GSMA

April 2024

Cross-border data flows:
Impact of data localisation on mobile money services in Africa and Asia

GSMA

The GSMA is a global organisation unifying the mobile ecosystem to discover, develop and deliver innovation foundational to positive business environments and societal change. Our vision is to unlock the full power of connectivity so that people, industry and society thrive. Representing mobile operators and organisations across the mobile ecosystem and adjacent industries, the GSMA delivers for its members across three broad pillars: Connectivity for Good, Industry Services and Solutions and Outreach. This activity includes advancing policy, tackling today's biggest societal challenges, underpinning the technology and interoperability that make mobile work and providing the world's largest platform to convene the mobile ecosystem at the MWC and M360 series of events.

We invite you to find out more at gsma.com

Follow the GSMA on Twitter/X: @GSMA

GSMA Mobile Money

The GSMA Mobile Money programme works to accelerate the development of the mobile money ecosystem for the underserved.

For more information, please contact us:

www.gsma.com/mobilemoney

mobilemoney@gsma.com

@GSMAMobileMoney

BILL & MELINDA GATES foundation

The Mobile Money programme is supported by the Bill & Melinda Gates Foundation.

Authors

Mercy Kingori – Tech Hive Advisory Africa
Dr. Opeyemi Kolawole - Tech Hive Advisory Africa
Deji Sarumi - Tech Hive Advisory Africa
Dorcas Tsebee - Tech Hive Advisory Africa
Adedolapo Evelyn Adegoroye - Tech Hive Advisory Africa
Mary Gichuki - Advocacy Manager, Mobile Money - GSMA

Contributors

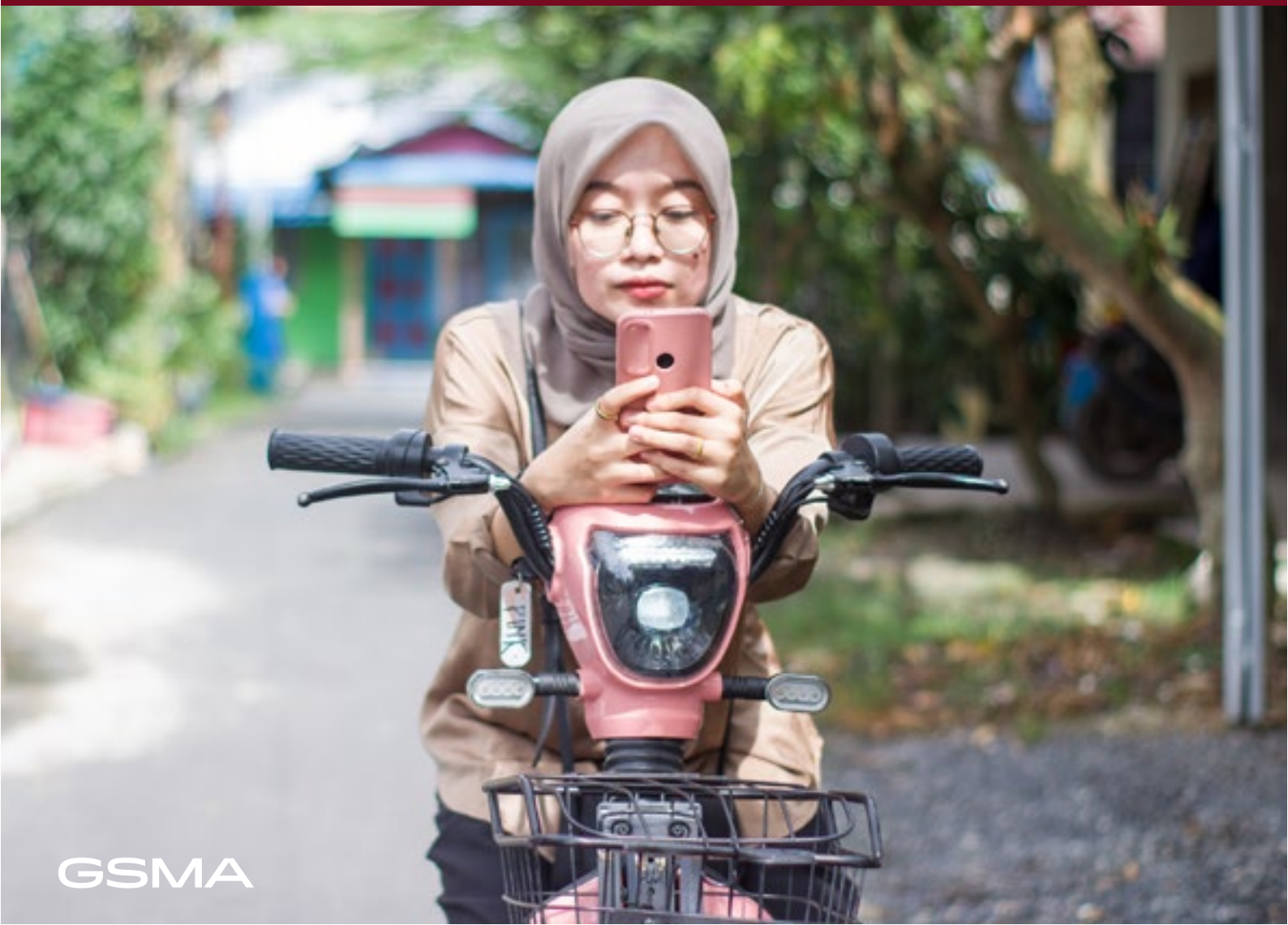
GSMA Public Policy team

Published April 2024

Contents

1

Executive summary



GSMA

In 2023, mobile money grew significantly in Africa and Asia, reaching $1.40 trillion in transactions.[1]

The substantial growth of mobile money in Africa and Asia can be attributed to a variety of factors. Firstly, there has been a notable increase in awareness of the advantages of mobile money. In both regions, it is increasingly recognised as a secure and convenient method for conducting financial transactions and storing currency. Moreover, there has been a significant evolution in the mobile money infrastructure itself. What initially began as rudimentary USSD-based applications has since transformed into sophisticated digital platforms accessible via mobile applications, catering to a wider audience and offering enhanced functionality. Furthermore, the scope of mobile money services has expanded considerably. Initially confined to peer-to-peer transfers, mobile money now encompasses a diverse array of products and services including e-commerce, e-health, insurance, savings, credit facilities, and international money transfers. This growth is further fuelled by the broader trend towards digitalisation in the economic landscape, underlining the increasing importance of mobile money in facilitating digital transactions. Supporting this expansion are favourable regulatory environments that have encouraged innovation and investment in mobile money infrastructure. Lastly, there is a concerted effort towards fostering financial inclusion, particularly among underserved communities. Mobile money plays a crucial role in this respect, providing access to financial services for individuals who were previously excluded from the traditional banking system.

The increased use of mobile money has led to more collaboration between various institutions and mobile money operators, resulting in operators gaining further access to customers' personal data, sometimes across borders. Cross-border data transfers play an important role in the growth of mobile money as we explain in this report. They support regulatory compliance and fraud risk mitigation, facilitate business expansion, and stimulate innovation within the industry.

Despite the evident advantages of cross-border data transfers, regulators have adopted varying approaches to its regulation. Countries in Africa and Asia are accelerating efforts to control data produced within their borders through the implementation of various data localisation laws, raising concerns about its impact on digital services, including mobile money. Restrictions on cross-border data transfers create significant operational challenges for mobile money operators. They also create significant trade barriers, limiting effective participation in regional and global digital trade.

In markets where data localisation regulations have been imposed, regulators and policymakers have provided several justifications for these requirements, including concerns about national security, data protection and privacy, and the protection of national sovereignty.

Like other international businesses, mobile money operators want to be able to use and realise the efficiencies of centralisation and virtualisation. However, due to data localisation mandates, information produced from individual transactions may be constrained by limitations on data transfers, sector-specific rules, or licensing requirements. This prevents the transfer of such metadata outside the country and requires processing and storage within its borders instead.

Such restrictions put mobile money operators at a disadvantage compared to other organisations within the sector that do not have to comply with such requirements. They also result in higher costs for business operations and compliance, and create barriers to new players entering the market.

In order to drive informed cross-border data transfer policies aimed at supporting the continued growth of mobile money and other digital solutions in Africa and Asia, we conducted a thorough analysis of the current data localisation landscape across several countries where localisation measures are rising. This report provides insight into the justification and impact of the existing regulation and data localisation requirements. Based on information gathered through in-depth interviews with mobile money operators and regulators in the identified countries, the report analyses the impact of data localisation requirements on mobile money services in Africa and Asia and provides recommendations on how to address them.

Countries in Africa and Asia are accelerating efforts to control data produced within their borders through the implementation of various data localisation laws, raising concerns about its impact on digital services, including mobile money

[1] GSMA State of the Industry Report on Mobile Money 2023

2

Methodology

GSMA

The methodology provides a nuanced understanding of the subject as derived from sixteen distinct markets: eleven in Africa and five in Asia.[2] Markets were selected based on their unique insights into diverse and mandatory data localisation models, the maturity of mobile money within these regions, and the existing state of relevant laws.

This report focuses on eight of these markets: five in Africa and three in Asia.[3] The research began with an extensive review of existing literature, market reports, regulatory documents, and other policy papers. The desktop research provided a foundation for understanding the current state of the market, mobile money adoption rates, user demographics, and other key data and information relevant for shaping the subsequent inquiry.

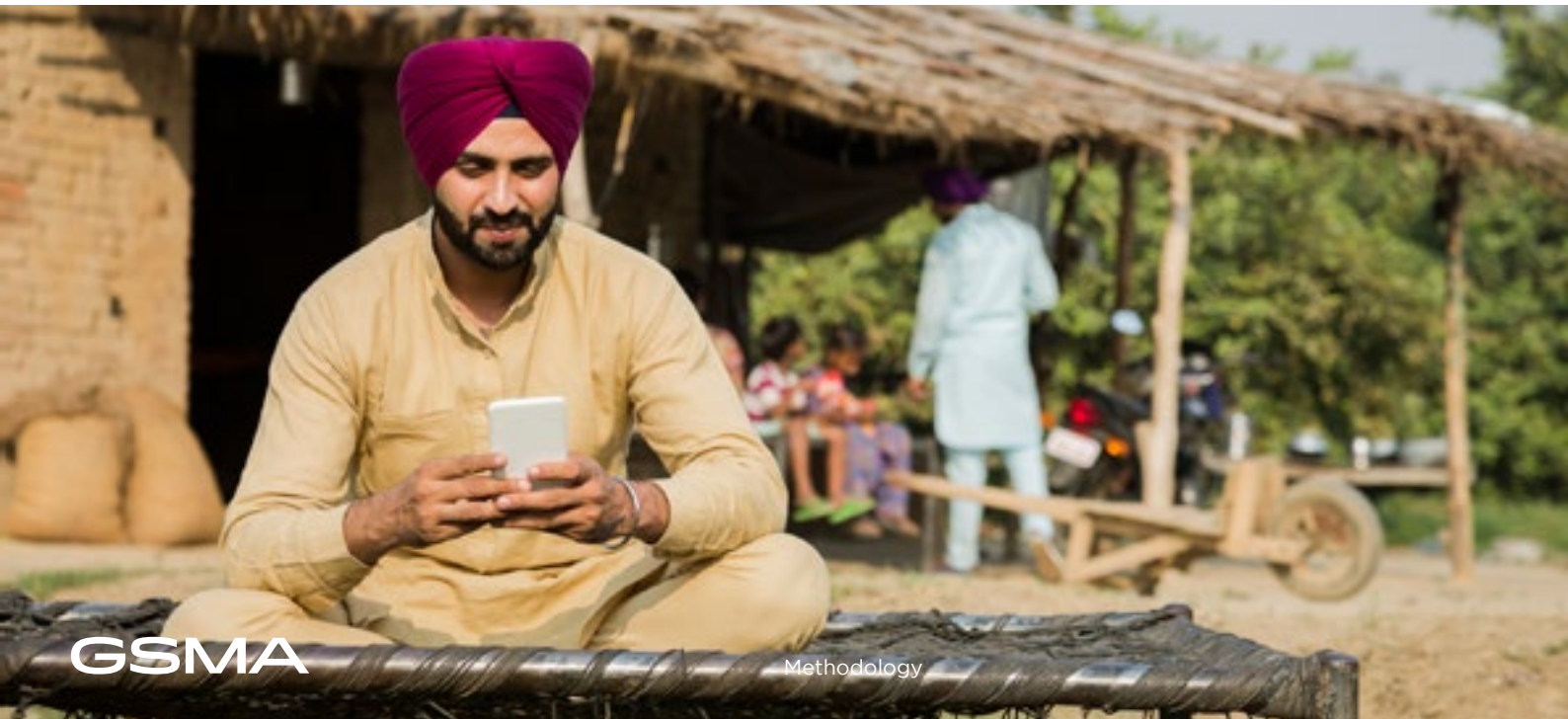
In-depth interviews were then conducted with both mobile money operators and regulatory authorities. Conversations with operators helped uncover market realities in selected countries, providing industry-specific insights into the effects of data localisation laws and restrictive cross-border data transfer rules. These discussions also initiated conversations about introducing alternative models for data transfers. On the other hand, regulator interviews clarified – and provided insight into the rationale behind – cross-border data transfer restriction laws in relevant mobile money markets. Structured questionnaires further complemented these qualitative insights, enabling a more quantifiable understanding of the perspectives, challenges, and trends of cross-border data transfer and its impact on mobile money.

These were carefully designed to extract information that could be translated into actionable insights for the industry.

Visual representations are employed to make complex data more understandable. These visual aids depict the regulatory landscape, and specific impacts highlighted from discussions with operators, making the information more accessible to a non-academic audience. Ethical considerations were paramount throughout the research process. All activities conducted contained measures to ensure the confidentiality of respondents, and permission was obtained for all interactions.

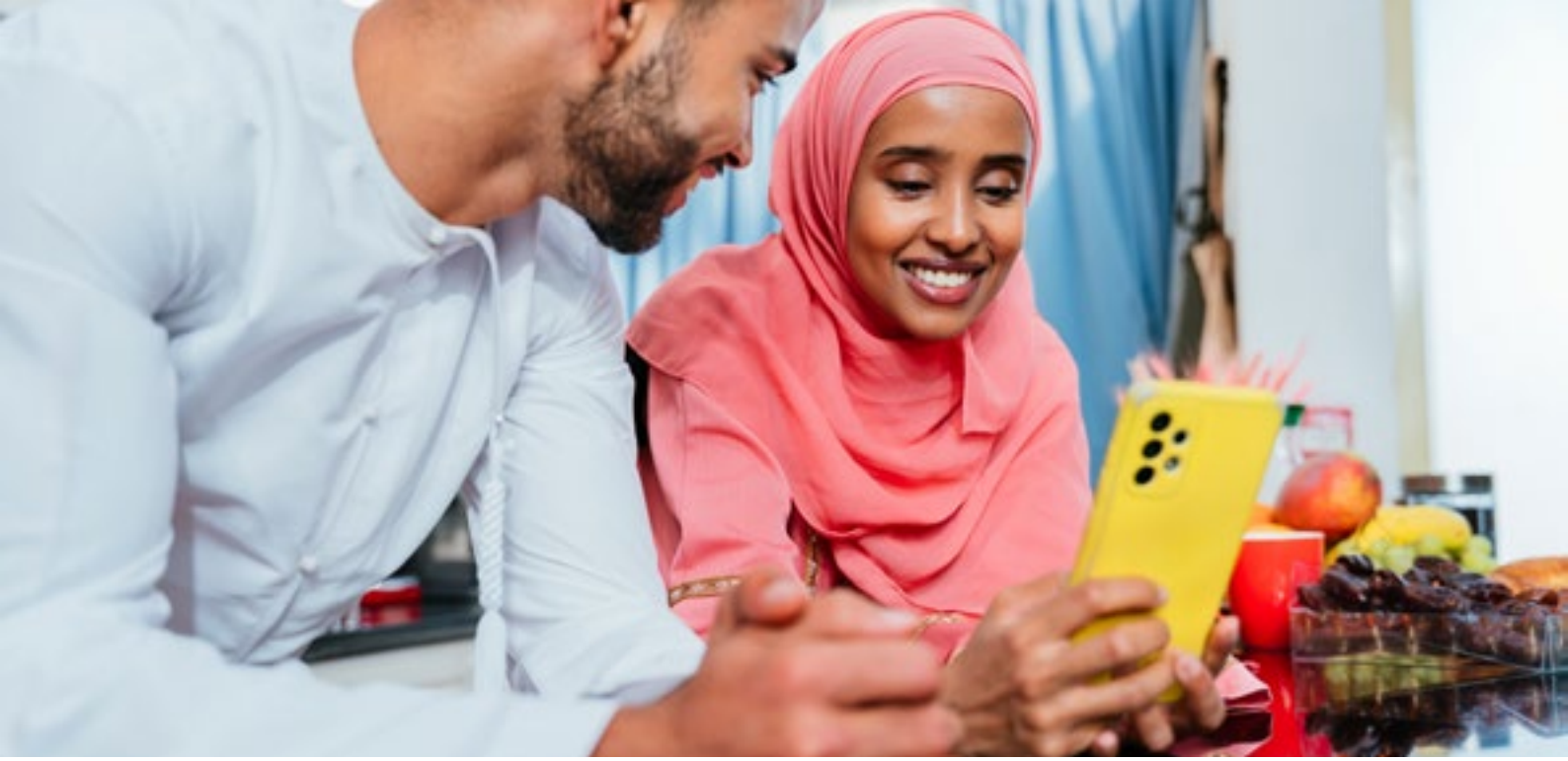
The study was mindful of potential limitations and assumptions inherent in the research. Acknowledging potential biases in the responses and the dynamic nature of regulatory environments provided a more balanced perspective and allowed for a more critical assessment of the findings. The methodology adopted in this study provides a comprehensive insight into the complex interplay between cross-border data transfer and the mobile money sector in the selected markets.

[2] Indonesia, Kenya, Uganda, Singapore, Ghana, Zambia, Cameroon, Republic of Congo, Rwanda, Ethiopia, Nigeria, Tanzania, Zimbabwe, Bangladesh, Indonesia, Pakistan
[3] Rwanda, Ethiopia, Nigeria, Tanzania, Zimbabwe, Bangladesh, Indonesia, Pakistan



3

Introduction



A thriving mobile money ecosystem provides social and economic gains to its networks of users and society at large.

Growing adoption, usage, transaction value, mobile money agent networks, international money transfer, and preference for mobile money services as a savings channel among the unbanked are all signs of a flourishing ecosystem. Diversification of mobile money-based services is alleviating the need for physical handling of money - allowing both small and large-scale businesses to operate digitally, and driving a need for interoperability with other services and payment platforms.

The upward trend in adoption of mobile money services has also been enabled by the secure flow of data across borders as mobile money operators expand into new geographies. This has resulted in the need to use infrastructure, such as international cloud services, to increase efficiency, enhance system security, lower operating costs, and enhance service delivery.

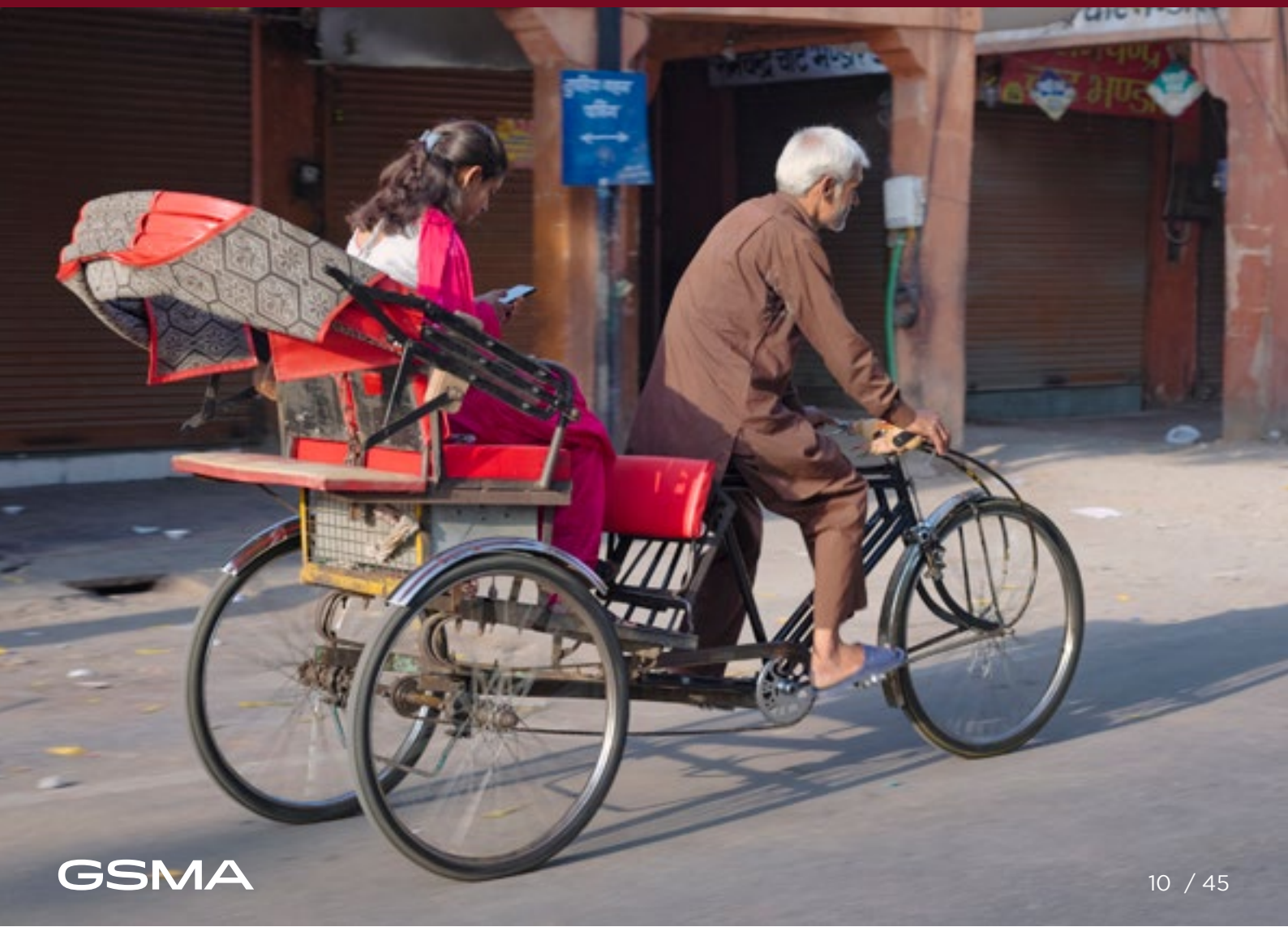
However, in some countries, there is also a trend towards restricting cross-border data flows. This poses a significant threat to the continued growth and innovation of mobile money services.

This report aims to provide a clear view of the impact of data localisation on mobile money in Rwanda, Zimbabwe, Indonesia, Bangladesh, Nigeria, Ethiopia, Tanzania, and Pakistan. It compares the localisation requirements outlined in law, taking into account the actual experiences of operators and regulators.

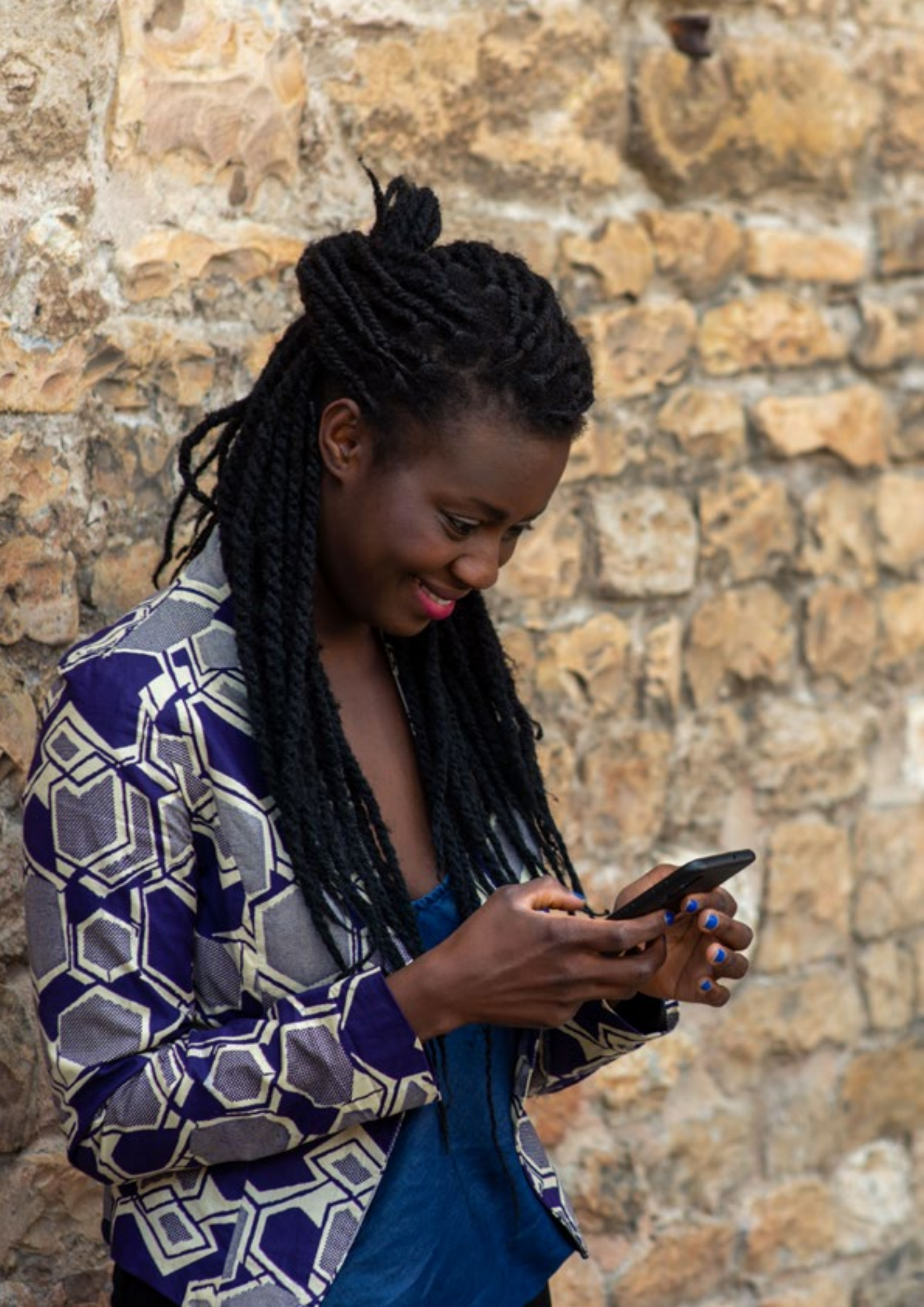
It begins with an assessment of the regulatory environment for these countries and then provides a detailed description and analysis of the current data protection laws, industry-specific regulations, and guidelines for cross-border data transfers and national data localisation rules. The impact of mandatory data localisation provisions is also examined. This includes insights from mobile money operators and regulators on the challenges and opportunities presented by these laws. The concluding section summarises the study's main findings and provides concrete recommendations for mobile money operators, policymakers, and regulators designed to advance the growth of mobile money. It presents strategies to navigate the complexities of data localisation laws while advancing the mobile money industry.

4

Mobile money regulatory landscape and cross-border data transfer rules



Country profiles				
Country	**Existence of data protection law**	**Existence of a data protection authority**	**Other relevant market regulators**	**Data localisation rules**
Rwanda	Privacy and Data Protection Law 2021	Data Protection and Privacy Office National Cyber Security Authority (NCSA)	National Bank of Rwanda (BNR)	**Restrictive** Data transfers are subject to prior authorisation from the data protection authority
Ethiopia	No	No	National Bank of Ethiopia (NBE) Ministry of Innovation and Technology	**Restrictive** Although no data protection law or authority exists, the existing legal framework mandates data storage within Ethiopia
Nigeria	Nigeria Data Protection Act, 2023 Nigeria Data Protection Regulation, 2019 NDPR Implementation Framework, 2020	Nigerian Data Protection Commission (NDPC)	Central Bank of Nigeria (CBN)	**Restrictive** Cross-border data transfer is prohibited unless certain conditions are met
Tanzania	Personal Data Protection Act, 2022	Personal Data Protection Commission	The Bank of Tanzania w	**Restrictive** The data protection law restricts the transfer of personal data outside Tanzania
Zimbabwe	Data Protection Act, 2021	Postal and Telecommunications Regulatory Authority of Zimbabwe	Reserve Bank of Zimbabwe	**Non-restrictive** Data may not be transferred to another country unless it meets the requirements under the law
Bangladesh	No	No	The Bangladesh Bank	**Restrictive** There are provisions in the laws that restrict the transfer of data outside Bangladesh without approval
Indonesia	Data Protection Act, 2022	No	Bank of Indonesia, Indonesian Financial Service Authority	**Restrictive** Data transfer is subject to safeguards put in place by the operators and authorisation from the authorities
Pakistan	No	No	State Bank of Pakistan (SBP) Ministry of Information Technology and Telecommunication	**Restrictive** Data localisation is regulated, and transfer outside the country is restricted



Rwanda

The National Bank of Rwanda (BNR) is the primary regulator of mobile money services in the country, and it has put in place a number of guidelines and requirements that mobile money operators must adhere to the obligations under the **Payment System Law of 2021**. In 2018, the BNR introduced regulations (amended in 2023) that require mobile money operators to obtain licenses in order to operate in the country. The regulations also require operators to maintain a minimum level of capital and comply with anti-money laundering and counter-terrorism financing measures and data protection. The BNR also encourages collaboration between mobile money operators and other financial institutions, such as banks, in order to promote interoperability and expand the reach of mobile money services.

The rules on data protection, data localisation, and cross-border transfer in Rwanda derives from the Rwandan Constitution, particularly Article 22, which guarantees and protects Rwandans' right to privacy. On 13 October 2021 Rwanda adopted its first data protection law: No. 058/2021. This law provides a comprehensive legal framework for regulating and protecting personal data, especially how it is processed and stored and, most importantly, the conditions that must be fulfilled before personal data are transferred outside Rwanda.

Articles 48 and 49 of the Privacy and Data Protection Act prescribe rules, conditions and precedents for international data transfers. From these provisions, it is evident that any international or cross-border transfer of personal data is subject to regulations adopted and enforced by the supervisory authority, which in this case is the National Cyber Security Authority (NCSA). The framing of Section 48 (1) suggests that it is not enough for a data controller or processor to show that it has implemented "appropriate safeguards concerning personal data protection". The relevant controller or processor must also obtain authorisation from the supervisory authority after providing proof of appropriate safeguards with respect to the protection of personal data.

Other conditions stipulated for cross-border data transfers in Article 48 are elementary, and most data controllers or processors, like mobile money operators, should be able to fulfil such requirements. For instance, the relevant data subjects must have given their consent before the cross-border data transfer occurs; the data controller or processor can also transfer for legitimate purposes, on public interest grounds, and on other grounds captured in Article 48 (3) (a–g). However, the conditions in Article 48 are cumulative. Therefore, seeking the data subject's consent or using any of the conditions in Article 48 (3) does not necessarily give a data controller the right to transfer personal data outside Rwanda. Article 49 stipulates that the data protection regulator may, via regulation, determine the form of the contract to be used for transfers of personal data outside Rwanda. The section goes further to stipulate that the supervisory authority may require the data controller or the data processor to demonstrate their compliance with the provisions of this Article, in particular with personal data security safeguards and interests referred to in Item 3° (f) of Article 48 of this law. Ultimately, cross-border data transfers depend on the ability of the data controller, in this case, a mobile money operator, to secure prior authorisation and hold a valid registration certificate from the NCSA.

Failure to comply with the provisions of the law is an offence under Article 56. Although the broad regulatory and prosecutorial power of the supervisory authority reflects the Rwandan government's commitment to upholding the constitutional guarantee of the right to privacy, the broad discretion afforded to the supervisory authority and the rigorous registration and approval procedure for authorisation may create significant operational challenges for new entrants into the mobile money services sector.

At a practical level, the government has taken steps to encourage the establishment of cloud services and has facilitated the licensing of private cloud hosting service providers like Microsoft. Nevertheless, financial services institutions are required to obtain approval before engaging private cloud hosting service providers.

Ethiopia

The expansion of mobile money services in Ethiopia still faces hurdles, particularly regarding rules and regulations restricting cross-border data transfer. Two critical directives pertain to mobile money operators and their data management practices. The Licensing and Authorization of Payments System Operators Directive,[4] particularly in paragraph 12 (2) (f), requires payment system operators to maintain the confidentiality of information about their service, which might have been outsourced to third parties. They must also keep an electronic record of all payment transactions in compliance with data archiving laws. The Directive does not refer to a specific data archiving law, as Ethiopia does not have one yet. However, paragraph 7.1 of the Financial Consumer Protection Directive of Ethiopia might be instructive, as it stipulates that financial services providers retain records relevant to their operations, products, and services for ten years or as required by law.[5]

Furthermore, any licensed gateway operator, including a mobile money operator, under paragraphs 13.5(e) and (f), shall not store customer data on a merchant's website or any e-commerce platform. The operator is also barred from storing customers' payment and account data on its server.[6] These provisions could have an effect on data flows for a mobile money operator that relies on infrastructure outside of Ethiopia.[7]

Notably, the Communications Consumer Rights and Protection Directive, which addresses broader consumer issues, including those associated with mobile money operations, requires consumers' personal data to be processed only within servers or data centres in Ethiopia.

Currently, there is no central legal framework for data protection or a national data protection authority, but the Ministry of Innovation and Technology (formerly known as the Ministry of Communication and Information Technology) issued a Draft Data Protection Proclamation in 2021. In 2023, the Council of Ministers approved the Draft Proclamation for parliamentary ratification.[8] It establishes a Data Protection Commission and contains data sovereignty clauses requiring the storage of personal data on a server or data centre located in Ethiopia.[9] Under the Proclamation, cross-border transfer of sensitive personal data also requires prior approval of the commission.[10] In the absence of a comprehensive data protection and localisation framework, there may be challenges in enforcing these requirements and addressing potential data breaches effectively.

The current disposition likely reflects the Ethiopian government's initial policy to protect existing state-backed entities and exclude foreign entities from operating in the mobile money sector. However, this direction of policy may change as the Ethiopian government pursues its market liberalisation objectives. Indeed, the liberalisation efforts are beginning to yield ample results, with M-PESA setting up shop in Ethiopia.[11]

The current disposition likely reflects the Ethiopian government's initial policy to protect existing state-backed entities and exclude foreign entities from operating in the mobile money sector

[6] Ibid, paragraph 18.2(d)
[7] Telecommunications Consumer Rights and Protection Directive No. 832/202
[8] https://ethiopianmonitor.com/2023/10/27/ethiopia-prepares-first-personal-data-protection-law/
[9] Proclamation to provide for personal data protection
[10] Section 31
[11] Hellen Githaiga, (2023) Ethiopia Grants Safaricom M-pesa License (Business Daily:2023)

Nigeria

Mobile money operations in Nigeria are regulated by the Central Bank of Nigeria (CBN) under the Banks and Other Financial Institutions Act (BOFIA), the principal financial services legislation.The CBN has issued various guidelines and regulations that govern mobile money service provision in Nigeria and provide different obligations for ensuring security and data protection.[12] The CBN's Exposure Draft of the Operational Guidelines for Open Banking 2022[13] provides a regulatory framework for data exchange among financial services participants, including mobile money operators.[14] The guidelines prohibit the disclosure of data to a non-Nigerian unless approved by the CBN. Before additional data can be disclosed, the CBN may require further information, such as a statement indicating how the data is disclosed, specific details about the data handling and privacy policy of the service provider, and a guarantee that customers can obtain further information about such disclosures from the policy or upon request from the participant, if desired.[15] The implication of this provision is that customer data is originally required to be kept within the country and not disclosed to an external entity unless these conditions have been met.

Additional regulations that apply to mobile money operators concerning cross-border data transfers include the recently enacted Nigeria Data Protection Act, 2023 (NDPA), the Nigeria Data Protection Regulations, 2019 (NDPR) and its Implementation Framework, 2020 (IF). The NDPR and IF, as the earliest regulatory regimes on data protection and cross-border data transfers, apply to the extent that their provisions are consistent with the NDPA, which is now the country's primary legislation on data protection.[16] The NDPA sets out the requirements for collecting and storing data in and out of Nigeria and stipulates several conditions to be met before transferring personal data out the country.

The Nigerian Data Protection Commission (NDPC) is mandated to determine whether the receiving country has an adequate level of protection for the data, which may take time and, hence, slow down operations for mobile money operators. This responsibility previously fell under the supervision of the Honourable Attorney General of the Federation (HAGF) and the National Information Technology Development Agency. However, since the enactment of the NDPA, it is solely vested with the NDPC.

According to the regulator, data will be transferred when Nigeria has issued an adequacy decision to the receiving country, with a few exceptions. Nigeria has yet to publish a new list of adequate countries to which data can be transferred, apart from the list issued on June 25, 2021, by the previous regulator, NITDA, when it oversaw data protection under the NDPR and the IF.[17] Until recently, the list continued to be in operation by virtue of Section 64 of the NDPA, which provides that all documents that were in effect before the coming of the NDPA shall continue to be in force as if the NDPC issued them until they are altered. However, the position has now changed following a decision of the Federal High Court invalidating the "whitelist" of countries for data transfer since some of the countries on the list did not provide adequate protection for personal data as required under the NDPR.[18] The court directed the regulator to review the list of countries to comply with the law. The implication of this judgement is that the list is no longer valid for purposes of international data transfer until the NDPC reviews it.

[12] Guidelines on Mobile Money Services, Regulatory Framework for Mobile Money Services in Nigeria, and Guidelines for Licensing and Regulation of Payment Service Banks
[13] Operational Guidelines for Open Banking in Nigeria
[14] Ibid.
[15] Article 11. 1.1
[16] Section 63, Nigeria Data Protection Act 2023
[17] NDPR Implementation Framework 2020
[18] 'Changing Trend in International Data Transfer in Nigeria: Reassessing the "adequacy of the Whitelist" and the Implications for Businesses' <https://www.linkedin.com/pulse/changing-trend-international-data-transfer-nigeria-zffuf> accessed 27 December 2023

In addition, relying on consent as a basis for transfer may pose challenges for mobile money operators due to the number of subscribers and the burden of establishing consent, and regulators generally dissuade data controllers from adopting this mechanism as it may be difficult to establish informed consent.

The NDPA contains other mechanisms like binding corporate rules, contractual clauses, certification mechanisms, and codes of conduct that mobile money operators can use during cross-border data transfers. However, there are restrictions on using these mechanisms, which require parliamentary approval before they can be recognised as lawful. Overall, the regulator maintains that establishing the lawful basis for transfers must be compliant with Nigeria's data protection principles, and this could ultimately earn the regulator's approval for cross-border data transfers. The receiving country's data protection and security standards must also be demonstrated.

Nigeria has launched its National Data Strategy, clarifying the country's position on cross-border data transfers.[19] The third pillar of the National Data Strategy emphasises mandatory localisation and residency of data as part of the country's data strategy. According to this pillar, residency and localisation of data are subject to Nigeria's national laws and regulations. This means that data collected in Nigeria and from Nigerians within or outside the country is subject to all relevant laws, rules, and regulations governing the use of data in Nigeria. The strategy aligns with existing laws, such as the NDPA, whose provisions lean more towards exercising sovereignty over data location by placing stringent requirements for cross-border data transfer. The Nigerian Government has officially launched the National Data Strategy.[20]

[19] NITDA, National Data Strategy Final Draft of National Data Strategy for Nigeria
[20] Rukayyat Sadauki, (2023) NITDA unveils National Data Strategy to drive Nigeria's Digital Economy

Tanzania

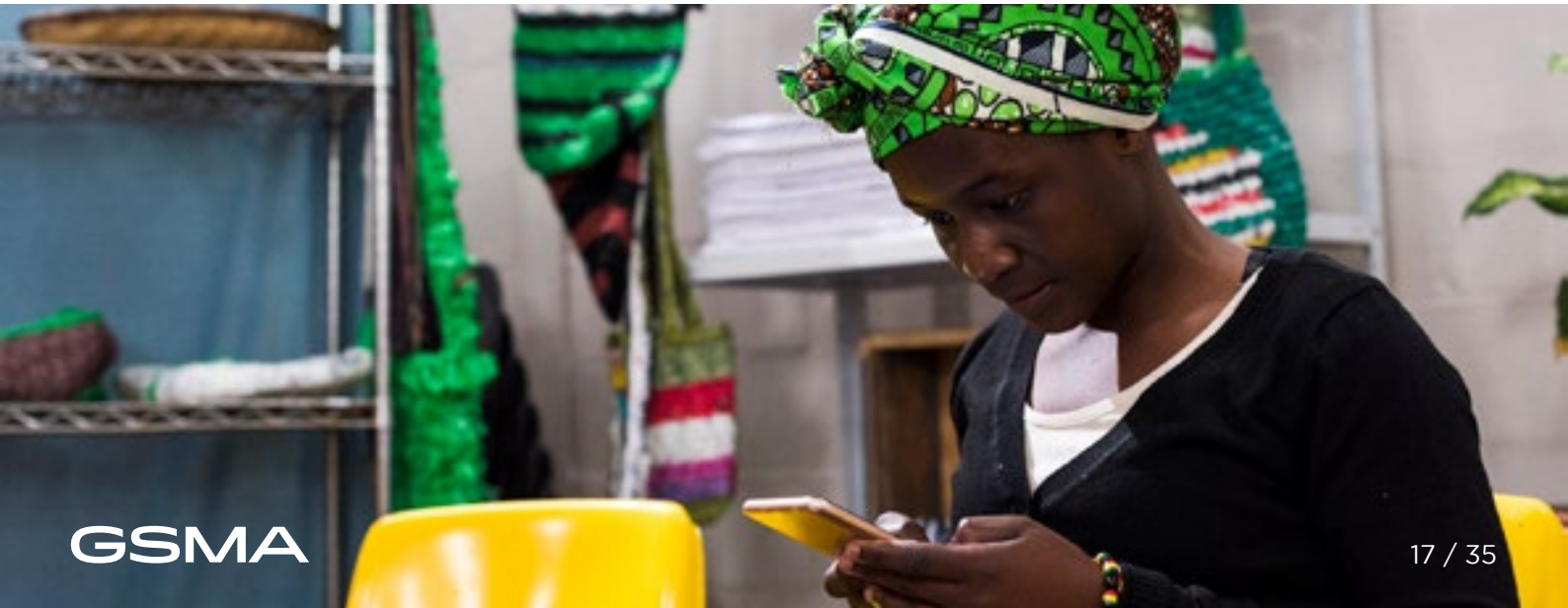
The Bank of Tanzania regulates mobile money operations in Tanzania. The Bank regulates the sector through the Banking and Financial Institutions Act of 2006.[21] The Act covers the licensing and regulation of banks and financial institutions operating in the country, including mobile money operators.[22]

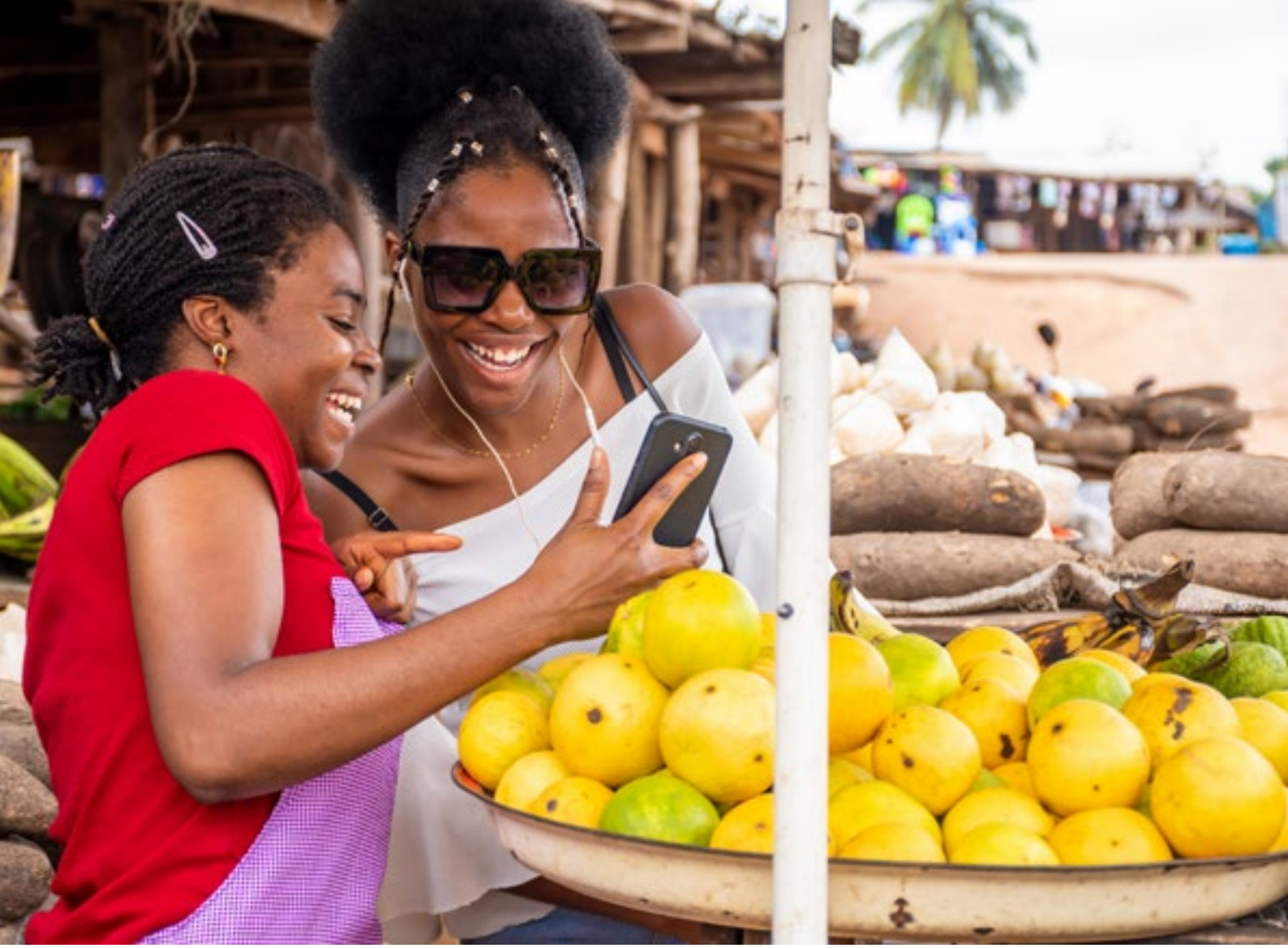
While regulatory interventions have been crucial to mobile money adoption, they are undermined by legal frameworks that seek to impose data localisation requirements on entities that process data, including mobile money operators. The National Payment Systems Act 2015, which regulates and supervises payment systems, including those of mobile money operators in the country, does not take into account cross-border data transfers. However, Regulation 42 of the Payment Systems (Licensing and Approval) Regulations of 2015 mandates payment system providers to place their primary data centre in Tanzania.[23] Further, the Regulations (46 and 47) prohibit payment system providers from operating cross-border payment system services, opening a branch in or outside the country, or creating a subsidiary without written approval from the Central Bank.[24] Operators must, therefore, store data in Tanzania and will only transfer such data outside with written approval from the Bank.

Cross-border data transfer is also regulated by the new Personal Data Protection Commission. The Commission was established under the Personal Data Protection Act 2022 to oversee data protection in Tanzania. The Act, the main framework for data collection, processing, and transmission in Tanzania, provides conditions for data transfers out of the country.[25] The Personal Data Protection Commission maintains wide discretion over transfers under the Act. Without robust guidance for outward data transfers, these conditions could restrict data transfers in practice. Requirements such as the obligation to conduct a transfer impact assessment and validate the significance of a transfer could potentially restrict the free flow of data out of the country.[26]

Additionally, the Finance Act of 2021 mandates that tax-related data be stored on a primary server located in Tanzania[27] and makes it an offence to store such data outside the country.[28] A primary data server is "a server that stores data created or collected by a taxable or liable person in the ordinary course of business."[29] This would include mobile money operators in their capacity as tax taxpayers in the country of operation.

[21] Banking and Financial Institutions Act 2006
[22] Section 4 (1) BAFIA 2006
[23] Payment Systems (Licensing and Approval) Regulations of 2015
[24] Regulation 46 ibid
[25] https://www.parliament.go.tz/polis/uploads/bills/1664436755-document%20(38).pdf) Section 31 of the Act
[26] Personal Data Protection Act 2022, Act No. 11 of 2022, Section 31 (3), (4) and (5)
[27] Section 57 which amended Section 35 of the Tax Administration Act, requires every taxable person or liable person who maintains documents in electronic form, to maintain in the United Republic a primary data server for the storage of documents in electronic form
[28] Section 65, which amends Section 85 of the Tax Administration Act, stipulates that failure to maintain a primary data server in the United Republic as required by Section 35 constitutes an offence
[29] Section 57(9) Finance Act 2021





The Outsourcing Guidelines for Banks and Financial Institutions, 2021, which applies to all outsourcing arrangements entered into by banks and financial institutions and includes non-strategic but material services, makes further restrictions on cross-border data flows.[30] The Guidelines prohibit banks and financial institutions from outsourcing their primary data centres outside the country. In recognition of the role of technology in developing the country's economy and the mandate to ensure the safe deployment of such technology, the Central Bank provides the necessary guidelines to regulate the transfer of data to cloud facilities in another country. However, there are restrictions on such operations. The Central Bank examines the technology and determines if it is critical security information, in which case it must be retained in Tanzania. In any other case, the data can be hosted in another country's cloud facilities.

The Draft Cloud Computing Guidelines for Financial Service Providers (2023) stipulate that in line with Guideline 10(g) of the Outsourcing Guidelines for Banks and Financial Institutions, financial service providers shall not host in a primary data centre outside Tanzania any mission-critical system or any other system whose data are considered critical for the operations of an institution. The restriction is limited to information the regulator finds critical for the company's business. This limits regional-based institutions wanting to leverage regional cloud solutions for their operations. It also means entities have to seek multiple regulatory approvals, adding another layer of compliance.

While this reflects the need for the regulator to ensure that leveraging data centres outside Tanzania doesn't compromise service delivery or the systems, the focus should be on ensuring proper system and service delivery safeguards are in place.

[30] Guideline 10(g) of the Guidelines

Zimbabwe

The legal instruments governing cross-border data transfers in Zimbabwe that affect mobile money operations include the Data Protection Act of 2021 and Postal and Telecommunications (Subscriber Registration) Regulations of 2014, as amended by Statutory Instrument 250 of 2019. The Data Protection Act deals with the general rules on processing personal data within Zimbabwe, including cross-border data transfers. The Act maintains a conditional transfer regime that mobile money operators must comply with to ensure the lawful transfer of personal data out of the country. Section 28(3) grants the Data Protection Authority and the Minister responsible for Cybersecurity discretionary powers to determine the circumstances in which data transfer to countries outside Zimbabwe are not authorised. As seen in Rwanda, Ethiopia, and Tanzania, regulators wield extensive discretionary powers, which could potentially result in the decision to localise data for mobile money operations. This arises from the ambiguity and uncertainty surrounding the specific requirements that need to be fulfilled.

Section 11 of the Postal and Telecommunications (Subscriber Registration) Regulations of 2014, as amended by Statutory Instrument 250 of 2019,[31] addresses the technical aspects of data management. It outlines a comprehensive framework for mobile service providers to use data storage services, including cloud services hosted by foreign data storage hosts. It stipulates that if transferring subscriber information to a foreign host becomes necessary or unavoidable for operational access to the data storage services, the service provider must ensure the data is encrypted in a way that prevents reading by the foreign host. The local service provider must retain the encryption keys to prevent unauthorised access, submit a report on data protection measures and hosting agreements to the authority before entering the storage arrangement, obtain clear affirmative consent in writing from the subscriber for the transfer of personal data, and refrain from selling, trading, or sharing the transferred data.

The importance of this provision for mobile money operators is that they may carry out data transfers in circumstances where it is necessary or will aid their operations, provided they follow the rules as determined by the law for carrying out the transaction. Generally, from a regulatory point of view, regulators maintain that although the framework for data transfers is not restrictive, approvals for data transfers are considered on a case-by-case basis. They maintain that it is essential to consider data transfers on a case-by-case basis to analyse each transfer's risk level and necessity. This equates to a hybrid approach that promotes both localising data and permitting data transfers where there is a need to do so. The regulatory regime for mobile money operations in Zimbabwe is quite sector-specific; however, the Reserve Bank of Zimbabwe and the Postal and Telecommunications Regulatory Authority of Zimbabwe, which oversee data protection authority in the country, have adopted a collaborative approach, formalised through signed Memoranda of Understanding, to jointly shape regulations and extend specific approvals or licenses to operators. Additionally, due to the newness of the Data Protection Act and regulatory authority for data protection, we anticipate that the regulator will develop further guidelines to support and eventually shape the regime for cross-border data transfer in Zimbabwe.

As seen in Rwanda, Ethiopia, and Tanzania, regulators wield extensive discretionary powers, which could potentially result in the decision to localise data for mobile money operations.

[31] Postal and Telecommunications (Subscriber Registration) (Amendment) Regulations, 2019

Bangladesh

Mobile money operations are exclusively regulated by the Bangladesh Bank. In 2022, the Bank adopted the latest Mobile Financial Services (MFS) Regulations, pursuant to Section 7A(e) and Section 82 of the Bangladesh Bank Order, 1972, and Section 26 of the Bank Companies Act, 1991. The new regulations aim to create a regulatory framework to sustain a competitive environment for mobile money services and promote affordability and accessibility, especially for the unbanked population.

It is important to note that the regulation provides for a bank-led model. Thus, telecommunications companies are excluded from providing the service. Paragraph 4.0 notes that "Bangladesh Bank will allow only scheduled commercial bank/financial institution/government entity-led MFS (Bank/FI/Government Entity-led MFS) in Bangladesh" to provide mobile money services.[32] With regard to cross-border transfers of data for mobile money operators, the regulation in paragraph 7.6 limits the operators from carrying out cross-border payments. The imposed limitation significantly hampers the capacity of mobile money operators to conduct cross-border payments, effectively undermining the essential requirement for a conducive framework that promotes seamless cross-border data transfers. This restriction prevents mobile money operators from engaging in cross-border payments, contradicting the purpose of establishing an environment supporting such cross-border data transfers.

The Information and Communication Technology Act 2006 and the Digital Security Act 2018 (amended in 2023) are the primary pieces of legislation relating to misuse of personal data, unfair disclosure, and breach of contractual terms in relation to personal information. On August 28, 2023, the Cabinet approved the new Cyber Security Act 2023 drafted to replace the Digital Security Act 2018.[33] There is no general restriction on data transfers outside Bangladesh, except as outlined in Section 26 of the Digital Security Act, which makes it an offence to supply (potentially including the transfer of) personal data without authority.[34] Additionally, Section 12 of the Bank Company Act 1991 ('the Bank Company Act') stipulates that banks specifically may only transfer records or documents relating to their business outside Bangladesh with the prior approval of the Central Bank.

Accompanying the ban on cross-border payments are proposals that may further restrict data transfers in Bangladesh. Section 42 of the proposed Data Protection Bill of 2022 requires that "sensitive data, user-created or generated data, and classified data be stored in Bangladesh." The framing of this provision makes room for broad interpretation, which may lead to restrictions on transferring any type of data to another jurisdiction or using public or private cloud hosting services. This could result in significant challenges for businesses and organisations operating in Bangladesh.

[32] Bangladesh Mobile Financial Services (MFS) Regulations, 2022
[33] 'Digital Security Act 2018 and the Draft Cyber Security Act 2023 : A Comparative Analysis' <https://ti-bangladesh.org/articles/position-paper/6752> accessed 2 January 2024
[34] Digital Security Act, 2018

Indonesia

Mobile money services in Indonesia are regulated by the Bank of Indonesia, which guides operators on transferring data generated during business activities. As in other countries discussed above, there are numerous such regulations in Indonesia. The country recently enacted its Data Protection Act, 2022 - before this, data protection in Indonesia fell under sector-specific laws. With regard to cross-border data transfers, the Act employs a conditional transfer regime that requires certain safeguards to be put in place before data is transferred out of Indonesia.[35] The Data Protection Act requires that an importing country's data protection law offer similar or higher protection than the Indonesian law, implement adequate and binding protection measures in the absence of an adequate regime, or obtain consent from a data subject. In addition, before transferring data, an entity must interface with the Directorate General for Informatics Applications within the Ministry of Communications and Informatics. While the law's data localisation provisions broadly exempt the financial services sector, they are provided for in other sector-specific laws with ramifications for the finance sector, including mobile money operations.

Several other legal frameworks impact mobile money service provision and impose data localisation requirements. Government Regulation No. 71 of 2019 on the Implementation of Electronic Systems and Transactions (GR 71)[36] and its implementing regulation, the Minister of Communications and Informatics (MOCI) Regulation No. 5 of 2020 regarding the Private Sector Electronic System Operator (ESO), impose localisation requirements for electronic system operators in Indonesia. Before the revised GR 71 was introduced,[37] the previous Regulation[38] made localising all "public service" data mandatory.

However, GR 71 distinguishes between private and public electronic system operators. Public electronic system operators are bound to process data within Indonesia, while private operators are exempt but could be compelled by sector-specific requirements. The definition of ESOs is broad, encompassing individual entities that provide, administer, and/or operate an electronic system for users. Mobile money operators thus fall within the ambit of this definition.

Due to the impact of sector-specific requirements on data localisation, Bank of Indonesia Regulation No. 23/6/PBI/2021 concerning Payment System Providers provides insight into such obligations for mobile money operators. It establishes a framework for payment systems, including the data processing requirements for payment system providers. Article 257 requires that data processing activities carried out through the Bank of Indonesia's infrastructure, which mobile money operators rely on, are conducted through the Bank of Indonesia's data infrastructure. Similarly, entities must seek authorisation from the Bank of Indonesia before using third-party data infrastructure.[39]

With regard to cross-border data transfers, the Act employs a conditional transfer regime that requires certain safeguards to be put in place before data is transferred out of Indonesia

[35] Indrawan Dwi Yuriutomo (2022) Indonesia Data Protection Overview
[36] Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions
[37] Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions
[38] Government Regulation Number 82 of 2012 regarding Electronic System and Transaction Implementation
[39] Article 257 of Bank Indonesia Regulation No. 23/6/PBI/2021 concerning Payment System Providers

The Banking Law and the Capital Market Law are other sector-specific laws impacting data transfers. They apply to both personal and corporate data and create a mandatory obligation for commercial banks to seek the approval of the Indonesian Financial Service Authority before establishing a data centre or storing data outside of Indonesia.[40]

By default, financial service institutions (FSIs) must use data centres and disaster recovery centres in Indonesia and carry out IT-based transaction processing in Indonesia. However, under certain specific circumstances, FSIs are allowed to place their electronic systems in data centres and/or disaster recovery centres outside of Indonesia as long as they obtain prior approval from the Indonesian Financial Services Authority. FSIs can place their electronic systems in data centres and/or disaster recovery centres outside of Indonesia if they are used for:

a. Supporting integrated analysis
b. Risk management of overseas-headquartered banks
c. AML/CTF functions of overseas-headquartered banks
d. Providing services to customers globally
e. Communication management between offices
f. Internal management, upon obtaining approval from the Indonesian Financial Service Authority

FSIs are allowed to conduct IT-based transaction processing outside of Indonesia if they attain prior approval from the Indonesian Financial Service Authority and demonstrate their attempt to develop the Indonesian economy. Therefore, the use of IT service providers outside the territory of Indonesia is restricted to certain scenarios and is subject to additional approval. In addition, payment transactions can be processed outside of the territory of Indonesia as long as prior approval has been obtained from the Bank of Indonesia.

Prior approval is also required for banks and non-bank institutions that provide payment services (including mobile payments, payments backend, point-of-sale (POS) payments, payments to and from customers, and consumer payments). Payment service providers are required to submit reports to Bank of Indonesia regularly on payment transaction processing.

The timeline of approval process varies but typically take about two to three months. Also, post-implementation notification to the Indonesian Financial Services Authority may be required one month from when outsourced activities commence following cloud implementation. Regulators in Indonesia support a comprehensive approach to data localisation as crucial to expanding the nation's technology market and assisting with law enforcement.

[40] (Article 35(2) and (3) of the Financial Services Authority Regulation No. 11/POJK.03/2022 on the Organisation of Information Technology by Commercial Banks)

Pakistan

Mobile money operations are regulated by the State Bank of Pakistan (SBP). The Regulations for Electronic Money Institutions,[41] which apply to mobile money operators in their capacity as electronic money institutions (EMIs), impose restrictions on the outsourcing of functions to third parties. Regulation 17 bars an EMI from outsourcing any services outside of Pakistan. As the Regulation does not limit the scope of functions that cannot be outsourced, this effectively includes any data processing operations, resulting in a total ban on data transfers.

The Framework on Outsourcing to Cloud Service Providers, 2023,[42] issued by the SBP, defines "permissible cloud computing arrangements".[43] While entities that fall under the framework's scope can outsource cloud-based services, limitations apply to outsourcing. Mobile money operators are permitted to outsource their material and non-material workloads to service providers outside the country. However, this can be subjected to restrictions by the SBP where it could have a systemic impact and/or generate unacceptable risks. The endorsement of Pakistan's cloud-first policy [44] conflicts with the endorsement of data localisation imposed by the Framework.

The Framework for Risk Management in Outsourcing Arrangements by Financial Institutions [45] provides robust data localisation requirements. All outsourcing arrangements are subject to the approval of SBP. The Framework demands that entities permitted to outsource services outside the country must satisfy requirements even after obtaining approval, such as ensuring that the offshore entity is regulated in its country. The SBP may even require the exporting entity to prove that the receiving entity is regulated. Additionally, the SBP prohibits, among other things, any form of subcontracting under offshore outsourcing agreements.

Restrictive data transfer requirements are also present in a new proposed data protection bill. Pakistan has yet to enact its Draft Personal Data Protection Bill, 2023, which was published by the Ministry of Information Technology and Telecommunication in May 2023.

However, the Bill will have data localisation implications once enacted. Section 31.2 of the Bill requires that critical personal data be processed only on a server or digital infrastructure located within the territory of Pakistan. This provision is highly restrictive due to the broad scope of critical personal data under the Bill and the wide discretion given to the Commission to designate personal data as "critical".

The Constitution of the Islamic Republic of Pakistan lays the groundwork for privacy protection in the country, securing the dignity and privacy of every citizen.[46] The Prevention of Electronic Crimes Act (PECA) further strengthens this foundation, addressing various electronic crimes, including potential data abuses and unauthorised data transmission. Section 7 prohibits and makes it an offence to transmit critical infrastructure data without authorisation. The Electronic Transactions Ordinance[47] acknowledges the legitimacy of electronic records and transactions but limits unauthorised alterations or transmissions of data. Also, financial institutions and other sensitive institutions in Pakistan are prohibited from transferring data to other countries without the authorisation of the relevant regulator and, in some instances, the data subject.

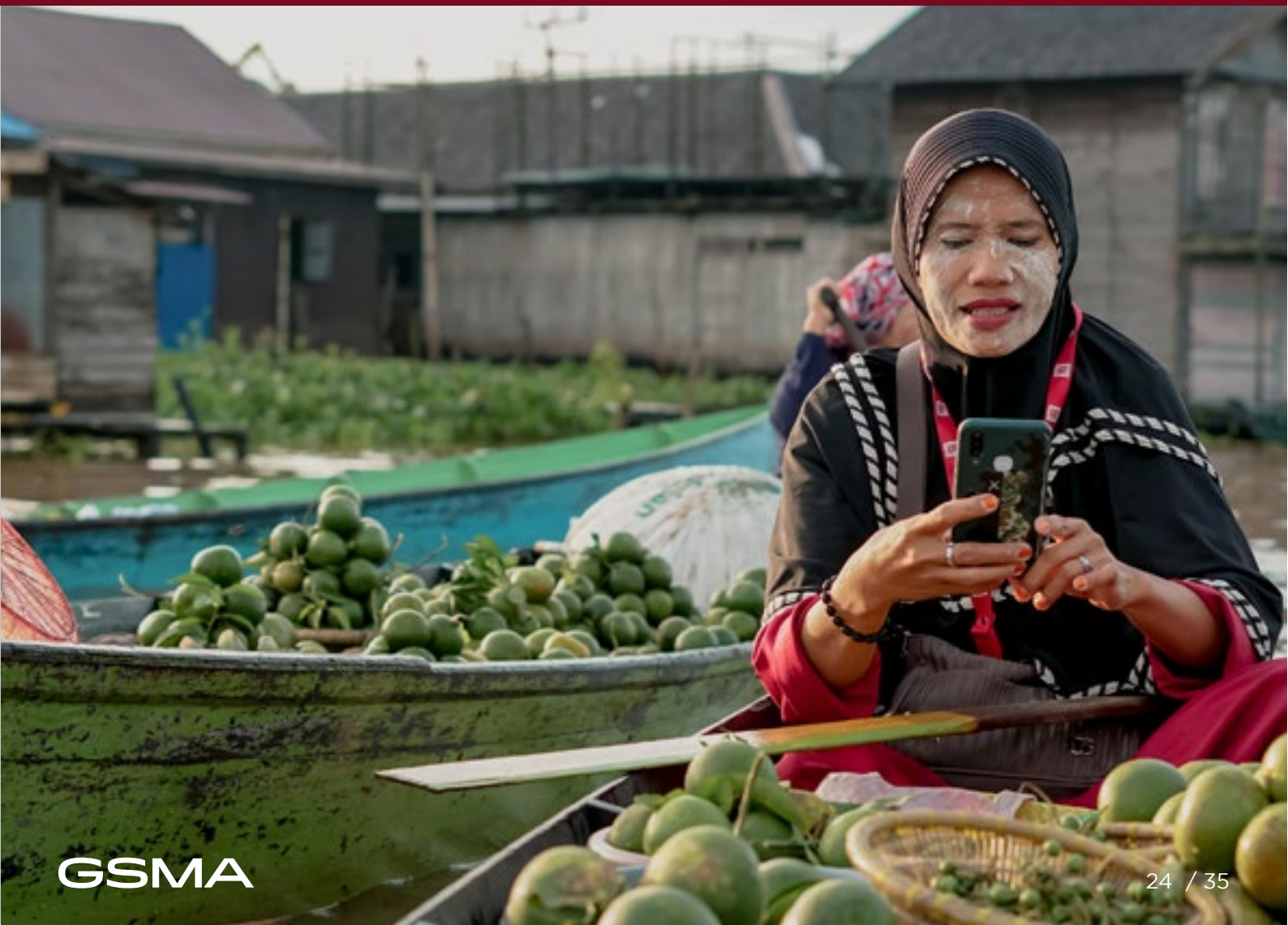
Cross-border data transfers also face hurdles due to the National Database and Registration Authority Ordinance[48] and the National Registration Act of 1973. Both laws impose limitations on accessing and disclosing information from the National Database, making it challenging for mobile money operators to conduct cross-border services given the inherent need for them to handle and transfer data.

In conclusion, while Pakistan has a legal structure to regulate data localisation and mobile money services, ambiguities and restrictions around cross-border data transfer pose potential challenges. Further, although the laws emphasise privacy and data security, they might unintentionally inhibit the opportunities for mobile money operators to expand their services beyond Pakistan.

41 State Bank of Pakistan Regulations for Electronic Money Institutions
42 Framework on Outsourcing to Cloud Service Providers, 2023
43 Banking Policy and Regulations Department (2017) Enterprise Technology Governance & Risk Management Framework for Financial Institutions
44 Pakistan Cloud-First Policy, 2022
45 Framework for Risk Management in Outsourcing Arrangements by Financial Institutions, 2019
46 Section 14 of the Pakistan Constitution
47 Electronic Transactions Ordinance, 2002
48 NADRA Ordinance of 2000

5

Impact of localisation laws on mobile money operators



This section explains the effect of data localisation on mobile money operators. It highlights the operational, strategic, and financial impacts of data localisation, including challenges observed by operators. The chapter analyses both the challenges and opportunities arising from these laws, which include:

Complex compliance procedures hampering the activities of mobile money operators

Mobile money operators in some of the countries examined are subject to data localisation requirements from multiple regulatory bodies simultaneously. Consequently, these operators must navigate a complex landscape to secure various data transfer approvals from different authorities, each with its own distinct timelines and requirements. This complicates the compliance process, especially where regulators have different approval criteria. Additionally, operators in some countries stated that they faced significant hurdles in their operations due to lack of clear and defined timelines for obtaining licenses and approvals, ultimately impacting their capacity to function effectively in the sector, which thrives on speed.

Constraints on the expansion of mobile money operators into other regions

In some countries with restrictive data localisation laws, operators encounter stringent regulations that can curtail scalability. The necessity of establishing localised data centres can slow down expansion initiatives, limiting operators' ability to respond rapidly to growing demand in new markets. In addition to a colossal compliance burden, operators, in addressing the pain points and challenges in data transfer regulation, have stated that the newness and lack of awareness of data protection acts and the cost of data centres remain significant concerns. Additionally, varying data localisation requirements make monitoring compliance difficult and can result in inconsistent user experiences across the different jurisdictions. Mobile money operators deem data localisation requirements a barrier to expanding into other countries, particularly where the country's data transfer requirements are highly restrictive.

Enabling cross-border data transfer can significantly reduce compliance burdens and operational costs, as operators need not navigate the complexities of varying data localisation requirements in different jurisdictions. This harmonisation of data handling leads to more efficient operations and streamlined processes. Furthermore, it ensures a consistent user experience across different regions, enhancing customer satisfaction.

Reduced efficiency in mobile money operations due to slow approval processes

Data protection authorities are one of the key regulators responsible for overseeing data transfers. In some countries under study, data protection authorities are still in their nascent stages and are not fully operational. Their limited operational capacity means that timelines for approval are often delayed, slowing down business processes and eventual service delivery to customers. A lack of cooperation among approving authorities further exacerbates delay. While some authorities have MoUs to ease the process of obtaining approvals from mobile money operators, the practice is not common in all countries.

Adding to the complexity, certain data protection regulators have yet to issue implementation guidelines for specific aspects of the law, thereby impairing their ability to grant approvals within precise timeframes, contributing to the overall challenges mobile money operators face. Allowing data to move freely across borders could mitigate the delays caused by the limited operational capacity of these authorities. The absence of cooperation among approving bodies could be alleviated through the establishment of regulatory sandboxes, capacity building, and the use of technology and automation (reg tech), depending on the root cause of the challenge.

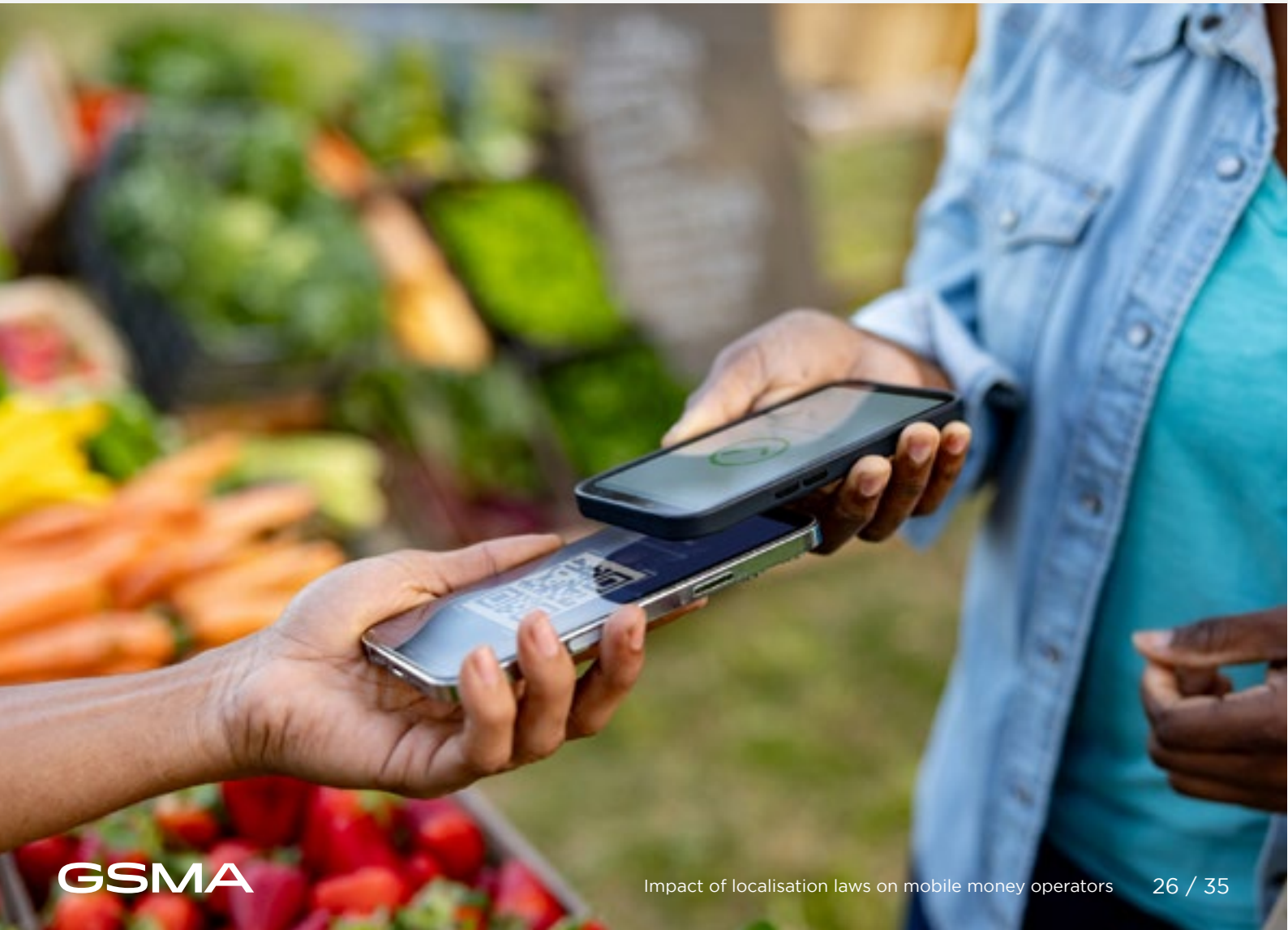
Limited access to the technology available to mobile money operators

Cross-border data flows provide mobile money operators with access to a broader range of technologies, including cloud services, AI, and machine learning. This enables operators to use advanced technologies available in various regions, enhancing their operational efficiency and innovation. With the ability to process data across borders, mobile money operators could seamlessly use cloud services provided by established entities in different jurisdictions, eliminating the need for local data storage facilities. The financial burden associated with setting up and maintaining local infrastructure would be significantly reduced, particularly benefiting smaller operators with limited resources. Cross-border data flows would create a more competitive landscape, allowing businesses to explore efficient solutions globally and fostering market forces that drive innovation and collaboration beyond local constraints.[49]

Increased cost of doing business

To meet data localisation compliance obligations, some operators have either established or are contemplating the development of their own in-house data centres. The cost of establishing and maintaining these facilities is high. This may cause a ripple effect, where heightened costs are transferred to consumers through increased transaction fees. This surge in consumer costs contradicts the very intentions of regulators, who aim to drive affordability. The free movement of data across borders allows businesses to operate globally, expand services internationally, and innovate with ease. This facilitates the emergence and adoption of services in one market that can readily expand to others, benefiting consumers and businesses alike.[50] Startups can achieve global reach from day one, and internet infrastructure suppliers can provide services to multiple markets at lower costs.

[49] GSMA Report on Cross-Border Data Flows Realising benefits and removing barriers 2018
[50] GSMA Cross-Border Data Flows Enable the Digital Economy: An overview 2017.



Data localisation limits information sharing for fraud prevention and increases cybersecurity risks

Data localisation disrupts the effective functioning of key compliance functions, such as anti-money laundering, counter-terrorism financing, and anti-bribery and corruption measures, by limiting the sharing of comprehensive personal data that spans multiple jurisdictions. These regulations result in a scenario where each country can only identify local fraud patterns, reducing visibility to more extensive fraud trends and threats. This localised approach risks turning these countries into safe havens for malicious actors, shielding their personal data from global fraud detection tools.

Data localisation regulations and requirements also compromise the tools and services used by financial institutions to identify and stop payment fraud, money laundering, and other financial and transactional offenses. The efficacy of functions such as anti-money laundering, counter-terrorism financing, anti-bribery and corruption, and know-your-customer (KYC) is contingent upon the availability of comprehensive personal data that is dispersed among various jurisdictions. Disconnecting these services from worldwide data transfers will result in a reduction in their precision and reliability. The potential consequences of this situation on the safety and security of individuals who depend on financial services and institutions are severe.

Additionally, data localisation measures hinder the deployment of essential fraud prevention tools, including spam detection and human verification tools, as the functionality of some of these tools often requires cross-border transfers of data. Information and intelligence-sharing across borders can help to reduce fraud and the associated costs.

Allowing cross-border data flows could provide mobile money operators with improved access to advanced cybersecurity tools and services, enhancing their ability to detect threats. According to research by the Centre for Information Policy Leadership (CIPL) and Tech, Law, and Security Programs (TLS),[52] data localisation laws limit the effectiveness of cybersecurity tools and services such as threat detection, thereby introducing risks to consumer data. To identify and address cyber threats, mobile money operators must be able to share information across multiple jurisdictions with clients, cloud service providers, and affiliates and ensure access to state-of-the-art cybersecurity systems. The prevention of information sharing among mobile money operators poses risks to data in situations where data sharing is essential for threat detection.

Operators generally consider cloud services to be immensely beneficial for safeguarding information. However, the restriction on the use of cloud services outside a country could hamper information sharing for threat detection. For countries like Tanzania, while this restriction applies to only critical information and not all personal data, it adds additional requirements for service providers to categorise their data into two main groups, critical and non-critical. This is not ideal, as from an operational perspective, it is easier, more efficient, and less costly to engage and contract a single provider. Lack of technological or cloud and cybersecurity policy means that there are no standards set for providers setting up local data centres, thus impacting integration with existing systems. This may also result in the need for operators to set up or adopt the use of different systems to enable compatibility with existing providers. Additionally, data localisation rules may impede organisations' ability to access state-of-the art cybersecurity applications.

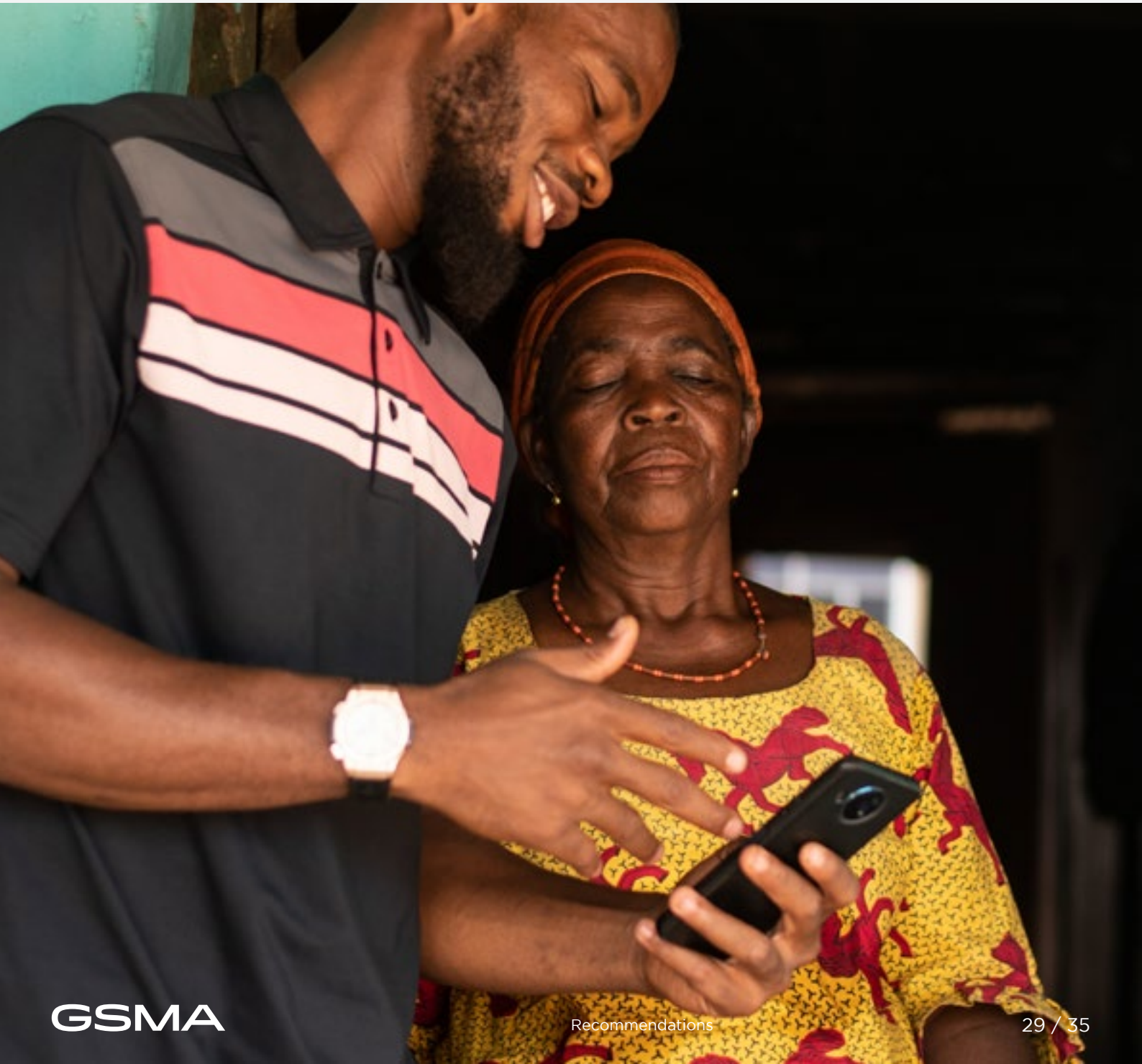
[51] Ibid
[52] CIPL and TLS (2023) Real Life Harms of Data Localization Policies

6

Recommendations

The analysis above of laws applicable to mobile money operators has shown that restrictions on cross-border data transfers create operational challenges for mobile operators.

Data localisation diminishes international trade and participation in the global data-driven economy. However, discussions with regulators and operators have provided insight into possible solutions to the challenges of data localisation and balancing the interests of governments, operators, and customers, whose data must be protected. Recommendations gleaned from these conversations lean more towards adopting ways to enhance security when handling personal data, while still being able to easily and efficiently obtain the necessary authorisations to transfer data to support operational efficiencies, cost, and technological advancements. To achieve this balance, the GSMA encourages operators, regulators, and policymakers to consider the following recommendations



Recommendations

Regulators and policy makers

Clear legal and regulatory requirements

Policymakers should establish clear and consistent international data transfer rules. This will reduce business challenges and protect personal data. Clarity in data localisation laws, especially concerning data specificity and categorisation, ensures effective data protection mechanisms are in place for each category.

Regulatory guidelines for cross-border data transfers should be clearly defined, ensuring operators can easily comprehend and adhere to them. Streamlining the authorisation process and reducing administrative hurdles will aid compliance, as witnessed in the complexities of the dual regulatory systems implemented in Tanzania and Nigeria.

Harmonisation of cross-border data transfer requirements

Harmonising cross-border data transfer requirements nationally, regionally, and globally will enhance global collaboration. This will allow businesses to operate more efficiently and effectively across different jurisdictions, resulting in increased innovation and the seamless flow of information that benefits both companies and consumers. In addition, harmonisation will help to facilitate equal opportunity for all market participants, ensuring fair competition and driving further advancements in technology and trade.

The legal framework to actualise this objective is available in Africa and Southeast Asia. In Africa, the African Union's Convention on Cyber Security and Personal Data Protection (Malabo Convention) calls for the harmonisation of laws and policies on cross-border transfer of data amongst its members.[53] The ASEAN Regulatory Pilot Space for Cross-Border Data Flows explains how to create a safe space for policymakers to understand and test possible policy solutions to facilitate cross-border data flows.

Adopt a dynamic approach to regulation

Adopt adaptive and technology-neutral regulatory frameworks that can evolve with technological advancements and stakeholder needs. This ensures that regulations remain relevant and do not stifle innovation.

This relies on capacity building to ensure that regulatory bodies understand the latest trends in mobile money. This will streamline market entry, minimise bureaucratic barriers for newcomers, and foster competition, innovation, and improved consumer experiences.

[53] https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

Public participation and stakeholder engagement

Public participation is a fundamental element of any successful policy initiative. Regulators are urged to maintain continuous dialogue with operators and other relevant stakeholders to comprehensively grasp operators' perspective. This way policy makers and regulators can harmonise policy objectives with operators' commercial interests and consumer protection. Understanding operator realities also promotes regulatory interventions that are closely aligned with the operational dynamics of the private sector.

Moreover, policymakers should institute feedback mechanisms enabling continuous evaluation of regulatory policies. These mechanisms should encompass channels for receiving input from industry stakeholders and the public to gauge policy effectiveness and pinpoint areas needing enhancement. A collaborative and feedback-driven approach to data regulation can help ensure that policies are effective, efficient, and equitable for all stakeholders involved.

Regulatory peer reviews and learning

In a world where innovation is fast outpacing regulation, regulators and policymakers are encouraged to leverage existing peer learning platforms, such as the Alliance for Financial Inclusion, to collaborate and share best practices with their counterparts.

This approach ensures that market-relevant strategies are developed to safeguard consumer rights while promoting global and regional trade and innovation. Regular updates to regulations, aligned with technological and market evolutions, along with clear communication about data localisation objectives, will enhance operator understanding and compliance.

Proportional data transfer regulation

Policy makers and regulators should prioritise the ease of cross-border data flows by re-evaluating and, where feasible, minimising or eliminating data localisation requirements. This approach would amplify the benefits of data mobility for the broader community, encompassing individuals, enterprises, and the public sector.

Also, evaluating their public interest, necessity, and legitimacy is crucial when imposing limitations on cross-border data transfers. Policies should only restrict data transfers when essential for protecting legitimate public interests, ensuring that any stipulated conditions are reasonable and not too stringent.

Policy and regulatory impact assessments

Policy makers and regulators are encouraged to regularly analyse the impact of regulatory measures such as data localisation. Such assessments ensure policies are grounded in real-world implications, leading to more informed policy making.

Recommendations

Operators

Collaboration with regulators and policy makers

Mobile money operators are encouraged to work closely and maintain open communication with regulators and policymakers to foster mutual understanding on regulation of data.

Operators should be actively involved in the legislative process, whether as individual operators or collectively.

They should suggest amendments based on their practical experience with existing laws and engage in policy debates on the formulation and implementation of domestic data protection and localisation laws and policies. Active involvement in policy making will help create laws prioritising data security and integrity without necessarily adopting or imposing strict data localisation obligations.

Advanced strategies for strengthening data security and compliance

Implementing robust encryption measures and data protection protocols can enhance data security and mitigate the risk of unauthorised access or breaches. Furthermore, conducting regular audits and assessments to evaluate the effectiveness of data transfer processes can help organisations identify and address potential vulnerabilities or non-compliance issues.

Using data transfer agreements or standard contractual clauses can also enhance compliance requirements while ensuring that organisations involved in data transfers comply with applicable data protection laws and regulations. If operators implement secure and encrypted communication channels, they can provide an extra layer of protection during data transfers, minimising the risk of interception or tampering.

Fostering collaborative responsibility in the finance sector

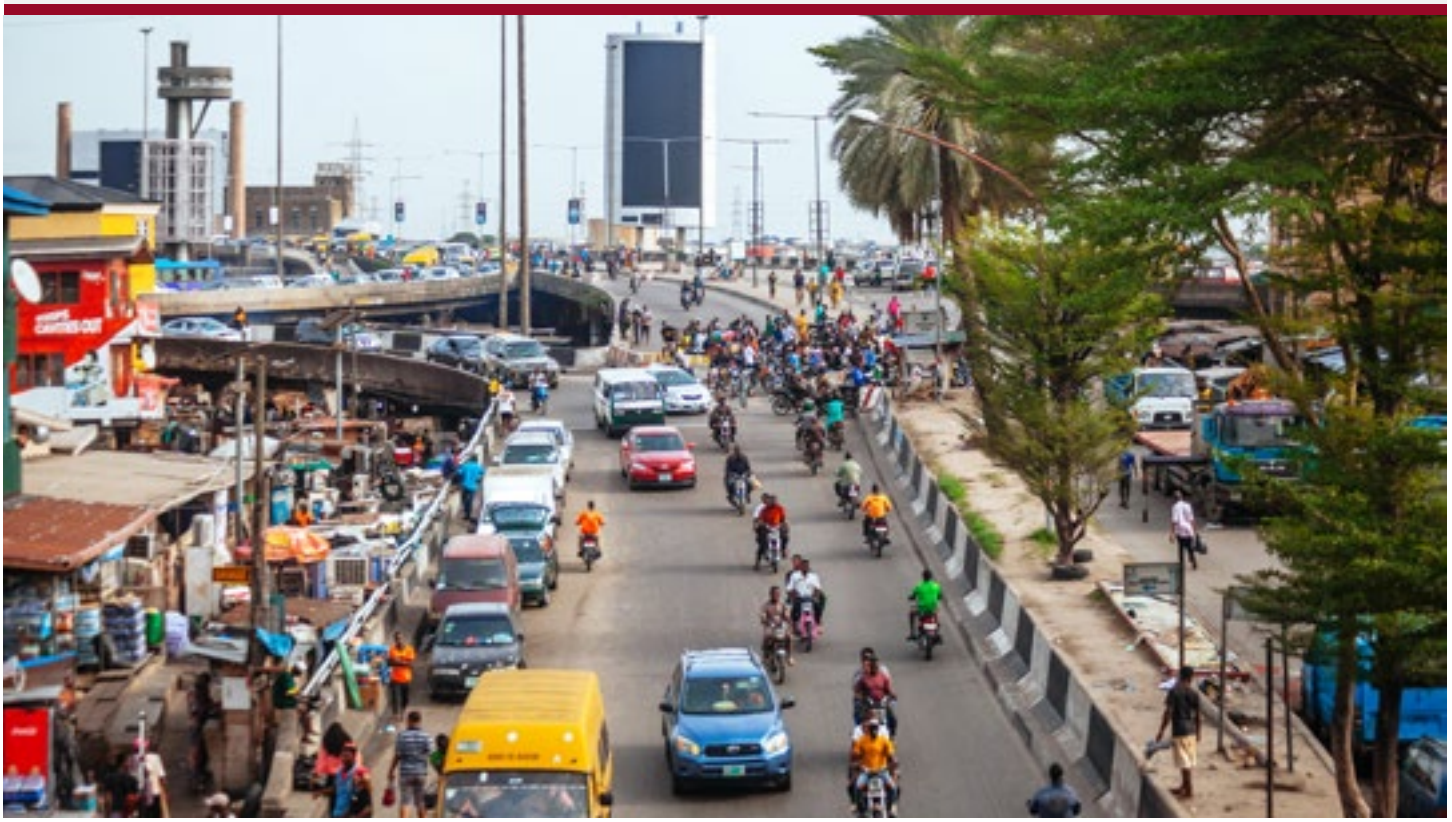
Operators are encouraged to work with other players in the financial ecosystem in establishing cross-border data best practices. Collaborating with technical experts in the international development community and standard-setting bodies could enhance frameworks for cross-border data transfers that could act as blueprints for policymakers. Mobile money operators may also use regulatory sandboxes, where available, to demonstrate their technical capabilities in addressing any regulatory concerns related to cross-border data transfers.

Conclusion

The examination of data localisation across the countries reviewed above reveals a multifaceted impact on data governance, economic development, and privacy considerations. It is evident that some nations view data localisation as a strategic move to bolster data security and cultivate indigenous digital ecosystems. However, this approach is not universally embraced, and challenges arise in finding a balance between national regulatory frameworks and the inherently global nature of data flows.

In navigating the dynamic landscape of data governance, it becomes imperative for policymakers, mobile money players, and international stakeholders to engage in collaborative dialogue. While recognising the nuanced implications, there is a pressing need to develop a harmonised approach that accommodates both local situations and the interconnectedness of the digital and financial services space. This collaborative effort is vital to fostering an environment conducive to sustainable economic growth and fair competition in the global market.

The path forward should involve finding a delicate balance that safeguards national interest and avoids undue hinderance to innovation, economic progress and operational costs for mobile money operators and digital financial service providers. Achieving this balance often depends on deep collaboration between organisations in the broader ecosystem, and is ultimately essential for sustainable and mutually beneficial integration of data localisation measures within the broader context of global data governance. Ultimately, policy makers are key to creating a secure and thriving digital market. Embracing cross-border data transfer policies conducive to innovative mobile money and digital financial services is crucial for advancing financial inclusion objectives, benefiting stakeholders across the board.



Glossary

Anti-money laundering/combating the financing of terrorism (AML/CFT)	A set of rules, typically issued by central banks, that attempt to prevent and detect the use of financial services for money laundering or to finance terrorism. The global standard setter for AML/CFT rules is the Financial Action Task Force (FATF).
Biometric data	Means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allows or confirm the unique identification of that natural person, such as facial images or dactyloscopy data.
Breach	Incident leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.
Consent	Means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
Controller	Means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
Cross-border data flow	The sharing of personal data from one national jurisdiction to another.
Data localisation	Refers to the compliance with respect to how data about citizens or residents of a certain country should be collected, processed, or stored within that country, before being transferred overseas.
Data protection regulator	In the context of mobile money, this typically refers to the regulator that has supervisory authority over the data protection framework in a jurisdiction.
Data subject	An identifiable natural person.
E-money	Short for 'electronic money,' e-money is stored value held in the accounts of users, agents and the provider of the mobile money service.
Interoperability	The ability of customers to undertake money transfers between two accounts at different mobile money schemes or to transfer money between accounts at mobile money schemes and accounts at banks.
Low-middle-income countries	Countries classified by the World Bank as low-income economies with a GNI per capita between $1,036 and $4,045.
Metadata	Information about other data. For example, regarding the content of a message, metadata can include location data, subscriber data, and specifically the type of data, the time a transaction was processed and received, device information, sender information, phone numbers, the origin of a message, and the IP address.

Glossary

Mobile money	A service is considered a mobile money service if it meets the following criteria: • A mobile money service includes transferring money and making and receiving payments using a mobile phone. • The service must offer a network of physical transactional points which can include agents, outside of bank branches and ATMs, that make the service widely accessible to everyone. The agent network must be larger than the service's formal outlets. • Mobile banking or payment services (such as Apple Pay and Google Pay) that offer the mobile phone as just another channel to access a traditional banking product are not included. • Payment services linked to a traditional banking product or credit card, such as Apple Pay, Google Pay and Samsung Pay, are not included.
Mobile money account	An e-money account that is primarily assessed using a mobile phone and that is held with the e-money issuer. In some jurisdictions, e-money accounts may resemble conventional bank accounts, but are treated differently under the regulatory framework because they are used for different purposes (for example, as a surrogate for cash or a stored value used to facilitate transactional services).
Mobile money operators	A licensed mobile money service provider.
Payment gateway	A payment gateway is an infrastructure that ensures the communication of payment details between merchants and payment processors by processing online payments, authenticating and safely passing data among the parties within the transaction flow.
Personal data	Means any information relating to an identified or identifiable natural person ('data subject'). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Processing	Means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Third party	Means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

GSMA Head Office
1 Angel Lane
London EC4R 3AB
United Kingdom
Tel: +44 (0)20 7356 0600