposes subject to a data subject's consent.[353] The Regulations also state that further processing of personal data by these apps should only be done for archiving, scientific research, historical research, or statistical purposes for the interest of the public.[354]

The Apps understudy, as illustrated above, indicate the purpose of collection of personal data, which includes, among others, provision of services (i.e., loans), credit scoring, and marketing. However, the question is whether the data collected is relevant concerning the purpose of data collection. A study of the apps' privacy policies (as shown above) indicates that they are excessive and contrary to the purpose of digital lending. This includes data stored in a user's device such as contact list, call logs, photos, and videos; social media information (including login information) and social media contacts; personal user description; financial and credit information; colleagues; and list of family members. The collection of this kind of information is intrusive and violates the right to privacy of a data subject.

353 Rule 2.1. (1) (a) NDPR
354 Rule 2.1 (1) (a) (i) NDPR

This kind of information is not required for digital lending purposes, and the apps should only stick to the collection of personal data necessary for lending.

Data Retention

The NDPR requires these apps to expressly indicate how long they will store their data and the criteria used to determine that period.[355] The Regulations further state that these apps should only store users personal data for the period within which it is needed.[356]
The apps understudy fail to comply with this principle. Some Apps allow deletion of data after the data has been used for its stated purpose. However, they still put a disclaimer to it contrary to the principle of deletion. Carbon app, for example, states that personal data shall be deleted after its purpose, i.e., lending, has been achieved.[357] It, however, says that despite the deletion of data, such data shall still be kept in their backup or archival media for legal, tax, or regulatory purposes.[358] This ultimately means that Carbon will still have a user's data despite deletion and the achievement of its goal. It is also worth noting that Carbon does not indicate the criteria used to determine the period for data retention.[359]
Palm Credit, on the other hand, goes the extra mile to show the criteria used to determine the period of data retention.[360] However, the App's privacy policy indicates that even if a user uninstalls the App, the App may still retain the user's data in an aggregated and anonymised form.[361] The policy also states that the App may still keep a user's data for purposes of complying with legal obligations and resolving or litigating disputes, and enforcing its agreements.[362] These read together indicates that the data will not be deleted and will still be in the App's possession.

The Branch App does not have a clause on data retention. QuickCheck, on the other hand, allows users to see, edit or delete their data except for their usernames.[363] Aella app indicates that users' data shall not be kept in a form that identifies them longer than is necessary for data collection.[364]

Data Security

The NDPR lays out elaborate measures that these apps should follow to ensure personal user data security. It states that these apps should protect private user data against all foreseeable hazards and breaches such as theft, cyberattack, viral attack, dissemination, manipulation, or damage.[365] In doing this, the NDPR requires these apps to employ security measures such as; protecting the system from hackers, setting up firewalls, storing data securely with access to specifically authorised individuals, utilising data encryption technologies, developing organisational policy for handling personal data, protecting

355 Rule 2.13.6 (g), NDPR
356 Rule 2.1. (1) (c) , NDPR
357 Carbon app Privacy Policy; Data Retention Clause
358 Carbon App Privacy Policy: Data Retention Clause
359 Ibid
360 Palm Credit Privacy Policy: Data Retention Clause
361 Palm Credit Privacy Policy: Data Retention Clause
362 Palm Credit Privacy Policy: Data Retention Clause
363 QuickCheck Privacy Policy: Data Retention Clause
364 Aella App Privacy Policy: Clause 1.4
365 Rule 2.1 (1) (d) NDPR

emailing systems, and building capacity for staff.[366]

These measures are essential given the intensity of the data collected by these lending apps. However, some measures concerning the security of data by these apps raise a lot of concern. Carbon and Palm Credit, for example, do not guarantee users the protection of the data they transmit to the App, i.e., passwords during login activities.[367] They indicate that such transmission is at the user's risk.[368] This is very unfortunate for a user who urgently needs the services of the App. The apps in line with the NDPR are required under such circumstances to use encryption technology to protect personal user data transmitted to the App during activities such as logins. The only apps that employ encryption technology are Branch and QuickCheck.[369]

The apps have put some degree of security; however, some have comprehensive security measures compared to the rest. These include; Branch and QuickCheck.

Data Subject's Consent

These apps are required under the NDPR to ensure that their processing activities are lawful. The apps must only process personal data subject to a data subject's consent and for a specific purpose in providing lawfulness.[370] The NDPR further obliges these apps to inform data subjects of the intention of data collection to ensure that the data subject consents from an informed perspective.[371]

This author believes that the apps do not allow users to give their consent freely. This is because the apps' services are pegged on a user's consent, and if the user objects to the processing of their data, the apps deny them access to the services.
Secondly, the NDPR states that when assessing whether consent has been freely given, consideration shall be given to whether the provision of a service is conditional on consent to the processing of personal data that is not necessary or (excessive) for the performance of the contract.[372]

In this case, access to lending services from the apps is pegged on the apps access to unnecessary and invasive data that violate the users' privacy. The apps require access to unnecessary data for lending purposes, such as social media information, user's contact list and list of family members, SMS, user's photos and videos, among others, that invade a user's privacy.

Publicity and Clarity of Privacy Policy

Under Rule 2.5 of the NDPR, any medium that processes personal data is required to

366 Rule 2.6 NDPR
367 Carbon and Palm Credit Privacy Policy: Security Clauses
368 Ibid
369 Branch and QuickCheck Security Clauses.
370 Rule 2.2 (a) NDPR
371 Rule 2.3 NDPR
372 Rule 2.3 (2) (d) NDPR

display a conspicuous and straightforward privacy policy that the class of data subjects targeted can understand. The Privacy Policy should contain:[373]
What constitutes the data subject's consent
Description of collectable personal information
Purpose of collection of personal data
Technical methods used to collect and store personal information and cookies
Access of third parties to the personal data and the purpose of access
A highlight of the principles of data protection
Available remedies in instances of breach
Timeframe for remedy
Branch lacks this. Its policy is not as detailed as required under this rule.
Third-Party Data Processing
The NDPR requires data processing by third parties to be governed by a written contract between the third party and the Data Controller.[374] It also states that data controllers engaging third parties in processing personal data of data subjects should ensure adherence to the NDPR.[375]

None of the apps understudied entered into contracts with the third parties they shared user information. Some of them, particularly QuickCheck and Branch, do not show the third parties they share this information with. What's more concerning is that these apps do not show the steps they will take to ensure that the third parties they share user information comply with the NDPR.

Transfer to a Foreign Country

The NDPR lays out critical issues that should be considered concerning the transfer of data to a foreign country. It states that such transfer should take place subject to the provisions of the NDPR and the supervision of the Honourable Attorney General of the Federation (HAGF).[376] The critical issue to be considered is that the foreign country should have an adequate level of data protection.[377] The HAGF should assess the foreign country's legal system concerning the rule of law and protection of human rights, among others.[378]

The NDPR also provides an exception to this.[379] It states that personal data shall be transferred to a foreign country; if the data subject has consented to it[380], where the transfer is necessary for the performance of a contract between the data subject and the controller[381] The data subject should be informed of the appropriate data protection safeguards in the foreign country. [382]

373 Rule 2.5 NDPR
374 Rule 2.7 NDPR
375 Ibid.
376 Rule 2.11 NDPR
377 Rule 2.11 (a) NDPR
378 Rule 2.11 (b) NDPR
379 Rule 2.12 NDPR
380 Rule 2.12 (a) NDPR
381 Rule 2.12 (b) NDPR
382 Rule 3.1 (8) NDPR

Rights of a Data Subject

The NDPR accords data subjects rights concerning the processing of their data.[383] It indicates that before the processing of the personal data of a data subject, the data controller should inform the data subject of the identity and contact details of the data controller, the contact details of the Data Protection Officer, the purpose of processing, the legitimate interest pursued by the controller, the recipients of the personal data, intention to transfer data to a third country, the period which the personal data will be stored and criteria for determining such period, data subject's right to request access, rectification or erasure of personal data, data subject's right to withdraw consent, the existence of automated decision making and profiling, information on the purpose of further processing, and information on the transfer of personal data to a foreign country.

Some of the apps understudies, such as Aella App, QuickCheck, and Carbon, do not provide the contact details of the Data Protection Officer, nor do they indicate whether the organisations have Data Protection Officers. Branch and Palm Credit are the only apps with Data Protection Officers. As discussed in the previous section, the apps indicate the purpose of data processing; however, the data processed is contrary to lending.
Some of the apps understudied inform users of the recipients of their data, and some do not. The apps also indicate their intention of transferring personal data to foreign countries but do not indicate the safeguard measures to protect data in the foreign countries. The only App that gives users room the right to request access, rectification and deletion of data is Palm Credit. The rest tend to limit this. For example, Branch only gives users the right to request rectification where information is inaccurate, and Carbon only offers users the right to object to the processing of their data for marketing purposes.
Only two apps enable users to exercise their right to data portability, i.e. Quick Check and Palm Credit.[384]

Public Shaming

Digital lending apps in Nigeria have also been notorious for public shaming.[385] The apps contain clauses in their privacy policies that give them the right to contact a user's contacts regarding the user's default in payment.[386] Some apps go as far as posting the defaulting borrowers on social media and portraying them as criminals.[387] All this is done to make the borrower pay the debt. However, such acts violate the borrower's privacy and defame their character.

The most notorious apps known for this practice include OKash, Soko Loan, LCredit, Credit9ja, and Fast Money.[388] In their privacy policies, these apps expressly indicate that they can use a user's contacts if the user defaults in payment. Such provisions are

383 Rule 3.1. (7) NDPR
384 Quick Check Privacy Policy: Rights of a User Clause Palm Credit Privacy Policy: Rights of a User Clause
385 https://twitter.com/EthanZ/status/1429845838751207432?s=19
386 The Intrusiveness of Money Lending Apps in Nigeria https://aanoip.org/the-intrusiveness-of-money-lending-apps-in-nigeria/
387 Violation of Digital Rights in Nigeria https://www.change.org/p/central-bank-of-nigeria-violation-of-digital-rights-of-nigerians
388 Violation of Digital Rights In Nigeria https://www.change.org/p/central-bank-of-nigeria-violation-of-digital-rights-of-nigerians

contrary to the NDPR, which prohibits unlawful processing of personal data.[389] The National Information Development Agency (NITDA) should take action on these practices and ensure that these apps process personal data fairly and legally. The Agency recently sanctioned Soko Loan for invading the privacy of borrowers after receiving complaints regarding its unwarranted disclosure of user information, failure to protect users personal information, and defamation of users.[390]

Privacy by Default or Design

The apps should be technically designed to limit them to collecting information that is necessary for lending purposes. The technical design of the apps should not allow them access to users' confidential data on their devices, such as photos, video, contact lists, SMS, and social media information. The App designers should design it in such a way that respects user privacy.

Conclusion

The apps under study can be said not to comply with the NDPR. The apps process a lot of personal data from data subjects that go against digital lending. The collection of such an amount of data is intrusive and violates the right to privacy of data subjects. The apps should strictly comply with the NDPR and limit themselves to the processing of personal data necessary for digital lending. The apps also share this data with third parties. Some (as mentioned above) do not indicate the third parties with whom they share this data. They do not inform users how long the third parties will have access to the data and what measures they are putting in place to ensure that the data shared with third parties is kept safe.

389 Rule 2.2, Nigeria Data Protection Regulations
390 NITDA Sanctions Soko Loan for Privacy Invasion https://nitda.gov.ng/nitda-sanctions-soko-loan-for-privacy-invasion/

South Africa

Country Profile

South Africa, also known as the Republic of South Africa, is found in the southernmost part of Africa.[391] It shares a border with Namibia, Botswana, Zimbabwe, and Eswatini[392] and is among the prominently toured locations in Africa. South Africa is known for its beautiful topography and cultural diversity.[393] The country has 11 official languages, i.e., Afrikaans, English, Ndebele, Northern Sotho, Sotho, Swazi, Tswana, Tsonga, Venda, Xhosa, and Zulu, with Zulu, Xhosa, and Afrikaans being the most spoken.[394] It has three capital cities, i.e., Pretoria, which hosts the Executive; Cape Town, which hosts the Legislature; and Bloemfontein, which hosts the Judiciary.[395] The country has a population of 60 million people[396] and covers an area of 1,221,037 sq kilometres.

391 South Africa https://www.britannica.com/place/South-Africa
392 Ibid
393 Ibid
394 South Africa https://www.nationsonline.org/oneworld/south_africa.htm
395 Ibid
396 South Africa Population 2021 https://worldpopulationreview.com/countries/south-africa-population

Data Protection in South Africa

Kenya, Nigeria, and South Africa are the leading countries in Africa in the fintech ecosystem, with 450 fintech companies.[397] South Africa has 200 fintech companies[398] broken down into several segments, i.e., payments, lendings, savings and deposits, among others.[399] Our key focus in this research is the lending sector, which is growing at a rapid rate.[400]

The lending sector comprises several platforms, including Pollen Finance, which is considered one of the country's largest lending platforms,[401] followed by Lulalend and Fundrr.[402] The industry falls under the purview of the National Credit Act,2005, which

397 South Africa, Nigeria and Kenya: Africa's Largest Fintech Hubs <https://fintechnews.africa/39379/kenya/south-africa-nigeria-and-kenya-africas-largest-fintech-hubs/ > Accessed on 4/8/2021
398 Ibid
399 Fintech Scoping in South Africa <http://www.treasury.gov.za/comm_media/press/2020/WB081_Fintech%20Scoping%20in%20SA_20191127_final%20(002).pdf > Accessed on 4/8/2021
400 (n1)
401 (n3) pg 8 (n1)
402 (n1)

provides for the regulation of the credit industry and the establishment of the National Credit Regulator, which is primarily responsible for supervising and regulating this sector.[403] The Act requires credit providers to register and makes the National Credit Provider responsible for such registration.[404] It also provides a detailed procedure for registering credit providers when applying for registration before the National Credit Provider.[405]

In terms of data processing activities, lending platforms must comply with the Protection of Personal Information Act (POPI Act) which lays out principles that should be adhered to by these platforms to ensure the security of personal data in their possession.[406] It is worth noting that the enforcement of the POPI Act by the Information Regulator began recently on the 1st of July 2020, and organisations were given a grace period of one year from the commencement date, i.e., the 1st of July 2020, to comply with the Act.[407]
So organisations (including entities owning the lending platforms) must ensure that their data processing activities are in line with the POPI Act. In line with this, this study seeks to analyse the data protection practices of these platforms. It starts by examining their policies to highlight the data collected by them. It then follows with an assessment of the data collected vis a viz the provisions of the POPI Act to establish whether these platforms comply with the data protection law.

Online Lending Platforms in this study

The online lending platforms in this study operate via websites, particularly Pollen Finance, Lulalend, and Fundrr. The only platform that works via an app is Niftycredit (GetBucks) which can be downloaded via Google Play.
Pollen Finance - One of the largest online lending platforms in the country
Lulalend - Lending
Fundrr - Lending
Nifty Credit (GetBucks) - Lending

Overview of Data Collected by the Digital Lending Apps in this study

403 National Credit Act, 2005 (Act No. 34 of 2005) https://www.gov.za/sites/default/files/gcis_document/201409/a34-050_0.pdf
404 Section 14, National Credit Act 2005
405 Chapter 3, National Credit Act 2005
406 Protection of Personal Information Act (POPI Act) https://popia.co.za/act/
407 POPI Commencement Date or POPI Effective Date starts the Clock
https://www.michalsons.com/blog/popi-commencement-date-popi-effective-date/13109

Pollen Finance[408] (Privacy Policy & Terms and Conditions)	Information Collected and Processed by the App	
	Permissions sought	
	Information collected from the user	General business information Contact numbers A street address, and An email address
	Information collected from the user's device/ Browser	Automatically collects the following information, which is stored in its server logs: IP address Cookie information Page requested
	Information received from third parties	
	Use of user's information by the App	User's information is used for the following purposes: Sending communication and updates regarding Pollen Finance' website or services The platform uses cookies to track a user's sessions and save them on its browsers and hard drives. The user's IP address is also used to identify problems within the website and administer it
	Information shared with third parties Duration of third party access	Pollen Finance shares information with third parties to deliver advertisements and online communication. The third parties use the data to assess the kind of offers, promotions, and advertisements that may appeal to the platform's users. However, the data shared is aggregated and not linked to any user of the platform. The platform gives users who do not wish their data to be used in advertisements room to exercise their opt-out option.

408 Pollen Finance Privacy Policy https://www.pollenfinance.co.za/privacy-policy/

	Disclosure of Information	Pollen Finance discloses user information for the following purposes: Market statistics: Discloses aggregate statistics to advertisers and business partners Third-party suppliers and agents: The third party is required to only use the data for providing the requested services Enforcement of Law: Discloses data when; required by law, protecting an individual's safety, and preventing violation of the law. The IP address may also be disclosed if necessary in a legal process or required by the law Change of ownership: Mergers, acquisition, sale of assets Pollen Finance Employees
	Tracking technologies/ website cookies	The platform uses cookies to track a user's sessions and save them on its browsers and hard drives. The user's IP address is also used to identify problems within the website and administer it
	Storage/ Security of data	"Website is hosted in a secure server environment that uses that uses a firewall and other security measures to prevent interference or access from outside intruders."
	Cross Border Transfer	Pollen Finance may transfer users' data outside the resident jurisdiction to other countries, including countries that do not have proportional laws (levels) on data protection.

Lulalend[409]	Information Collected and Processed by the App	
	Permissions sought	
	Information collected from the user	Name, registration number/ date of birth, physical & postal address, email address, telephone number, gender/ nationality/ ethnic origin and social origin/ age, financial information, personal opinion/ views/ preferences, confidential correspondence sent by a user, views/ opinions of others about a user, user's credit information and history,

409 Lulalend Privacy Policy https://www.lulalend.co.za/PrivacyPolicy

	Information collected from the user's device	Once a user visits Lulalend's website, the website servers automatically collect technical information regarding the user's visit and computer. This information includes details of the user's computer, IP address, operating system and browser type, location, and usage information.
	Information received from third parties	
	Use of user's information/purpose of collection of data	Lulalend uses a user's data for the following purposes: Decision making on whether to enter into a contract with a user Performance of obligations under the contract Compliance with a legal obligation Protection of user's legitimate interest Pursuance of Lulalend's legitimate interest Credit reporting purposes Direct marketing purposes Customisation and display of content such as products, articles, advertisements etc Send content on articles, products, advertisements, e.t.c., Notify users of the changes on the website
	Information shared with third parties Duration of third party access	Lulalend shares personal information with the following third parties: User's banks or financial institutions Credit bureau service providers Professional service providers providing legal assistance, accounting or auditing services Delivery and courier service providers Payment gateway provider Lulalend may share user's aggregated information and usage patterns of the website for advertising purposes

	Storage of user information by the App/ Security safeguards	.Lulalend commits to protecting personal data against loss, destruction and unauthorised access Lulalend identifies potential risks to personal information and puts safeguards to protect against those risks Lulalend ensures that their contracts with third parties have the following obligations: Third parties are not allowed to process personal info without Lulalend's consent Third parties to treat personal information as confidential and not to share with unauthorised parties Third-party to employ security measures of the same standard as Lulalend Third-party to notify Lulalend when unauthorised parties have accessed personal info If a third party is situated in another country, it should comply with the data protection laws of that country If a third party is legally obliged to disclose user info, it should inform Lulalend
	Cross Border Transfers of personal information	Lulalend transfers a user's data to another country subject to consent. The data is transmitted in the following circumstances: Where the transfer is necessary for the performance of the contract between Lulalend and the user Where the transfer is required for the fulfilment of pre-contractual measures The transfer is for the user's benefit The user has consented to the transfer To store user's information electronically in a secure database Lulalend's service providers have a right to transmit user's data electronically in databases hosted outside South Africa provided that they have the same level of security, policy and procedures on data protection as Lulalend
	Tracking and Cookies	Lulalend uses cookies on its website to: Distinguish users Keep track of users sessions on the website Store info on the users' preference Estimate the size of the website's audience and pattern usage Increase the speed of searches

Fundrr[410]	Information Collected and Processed by the App	
	Permissions sought	
	Information collected from the user	Fundrr collects the following information from users: IP address Contact information Business information Financial information, and Any info required by Fundrr
	Information collected from the user's device	(Internet Protocol) IP address Domain name address Identity of internet service or access provider Type of web browsing software Computer operating system URL of the page visited by a user on the website The language selected by a user for web browsing software
	Information received from third parties	
	Use of user's information by the App	
	Information shared with third parties/ Sharing of personal information Duration of third party access	Fundrr shares information with third parties in the following circumstances: When processing information for credit reporting purposes When enlisting services of partner organisations When enlisting services of third parties who provide services such as; billing and debt recovery, credit-related services (such as creditworthiness, credit rating, default listing, e.t.c.,) among others
	Tracking and cookies	Information gathered by cookies is stored and used to create profiles on users of the website. The report enables Fundrr to know user's preferences, use and behavioural activity.
	Storage of user information by the App/ Security	Information stored in a secure server for a period legally required of Fundrr
Niftycredit (GetBucks)[411]	Information Collected and Processed by the App	
	Permissions sought	

410 Fundrr Privacy Policy https://fundrr.co.za/privacy-policy/
411 Nifty Credit Privacy Policy https://niftycredit.co.za/za/terms-and-conditions

	Information collected from the user	The information collected from users by Niftycredit include: General information: name, ID number, gender, date of birth, residential address, contact details such as email and telephone number Employment information: employment history, education, qualifications, experience, demographic data, geographic data, and salary information Application information: Information provided during the application, including assets, income, and debt Account information: bank account information, loan Transaction information: Information relating to transactions and account activity such as account balances, payment history, and account usage Consumer report information: Information obtained from cookies Telephone recordings User's marketing preferences Identifiers such as (internet protocol) IP address Information is obtained from a user when: Viewing Niftycredit website Opening an account/ applying for Niftycredit services Contacting Niftycredit via email, social media, or telephone Information is also obtained from third parties who: Monitor use of the website Carry out market research, surveys and business and statistical analysis
	Information collected from the user's device	
	Information received from third parties	
	Use of user's information by the App	Niftycredit uses user information for the following purposes: Provision of products and services Facilitation of transactions Servicing, maintenance, or collection of accounts Product applications and evaluation of user's eligibility Conducting credit reference searches or verifications Conducting credit scoring and assessment Performing risk management Providing users security Verifying accounts Confirming and verifying user's identity Debt recovery Compliance with legal and regulatory requirements, among others

	Information shared with third parties/ Sharing of personal information	Niftycredit shares the news with members of its group and professional advisers to obtain professional advice and defend legal claims, among others. It also shares information with the following third parties: Providers of payment systems, debt collection agencies, tracing agents, and suppliers monitoring the use of social media IT suppliers, auditors, marketing agencies, tax providers, e.t.c., Law enforcement agencies Law firms or organisations for purposes of providing legal advice or legal representation Survey providers Regulators and governmental authorities, ombudspersons or tax authorities
	Tracking and cookies	Uses cookies for the following purposes: Authentication of users Status of user's use of the site (i.e., if a user is logged into the site) Personalisation of the site for users Protection of user's account and prevention of fraudulent logins Advertisement Analysis of the performance of the website
	Storage of user information by the App/ International transfer of data	Seeks user consent in instances where data is processed outside the country. Where servers, suppliers, or service providers are based outside the country, or where servers are based outside South Africa, Niftycredit shall ask the party to whom user's data is transferred to agree to its privacy principles and practices.

Analysis of the Data Protection Practices of the Online Lending Platforms

Accountability

The Protection of Personal Information Act (POPI Act)[412] requires online lending platforms, among other bodies, to process personal data to ensure accountability when processing data. It specifically requires them to comply with the conditions set out in the Act for lawful processing. These conditions must be applied when determining the purpose and means for processing personal data.[413]

The conditions include accountability, processing limitation, purpose specification, further processing limitation, information quality, openness, security safeguards, and data subject participation, as discussed in the following sections.[414]

412 Protection of Personal Information Act (POPI Act), Act 4 of 2013 https://popia.co.za/
413 Section 4 (1) (a) POPI Act
414 Section 4, POPI Act

Processing Limitation

This condition enshrines several principles in it.[415] First, it requires personal data to be processed lawfully and reasonably, not infringing the right to privacy of the data subject.[416] Secondly, it requires personal data to be collected directly from the data subject, unless in exceptional circumstances laid out in the Act.[417] Thirdly, it requires that personal data is processed for the intended purpose for which it was collected and that such data should be adequate, relevant, and not excessive. Lastly, this condition requires that such data collection is subject to the user's consent, with reasonable justification given for the processing. The user has a right to object to such processing.[418]

An examination of the online lending platforms in this study indicates that the lending companies automatically obtain personal data once a user uses the website, submits details during registration, or uses the products. Users who do not consent/ object to the processing of their data are advised to stop accessing the websites and are automatically deprived of the products offered by the websites. In this case, it can be said that consent is not given out of a user's free will but the user's need to access the product.

Some of the platforms under study collect irrelevant information that is not in line with such processing. Niftycredit, for instance, collects information such as a user's employment history, experience, bank account details, and telephone readings that are not relevant for purposes of lending.[419] Lulalend, on the other hand, collects information such as the user's ethnic origin, personal opinion/ views, and other people's personal opinion/ views about the user, which are not relevant.[420]

Lulalend complies with the requirement to collect user information directly from the user and provides exceptional circumstances in line with POPI Act where compliance may not be heeded.[421]

Data Retention

Online lending platforms are required under the POPI Act not to retain personal information for longer than is necessary for achieving the purpose of collection.[422] It states that the company shall only have personal data for extended periods if the law requires it. The lending platform requires it for a lawful purpose, a contract between the parties involves retention, or the data subject consents to it[423].

The platforms reviewed in this study indicated this principle in their privacy policies, stating expressly that the company will delete users' data once the purpose of such collection has

415 Section 4 (1) (b), POPI Act
416 Section 4 (1) (9), POPI Act
417 Section 12, POPI Act
418 Section 11, POPI Act
419 Nifty Credit Privacy Policy https://niftycredit.co.za/za/terms-and-conditions
420 Lulalend Privacy Policy https://www.lulalend.co.za/PrivacyPolicy
421 Lulalend Privacy Policy https://www.lulalend.co.za/PrivacyPolicy
422 Section 14, POPI Act
423 Section 14 (1), POPI Act

been achieved.[424] However, other platforms such as Fundrr and Nifty Credit require users to request the deletion of their information. On the other hand, Pollen Finance makes no mention of this principle in its Privacy Policy, and it is unclear whether it complies with this principle.

Security Safeguards

POPI Act requires these online lending platforms to secure the integrity and confidentiality of personal information in their possession by taking appropriate, reasonable, technical and organisational measures to prevent; loss, damage or unauthorised destruction of personal data and unlawful access to confidential information.[425] In line with this, it adds that these platforms should take reasonable measures to: identify all foreseeable risks to personal information, maintain appropriate safeguards against the risks identified, verify that the securities are implemented, and ensure that the safeguards are continually updated in response to new threats.[426]

Where there has been a security breach, these platforms are called upon to notify the Regulator and the data subject.[427] Regarding third parties processing personal information on behalf of these platforms, the Act requires them to; process such data with the authorisation of these platforms and treat such data as confidential.[428] Lulalend and Nifty credit seem to have incorporated these measures in their privacy policies among the platforms in this study. Fundrr and Pollen Finance privacy policies, on the other hand, only give an undertaking of ensuring the security of personal data but do not indicate to users the security measures that the platforms will take to ensure confidentiality of their personal information.

User's Rights and Participation

Data subjects are provided with rights concerning their data. In particular, they have the right to access their personal information[429]and the right to request for its correction[430]. The Act further provides access to information wherein the provisions of the Promotion of Access to Information Act (PAIA).[431]

The platforms give users room to access, correct, and update their personal information. They also provide avenues (i.e., contact details) on how this can be done. The platforms further allow users to raise concerns and lodge complaints.

Opt-Out Option

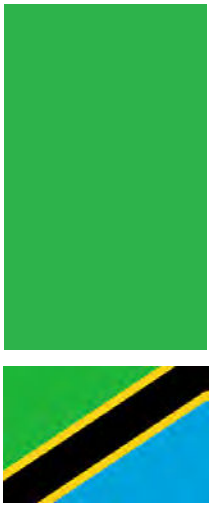
Inline requirement of consent under POPIA concerning marketing by electronic means[432]All platforms understudy give users an option of opting-out of marketing messages.

424 Lulalend Privacy Policy https://www.lulalend.co.za/PrivacyPolicy
425 Section 19, POPI Act
426 Section 19 (2), POPI Act
427 Section 22 (1), POPI Act
428 Section 21 (1), POPI Act
429 Section 23, POPI Act
430 Section 24, POPI Act
431 Section 25, POPI Act
432 Section 69, POPI Act

Conclusion

In conclusion, the Privacy Policies of some of the platforms in this study can be compliant with POPIA. However, this compliance is only at the policy level. We are keen to see whether the platforms will comply with POPIA in practice, given that it commenced operation on the 1st of June.

Tanzania



Country Profile

Located in East Africa, the United Republic of Tanzania borders the Indian Ocean to the east. It has land borders with eight countries: (anti-clockwise from the north) Kenya, Uganda, Rwanda, Burundi, the Democratic Republic of Congo (across Lake Tanganyika), Zambia, Malawi and Mozambique. The country includes Zanzibar (the main island Unguja, plus Pemba and other smaller islands).[433] The country's population is estimated to be 59,734,210 as of 2020.[434]

433 https://www.eac.int/eac-partner-states/tanzania
434 https://data.worldbank.org/indicator/SP.POP.TOTL?locations=TZ

Data Protection in Tanzania

In 2014, Vodacom Tanzania became a forerunner in the fintech ecosystem in Tanzania. This shift resulted from when it partnered with Commercial Bank of Africa - CBA (Now NCBA), to launch MPawa, a revolutionary banking product allowing Vodacom subscribers to save money through their phone, earn interest from their savings and eventually get microloans.[435]

Ever since, the fintech ecosystem in Tanzania has been on a rapid and upward trajectory, culminating in the rise and popularity of financial Apps for consumers.
More than 54 per cent of Tanzania's population uses mobile payment and money transaction services.[436]

Traditional banking institutions, non-banking institutions, and Mobile Network Operators - MNOs (with their mobile wallets) have launched their own digital lending mobile Apps over the years. These include but are not limited to; TigoPesa Nivushe,[437] Branch,[438] Halotel Haloyako,[439] etc.

435 https://www.vodacom.co.tz/mpawa
436 https://www.statista.com/statistics/1082056/tanzania-mobile-money-transaction-value/
437 https://www.tigo.co.tz/tigo-pesa-nivushe
438 https://branch.co.tz
439 https://halotel.co.tz/package-mobile/1552657603579

With Tanzania lacking Data Protection and Privacy legislation,[440] the predatory nature of some of these Apps is likely to put users privacy and personal data at risk.

Digital lending Apps and their Data Collection Practices

Vodacom MPawa[441]	Data collected and processed by the App	
	App permissions sought	This app has access to: Phone contacts Location (GPS and network-based) User's SMS Phone status and identity Content of device storage Camera Device ID & call information Network connections
	User Data collected	Where applicable: Name, address, phone and mobile number, date of birth, gender and email address; Credit or debit card information, information about bank account and other banking information
	Information collected from the user's device	Device ID Traffic data. Location data; Global Positioning System (GPS) data /Wi-Fi hotspots /IP address or information such as a post-code or name of a town or city;
	Information received from third parties	Credit reference
	Use of user's information by the app	Processing orders and providing a user with products and service Improving and innovating products and services Marketing & tailoring service to a user Profiling (for credit, fraud and security purposes)

440 https://www.mwananchi.co.tz/mw/habari/kitaifa/usalama-taarifa-binafsi-shakani-3006726
441 https://www.vodacom.co.tz/mpawa

	Data sharing with Third parties	Where applicable, Vodacom shares information with: Companies in the Vodacom Group Partners or agents involved in delivering the products and services ordered or used; Companies who are engaged to perform services for, or on behalf of, Vodacom Tanzania Public Limited Company, Vodacom Group or Vodafone Group; Credit reference, fraud-prevention or business-scoring agencies, or other credit scoring agencies; Debt collection agencies or other debt-recovery organisations; Law enforcement agencies, government bodies, regulatory organisations, courts or other public authorities if we have to, or are authorised to by law; A third party or body where such disclosure is required to satisfy any applicable law or other legal or regulatory requirements; Emergency services (if you make an emergency call), including your approximate location; Third parties for joint promotions with that third party;
	Tracking technologies/ website cookies	GPS / Website cookies
	Storage of user information by the app	Personal data is stored in Tanzania

TigoPesa Nivushe[442]	Data collected and processed by the app	
	App permissions sought	This app has access to: Phone contacts Location (GPS and network-based) User's SMS Phone status and identity Content of device storage Camera Device ID & call information Network connections
	User Data collected	registration information: User's full name, age, telephone number, email address, mailing address, payment information, billing address or username and password.

442 https://www.tigo.co.tz/tigo-pesa-nivushe

	Information collected from the user's device	information about user location. Mobile application information is based on the websites visited and applications downloaded from the Tigo network. Information about the use of the Portal: the network address and operating system of a computer, type of browser used, the website from which one linked to the site, user activity on Portal, as well as user's viewing history, the time and date they visited and purchased products and services through the Portal.
	Information received from third parties	Credit reference
	Use of user's information by the app	Determination of consumption, maintenance and improvement of services, Customer service, customisation of content, services and offers, business plans, customer satisfaction, creation of databases, analysis of information and data, design of key performance indicators (KPI) applications, billing, security, quality control and, in general, all information necessary to comply with Tigo's product or service contracts, as well as applicable laws and regulations To extend offers, promotions, products, advertisements, opportunities, sweepstakes, campaigns, loyalty programs, customer retention
	Data sharing with Third parties	Tigo shares personal data with: Third parties who provide services to Tigo such as storage services, order fulfilment, collection and shipping, surveys, customer service, or advertising Law enforcement Other Tigo entities, or in the event of a merger, acquisition, sale of company assets, or transition of service to another provider Other jurisdictions that have data protection laws other than those established in Tanzania, by written order of a competent judicial authority or where permitted in compliance with the law
	Tracking technologies/ website cookies	GPS / Website cookies
	Storage of user information by the app	Personal data is primarily stored in Tanzania but may be transferred to other jurisdictions with data protection laws other than those established in Tanzania by written order of a competent judicial authority or where permitted in compliance with the law.

Branch Tanzania[443]	Data collected and processed by the app	
	App permissions sought	This app has access to: Phone contacts Location (GPS and network-based) User's SMS Phone status and identity Content of device storage Camera Device ID & call information Network connections
	User Data collected	Name, address, email address and phone number, the device's phone number, SIM card details, age, username, password and other registration information, financial and credit information (including mobile money account details, bank account details, and bank verification number, where applicable), personal description and photograph.
	Information collected from the user's device	Technical information, including the type of mobile device, unique device identifiers (for example, user Device's IMEI or serial number), information about the SIM card used by the device, mobile network information, your device's operating system, the type of browser, or device's location and time zone setting (Device Information); Information stored on user Device, including contact lists, call logs, SMS logs, Facebook friends, contact lists from other social media accounts, photos, videos or other digital content (Content Information); Data from the use of any other third-party application on the Device or the Service Sites
	Information received from third parties	Credit reference agencies and mobile network providers
	Use of user's information by the app	Information collected is used to determine the customer's eligibility, the amount of such loan, and the terms and conditions applicable to such loan. Where applicable: In compliance with an order of the Court, Arbitral Panel, Tribunal, Regulatory Directive or Order or any other legal or regulatory obligation
	Data sharing with Third parties	Branch shares personal data with: Credit reference bureaus Any member of Branch group, i.e. subsidiaries, affiliates, holding company and its subsidiaries Any legal or regulatory authorities as requested
	Tracking technologies/ website cookies	GPS / Website cookies

443 https://branch.co.tz

	Storage of user information by the app	Data may be transferred to, and stored at, a destination outside Tanzania (as applicable). It may also be processed by staff operating outside Tanzania (as appropriate)

Halotel Haloyako[444]	Data collected and processed by the app	
	App permissions sought	This app has access to: Phone contacts Location (GPS and network-based) User's SMS Phone status and identity Content of device storage Camera Device ID & call information Network connections
	User Data collected	Name, date of birth, address, type and number of Identification Document, place of birth and nationality, marital status, account information, email, etc.
	Information collected from the user's device	information about user location.
	Information received from third parties	Credit reference
	Use of user's information by the app	Process the goods and services bought from Halotel Provide the relevant service or product to a user Bill user for using our products or services. Let the user know about other companies' products and services that may be of interest to them Carry out research and statistical analysis, including monitoring how customers use products and services on an anonymous or personal basis. Prevent and detect fraud or other crimes, recover debts or trace those who owe Halotel money. Provide aggregated reports to third parties

444 https://finca.co.tz/haloyako/

	Data sharing with Third parties	Partners or agents involved in delivering the products and services you have ordered or used Partners or agents that conduct customer satisfaction surveys and any other surveys related to the products or services provided to a user Companies who are engaged to perform services for, on behalf of HaloPesa or Halotel Tanzania. Where applicable, credit reference, fraud prevention, business scoring agencies, or other credit scoring agencies. Debt collection agencies or other debt recovery organisations. Law enforcement agencies, regulatory organisations, courts or other public authorities if we have to, or are authorised to by law. Emergency services (in cases of an emergency call)
	Tracking technologies/ website cookies	GPS / Website cookies
	Storage of user information by the app	Personal data is handled by Halotel in Tanzania but may be processed by other organisations with contractual obligations with HaloPesa or Halotel Tanzania in compliance with the law.

Analysis of Pay Day Apps with Regards to the Regulatory Ecosystem

While Tanzania has no Data protection legislation in place, the Constitution of the United Republic of Tanzania, 1977 ("the Constitution"), does guarantee the right to privacy and personal security.[445] Sections 98 and 99 of The Electronic and Postal Communications Act 2010 ("the EPOCA") place the onus of confidentiality of information on network service licensees and prohibit the disclosure of such information without authorisation, respectively.[446] On its part, the Electronic and Postal Communications (Consumer Protection) Regulations 2018 requires a licensee to protect consumer information against improper or accidental disclosure.[447]

The National Payment Systems (NPS) Act of 2015 and the Bank of Tanzania Act 2006 empower the Bank of Tanzania (BoT) to regulate and supervise the payment systems services and products offered by both banks non-bank institutions in Tanzania.[448]

Right to Privacy

Each assessed digital lending App seeks permission to access users' phone contacts, location, user's SMS, and other permissions. This permission puts the users of these Apps at risk of having their privacy compromised if they land in the hands of rogue data controllers.

445 Article 16, The Constitution of the United Republic of Tanzania (1977) https://rsf.org/sites/default/files/constitution.pdf
446 The Electronic and Postal Communications Act 2010 ("the EPOCA") https://www.tcra.go.tz/uploads/documents/sw-1619082940-The%20Electronic%20and%20Postal%20Communications%20Act,%202010%20(Act%20No.%203%20out%20of%2010).pdf
447 Regulation 6 (1) & (2) https://www.tanzania.go.tz/egov_uploads/documents/EPC%20consumer%20Protection%20Regulations%202011.pdf
448 https://www.bot.go.tz/PaymentSystem

Transparency

It is apparent that the Apps privacy policies are transparent, as they both lay bare what kind of information they collect from users, the reason for the collection, who they share the collected data with and why, and whether the data sharing is within and or outside the country of domicile.

Right of Access and Deletion of Personal Data

While the users of these Apps can have their data amended by the data operators, the question of the right to deletion of their data is vague in some of the Apps.[449] Vodacom remains the only company that attempts to tackle the question of the Right of Access in its retention schedule. According to Vodacom, user information is retained for the duration of a user's contract or as required by law. Vodacom will delete user information afterwards.[450]

449 Section 93(4) of Electronic & Postal Communications Act https://www.tcra.go.tz/uploads/documents/sw-1619082940 The%20Electronic%20and%20Postal%20Communications%20Act,%202010%20(Act%20No.%203%20out%20of%2010).pdf

450 https://www.vodacom.co.tz/public/assets/files/Vodacom%20Tz-%20%20Customer%20Privacy%20Statement-retention-schedule.pdf

Uganda

Country Profile

Located in East Africa, Uganda is a landlocked country lying astride the equator. It is bordered (clockwise from north) by Sudan, Kenya, the United Republic of Tanzania, Rwanda and the Democratic Republic of Congo.[451] The country has an estimated population of 39.0 million[452]

451 EAC https://www.eac.int/eac-partner-states/uganda
452 https://www.eac.int/component/documentmananger/?task=download.document&file=b-WFpbl9kb2N1bWVudHNfcGRmX0V2cFVzSHl3RUF6dUhnS2hXc3RkVkRNRUFDIEZhY3RzIEZpZ3VyZX-MgMjAxOQ==&counter=575

Data Protection in Uganda

Uganda boasts of a vibrant and fast-growing ICT sector, with more than half its population having access to mobile phones. Uganda has an autonomous statutory body known as the National Information Technology Authority-Uganda (NITA-U), established under the NITA-U Act 2009. Its role is to coordinate and regulate Information Technology services in Uganda. Data from the NITA-U show that smartphones and feature phones with direct internet access remain the driver of new mobile Internet subscriptions. Subscriptions have grown from 21.5 million smartphones and feature phones in the Financial Year 2018/19 to about 24.1 million in the Financial Year 2019/20.[453]

Digital lending, a concept rapidly taking root in East Africa, has facilitated mobile subscribers with fast and easy access to lending facilities. MTN, the country's largest mobile phone company, with the partnership of Commercial Bank of Africa (CBA) – now NCBA - launched MoKash, a mobile-enabled digital lending service, in 2016[454].
Based on customer need for more saving and lending options, MoKash drew lessons from similar launches and successes of M-shwari in Kenya in 2012 and M-Pawa in the United Republic of Tanzania in 2014.[455]

Following MoKash's launch, 83,000 customers signed up within the first 48 hours, 650,000

453 NITA https://www.nita.go.ug/publication/nita-u-statistical-abstract-2020
454 https://techweez.com/2016/08/10/cba-partners-mtn-launching-mokash-m-shwari-equivalent-uganda/ accessed 18 July 2021
455 https://www.uncdf.org/article/2844/disrupting-savings-lending-market-uganda-mokash accessed 20 July 2021

after one month and over 1,000,000 in three months,[456] beating previous records set by its counterparts M-Shwari in Kenya (645,000 customers in the 21 days after launch) and M-Pawa in the United Republic of Tanzania (250,000 customers in the first month).[457]

The vibrant Financial technology (Fintech) ecosystem in Uganda has spurred the mushrooming of payday Apps. Apart from MTN's MoKash, other Apps familiar include Airtel's Wewole, Money Mate Uganda, and last but not least, Numida Business Loans.

Digital lending Apps and their Data Collection Practices

456 https://www.uncdf.org/article/1675/three-months-down-the-road-the-story-of-mokash-in-uganda-migration accessed 20 July 2021

457 Ibid.

MTN MoKash[458]	Data collected and processed by App	
	App permissions sought	This app has access to: Phone contacts Location (GPS and network-based) User's SMS Phone status and identity Content of device storage Camera Device ID & call information Network connections
	User Data collected	Name, Identification number, physical address, date of birth, nationality, email address, telephone numbers
	Information collected from the user's device	mobile station identification number Global System for Mobile telecommunication ("GSM")
	Information received from third parties	Credit reference
	Use of user's information by the App	Processing orders and providing a user with products and service Marketing & tailoring service to a user
	Data sharing with Third parties	Partners or agents involved in delivering products and services; Credit reference, fraud-prevention or business-scoring agencies; Law enforcement agencies, government bodies, regulatory organisations, courts or other public authorities if required, or if authorised by law;
	Tracking technologies/ website cookies	GPS / Website cookies
	Storage of user information by the App	Personal data is stored in Uganda

458 https://www.mtn.co.ug/mtn-momo/

AirtelMoney Wewole[459]	Data collected and processed by App	
	App permissions sought	This app has access to: Phone contacts Location (GPS and network-based) User's SMS Phone status and identity Content of device storage Camera Device ID & call information Network connections
	User Data collected	Name, Identification number, physical address, date of birth, nationality, telephone number
	Information collected from the user's device	Mobile Subscriber Integration Services Digital Number, and corresponding identification number and PUK for accessing the Airtel Network
	Information received from third parties	Credit reference
	Use of user's information by the App	Processing orders and providing a user with products and service
	Data sharing with Third parties	Partners and or agents involved in delivering products and services; Law enforcement / regulatory agencies
	Tracking technologies/ website cookies	GPS / Website cookies
	Storage of user information by the App	While domiciled in Uganda, it is undefined on where the data is stored

459 https://www.airtel.co.ug/media/press_release/extends_credit_services

MoneyMate Uganda[460]	Data collected and processed by App	
	App permissions sought	This app has access to: Phone status and identity Network connections
	User Data collected	Username, Phone user number, Identification number, mobile phone number, fixed-line phone, correspondence addresses, Company or Registered Corporation (for business entities)
	Information collected from the user's device	Device ID
	Information received from third parties	Undefined service providers
	Use of user's information by the App	Processing requests / transacting
	Data sharing with Third parties	Undefined service providers
	Tracking technologies/ website cookies	GPS / Website cookies
	Storage of user information by the App	Uganda

Numida - Business Loans[461]	Data collected and processed by App	
	App permissions sought	This app has access to: Location (GPS and network-based) Content of device storage Camera Device ID & call information Network connections
	User Data collected	Name, ID, phone number/business information (for businesses)
	Information collected from the user's device	Device ID / Operating System (OS)
	Information received from third parties	Credit reference bureaus
	Use of user's information by the App	Provide and improve our services. Targeted advertising Communication with user

460 https://play.google.com/store/apps/details?id=com.moneymateuganda.mmg
461 https://play.google.com/store/apps/details?id=com.numidatech.numida&hl=en_US&gl=US

	Data sharing with Third parties	Credit reference bureaus Staff and suppliers
	Tracking technologies/ website cookies	GPS / Website cookies
	Storage of user information by the App	Personal data is stored in Uganda but may be shared with and processed by staff operating inside or outside of Uganda

Analysis of Pay Day Apps with regards to the Regulatory Ecosystem

In the period preceding the era of the rapid growth of the Fintech ecosystem in Uganda, the regulators enacted many legislations.

These include the Electronic Transactions Act (2011),[462] an Act to provide for the use, security, facilitation and regulation of electronic communications and transactions, encourage the use of e-government services and provide for related matters; Computer Misuse Act (2011),[463] an Act making provision for the safety and security of electronic transactions and information systems to prevent unlawful access, abuse or misuse; the Contracts Act (2010);[464] the Electronic Signatures Act (2011);[465] and Bank of Uganda (BoU) Mobile Money Guidelines (2013)[466]

Despite these different legislations' inability to address constraints to, or support, digital payment systems' operation or future development, in theory, they seemed to accord stakeholders some 'protection'.

In efforts to stay abreast with the latest technological advancements in the digital sector, additional legislation geared at regulating the flourishing fintech ecosystem have recently been passed. The National Payments System Act (2020)[467] seeks to provide for the safety and efficiency of payment systems, to provide for the functions of the Central Bank concerning payment systems. The National Payment Systems Agents Regulations (2021)[468] aims to streamline the licensing of mobile money agents. The National Payment Systems (Sandbox) Regulations (2021),[469] on the other hand, provides a 'sub regulatory' sandbox framework for innovative financial products and services, business models, or delivery mechanisms in the payments systems ecosystem.

462 https://ict.go.ug/2019/12/03/the-electronics-transactions-act-2011/
463 https://ict.go.ug/2019/12/03/the-computer-misuse-act-2011/
464 https://commons.laws.africa/akn/ug/act/2010/7/eng@2010-05-28.pdf
465 https://www.nita.go.ug/publication/electronic-signatures-act-2011-act-no-7-2011
466 https://www.bou.or.ug/bou/bouwebsite/FinancialInclusion/innovations.html
467 https://www.bou.or.ug/bou/bouwebsite/bouwebsitecontent/acts/supervision_acts_regulations/Payment-Systems-Act/The-National-Payments-Systems-Act-2020.pdf
468 https://www.bou.or.ug/bou/bouwebsite/bouwebsitecontent/acts/supervision_acts_regulations/Payment-Systems-Regulations/The-National-Payment-Systems-Agents-Regulations-2021.pdf
469 https://www.bou.or.ug/bou/bouwebsite/bouwebsitecontent/acts/supervision_acts_regulations/Payment-Systems-Regulations/The-National-Payment-Systems-Sandbox-Regulations-2021.pdf

The Data Protection and Privacy Act[470] was assented to on 25 February 2019 but came into effect on 3 May 2019. The Act regulates the collection and processing of personal information. It applies to any person, institution, or public body that collects, processes, stores, or uses personal data within Uganda or outside Uganda.

For entities domiciled outside Uganda, the Act is restricted to personal data relating to Ugandan citizens.

Right to Privacy

With the various regulations in place, among them Uganda's Data Protection and Privacy legislation, the lending App companies seem to have integrated considerations of privacy issues from the beginning of the development of their products and services in the quest to maintain privacy and confidentiality of all personal information collected.

Transparency

The lending App companies are open on the personal data collection practices; collection, storing, sharing with third parties, and administrative measures to guarantee security with collected personal data, a move that complies with data protection impact assessment.

Right of Access and Deletion of Personal Data

Section 35 of the Data Protection and Privacy Acts spells out the Right to access personal information in possession by a data controller. A data subject has a right to request the same be amended accordingly. S/he (data subject), however, must satisfy the requirement of proof of identity, where the data subject the provide any of the following - (a) a national identification card or aliens identification card; (b) a passport or any travel document; or (c) a drivers licence. On their part, a data controller is required to inform the data subject of its decision within seven days after receipt of the request.

In its consumer terms, MTN states that 'any person submitting any information to MTN through the Mobile Money System may be granted access rights to that information. The statement adds that 'MTN has developed systems that enable access and correction of information submitted to it.'[471] The others, Airtel Money, Money Mate and Numida, are silent on actions regarding this provision.

470 Uganda Data Protection and Privacy Act https://ict.go.ug/wp-content/uploads/2019/03/Data-Protection-and-Privacy-Act-2019.pdf <https://www.nita.go.ug/sites/default/files/publications/Data%20Protection%20and%20Privacy%20Act%20No.%209%20of%202019.pdf> accessed 23 July 2021.

471 https://www.mtn.co.ug/wp-content/uploads/2019/10/MTN-MOBILE-MONEY-Consumer-Terms-and-Conditions-0519.pdf

Zimbabwe

Country Profile

Zimbabwe, also known as the Republic of Zimbabwe, is located in Southern Africa.[472] It shares a border with South Africa, Botswana, Zambia, and Mozambique.[473] It covers an area of 390,757 km and has a population of 15 million.[474] Its capital city is Harare, and English, Shona, Ndebele are its most spoken languages.[475]

472 Britannica https://www.britannica.com/place/Zimbabwe
473 Britannica https://www.britannica.com/place/Zimbabwe
474 Zimbabwe https://www.nationsonline.org/oneworld/zimbabwe.htm
475 Zimbabwe https://www.nationsonline.org/oneworld/zimbabwe.htm

Data Protection in Zimbabwe

The emergence of technology has brought about significant development in the financial sector in Zimbabwe. It has given rise to fintech, which has revolutionized the industry and brought about financial inclusion where the unbanked population can access financial services. The digital lending sector is an essential feature in the fintech ecosystem, facilitating fast and easy access to cash online with no security.

Digital lending in Zimbabwe, however, remains unregulated. The financial systems regulatory framework only covers financial institutions such as banks, building societies, and insurance companies.[476] The Banking Act limits the licensing, supervisory and regulatory powers of the Reserve Bank of Zimbabwe to deposit-taking and loan issuing institutions.[477] This leaves a wide gap in terms of the regulation of practices of lending platforms.

There is also no regulatory framework covering the data protection practices of the digital lending platforms. Zimbabwe currently has a Data Protection Bill that has not been enacted yet. The Senate recently passed the Bill but was subsequently returned to parliament for amendments.[478] The right to privacy is provided for in the constitution and some sectoral laws, such as the Freedom of Information Act, which governs data protection by public

476 Section 2 (a)(iii), Banking Amendment Act, 2015 https://www.rbz.co.zw/documents/acts/Banking%20Amendment%20Act,%202015.pdf
477 Fsd Africa, Zimbabwe Fintech Ecosystem Study (March 2020) pg 27 https://www.fsdafrica.org/wp-content/uploads/2020/03/Zim-Fintech-Report-25.03.20_FINAL.pdf
478 Zimbabwe on the Cusp of Finalizing Data Protection Law https://iapp.org/news/a/zimbabwe-on-the-cusp-of-finalizing-data-protection-law/# Zimbabwe's Controversial Cybersecurity and Privacy Bill Sent Back https://www.grcworldforums.com/global/zimbabwes-controversial-cyber-security-and-privacy-bill-sent-back/2325.article

bodies.[479]

The lack of a data protection law in Zimbabwe leaves the data protection practices of the lending apps unregulated and poses a significant risk to the users of the apps. This study examines the data collected by three notable apps in Zimbabwe, i.e., GetBucks, MyBucks, and eShagi. It subsequently provides guidance on data protection practices that the apps should adopt based on international best practices.

Overview of Data Collected by the Digital Lending Apps in this study

GetBucks[480]	Information Collected and Processed by the App	
	Permissions sought	
	Information collected from the user	ID number, contact number, street number, email address, and IP address The platform receives and records user information processed from a user's browser on its servers upon using the website. This information includes: IP address Cookie information The page requested by a user "GetBucks may also intercept, monitor, block, filter, read, delete, and disclose any communication over its information system. This includes but is not limited to the tracking of user Internet Protocol addresses (IP Addresses), and users agree that GetBucks may request their personal information from their Internet Service Provider for whatever reason the site sees fit to ensure a safe and trusted relationship with the user".
	Information collected from the user's device/ Use of the website	The platform receives and records user information processed from a user's browser on its servers upon using the website. This information includes: IP address Cookie information The page requested by a user
	How is user info collected	User information is collected on the use of the website
	Information received from third parties	
	Use of user's information by the App	

479 Zimbabwe: Data Protection Overview https://www.dataguidance.com/notes/zimbabwe-data-protection-overview
480 GetBucks Privacy Policy https://zw.getbucks.com/site-policy

	Information shared with third parties/ Disclosure of Information Duration of third party access	GetBucks shares user personal information with the following third parties: Marketers - disclose user information for marketing purposes Suppliers or agents - disclose user information to suppliers for the provision of services Law enforcement agencies - disclose user information when required by a court order or law May disclose a user's IP address when required by law Affiliates Business partners in cases of; change of ownership, mergers, acquisition, or sale of assets Employees - when doing their jobs Third parties when resolving or investigating complaints[481]
	Tracking technologies/ website cookies	
	International data transfers	This platform may transmit or transfer personal user data to countries outside Zimbabwe. The countries may have data protection laws that are less stringent.
	Storage of information/ security of data	"Uses advanced security measures to protect personal data in its possession."

MyBucks[482]	Information Collected and Processed by the App	
	Permissions sought	

481 GetBucks Privacy Policy: Disclosure Clause https://zw.getbucks.com/site-policy
482 MyBucks Privacy Policy https://corporate.mybucks.com/privacy

	Information collected from the user	Processes the following user information/ data: Usage data: IP address, geographical location, type of browser and version, operating system, referral source, length of visit, pages viewed and website navigation paths, timing of usage, user frequency and pattern of use of the service.[483] User account data: user's name and email address User profile data: name, address, telephone number, email address, profile picture, gender, date of birth, relationship status, interests and hobbies, educational details and employment details User employment data: name, address, telephone number, email address, profile picture, gender, date of birth, relationship status, interest and hobbies, employment history, education, qualifications, experience, demographic information, geographic location, and salary information User service data: data related to user's use of MyBuck's services Publication data: data based on information published by the user on the MyBucks website. Enquiry data: data based on a user's enquiry regarding MyBucks products, services or employment Customer relationship data: Includes a user's; name, employer, job title, contact details, the information contained in correspondence between MyBucks and the user or the user's employer. Transaction data: information relating to user's transactions with MyBucks through the website Notification data: includes information relating to a user's subscription to MyBucks email notifications. Correspondence data: information relating to a user's communication with MyBucks Information processed through cookies Telephone recordings User market preferences User's IP address
	Information collected from the user's device	
	How is user information collected	
	Information received from third parties	

483 MyBucks Privacy Policy: Clause 3.2

	Use of user's information by the App	MyBucks uses user information for the following purposes: Running MyBucks and its internal operations Compliance with legal and regulatory obligations Evaluating user's ability to pay the loan Providing users with sustainable services Providing users with appropriate high-quality services Providing MyBucks with an understanding of its business and improving its services Ensuring MyBucks systems work efficiently Ensuring information processed about users is correct Preventing crimes such as fraud Administering repayments Recovering debt Maintaining business records Marketing MyBucks products and services Improving the quality of services offered by MyBucks Ensuring MyBucks systems work efficiently Protecting the security of MyBucks systems Resolving complaints Defending legal claims Compliance with a legal obligation[484]
	Information shared with third parties Duration of third party access	Discloses user information to the following parties: Members of MyBucks group Insurers and professional advisers Service providers, i.e., providers of payment systems, debt collection agencies, e.t.c., IT suppliers, auditors, marketing agencies, tax advisers, suppliers monitoring the use of the MyBucks website A user's agent Banks or financial institutions Law enforcement agencies in the investigation and prevention of crime Law firms/ organizations providing MyBucks with legal advice or representing them in legal proceedings Surveyors appointed to carry out market research Business partners during the sale, transfer, or disposal of MyBuck's business Regulators and government authorities
	Tracking technologies/ website cookies	

484 MyBuck Privacy Policy: Clause 3 'How we Use Your Personal Data'

	International data transfers/ Cross border data transfer	MyBucks transfers user data to countries outside the user's jurisdiction.
	Storage of user information by the App	

eShagi[485] -eShagi has no privacy policy -Neither does it have terms and conditions	Information Collected and Processed by the App	
	Permissions sought	
	Information collected from the user	
	Information collected from the user's device	
	How Branch collects the information	
	Information received from third parties	
	Use of user's information	
	Information shared with third parties Duration of third party access	
	Tracking technologies/ website cookies	
	International data transfers	
	Storage of user information by the App	

Analysis of the Data Protection Practices of the Apps

User Control

Digital lending platforms should allow users to exercise autonomy over their data. They should enable users to know the nature of personal data being processed, how the information is being used, the parties the data will be shared with, and how it will be handled. They should also create avenues for users to access their data, seek to correct or update

485 eShagi website https://www.eshagi.com/

it, and even delete it. This is important because users have rights over their data, and any action taken on the data should be done subject to their consent. GetBucks lending app seems not to guarantee the complete enjoyment of this right. The policy only allows users to correct or update their data.[486] There is no avenue for users to access their data or even delete it when no longer needing the services. Users also cannot seek to transfer their data. MyBucks, on the other hand, guarantees users these rights. Under their policy, users have the right to access, rectify, delete, and port their data.[487]

Consent

Consent of users to the privacy policies is on a 'take it or leave it' basis. These apps collect excessive data and leave users with no option but to accept the terms due to their 'need' for the services. Take, for example, the GetBucks Privacy Policy "Intercept and Monitor Clause". This clause states that the platform "may intercept, monitor, block, filter, read, delete, and disclose any communication over its system. This includes but is not limited to the tracking of user internet protocol addresses (IP addresses), and request of user's personal information from their Internet Service Provider for whatever reasons the site deems fit ...."

Purpose Limit

Digital lending apps should indicate to users the purpose of data collection and the proposed use.[488] They should also ensure that they limit themselves to processing data necessary to provide their services.[489] In doing this, they should ensure that they process personal data that is adequate, relevant, and not excessive.

The apps studied appear to collect more data than necessary for digital lending. MyBucks processes user information such as users interests and hobbies, relationship status, employment history, professional experience, among others that are not relevant for purposes of digital lending.[490]

International Data Transfer

The lending apps studied transfer users' data to jurisdictions outside Zimbabwe. Apps such as GetBucks, for example, transfer personal user data to jurisdictions that have less stringent data protection laws.[491] This transfer poses a significant risk to the users' data security.

The apps should ensure that personal data transferred outside the country is protected. In doing this, they should set up appropriate safeguards to protect the data and ensure that data is transferred to jurisdictions with adequate data protection laws.

---

486 GetBucks Privacy Policy https://zw.getbucks.com/site-policy
487 MyBucks Privacy Policy: Clause 10 https://corporate.mybucks.com/privacy
488 Privacy International - pg 39
489 Data Minimization Report - pg.4
490 MyBucks Privacy Policy: Clause 3 'Use of Personal Data' https://corporate.mybucks.com/privacy
491 GetBucks Privacy Policy: Transfer Across Borders https://zw.getbucks.com/site-policy

Sharing of User Data with Third Parties

Digital lending apps should indicate to users the third parties they intend to share their data. They should make it clear in their policies the data they intend to share with the third parties, the duration of access to the data by the third parties, and the security measures put in place to protect the data shared with third parties.

The apps studied fail to indicate these in their privacy policies. Getbucks only displays the third parties they share information with and no information on the data shared with the third parties, duration of access or security measures.[492] MyBucks, on the other hand, does not clearly state the third parties with whom they share information.[493] eShagi lacks a privacy policy leaving users with no information on third parties who access their data.

Retention of User Data

The apps in this study do not indicate the parameters they use to determine how long they will store a user's data. They also do not show users the precise period they will keep their data. This information is critical to users of the apps to help them know how long the apps will have access to their data and what avenues they can use to remove their data from the apps.

492 GetBucks Privacy Policy: Disclosure Clause https://zw.getbucks.com/site-policy
493 MyBucks Privacy Policy https://corporate.mybucks.com/privacy

Conclusion

It is no secret that digital financial applications have improved and increased the penetration of banking facilities, particularly to rural parts of African countries. This support to the financial sector appears to be a Greek gift as the digital applications collect large amounts of [personal data without clarity on its handling, and the regulators seem to be overwhelmed or clueless on how to control collection and usage.

While countries have enacted data protection laws, financial technology companies have found ways of working around this to obtain personally identifiable information. Many digital applications, including those offering cryptocurrencies, have not granted users full access to modifying or erasing their data when they no longer need or use the applications. The digital contracts from these mobile applications appear to have a lifetime hold over users' personal data except a few.

In pioneer regulatory savvy countries like Cape Verde, the financial sector is monitored heavily on handling consumers' data. However, this has not stopped the misuse of this data as there is vagueness on how much regulatory control the Data protection agency has over digital applications. It has now become critical for laws to express clarity and details on;

Whether digital financial applications are subject to the same rules as traditional banks
The regulatory framework is needed to support and safeguard user data from the ever-growing and innovative financial technology sector.