# The impact of data localisation requirements on the growth of mobile money-enabled remittances

## GSMA Mobile Money

The GSMA represents the interests of mobile operators worldwide, uniting more than 750 operators with over 350 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and internet companies, as well as organisations in adjacent industry sectors. The GSMA also produces industry-leading events such as Mobile World Congress, Mobile World Congress Shanghai, Mobile World Congress Americas and the Mobile 360 Series of conferences.

For more information, please visit the GSMA corporate website at www.gsma.com.

Follow the GSMA on Twitter: @GSMA.

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

For more information, please contact us:
Web: www.gsma.com/mobilemoney
Twitter: @gsmammu
Email: mobilemoney@gsma.com

The content of this working paper solely reflect the views of the GSMA and the authors.

**About this report**

This report was published in March 2019.
The author is Claire Scharwatt, Advocacy Director, Digital Inclusion, GSMA.

THE MOBILE MONEY PROGRAMME IS SUPPORTED BY THE BILL & MELINDA GATES FOUNDATION, THE MASTERCARD FOUNDATION, AND OMIDYAR NETWORK



# Contents

# Background

Cross-border data flows are key to enabling the digital economy and as such, the development of data localisation requirements is becoming a major area of concern for mobile and digital players.[1] This is particularly true for e-commerce and internet-enabled services within countries as they rely on the movement of data internationally.[2]

Recently, a growing number of emerging economies have adopted data localisation requirements as part of their efforts to regulate cross-border data flows. This is the case for example in China,[3] India,[4] Nigeria,[5] Russia,[6] Rwanda[7] and Vietnam.[8]

Data localisation regimes usually involve two main types of requirements, which result in extra costs for companies who could otherwise use cloud-based data services or global data centres:

- **Data storage requirements** stipulate that certain sets of data - typically government data as well as the personal data of national citizens - are hosted in data centres located on the national territory.
- **Data processing requirements** stipulate that specific activities relating to data entry, manipulation, processing and management should take place domestically.

In this paper, we explore the implications of data localisation rules on the mobile money business and argue that such regulatory requirements may dramatically hamper the growth of mobile money in general, and of mobile money-enabled international remittances in particular. There are more subtle and direct mechanisms that governments can use to facilitate cross-border flows of data in a way while ensuring data security and data privacy.

1. GSMA (2017). Cross-border data flows.
2. In many circumstances, such requirements can restrict or, de facto, prohibit cross-border trade in services, and must be analysed in the context of applicable World Trade Organisation's General Agreement on Trade in Services rules and commitments. In particular, the GATS Annex on Telecommunications seeks to ensure that members' commitments on trade in services are not undermined by restrictions on cross-border data flows such as requirements to localise data processing.
   Source: International Centre for Trade and Sustainable Development (ICTSD) and World Economic Forum (2016). Analysis of Data Localization Measures Under WTO Services Trade Rules and Commitments.
3. In China, the Cybersecurity Law that came into effect in June 2017 requires that personal information as well as "important data" should be stored in China.
4. The Reserve Bank of India's recent directive on data localisation requires all payment system operators to ensure that data is stored only within the country by October 2018. For the foreign leg of the transaction, if any, the data can also be stored in the foreign country, if required. See: Reserve Bank of India (2017-18). RBI/2017-18/153: Storage of Payment System Data.
5. Nigeria has required all subscriber and consumer data of ICT service providers as well as all government data to be stored locally within the country since December 2013 through its Guidelines on Nigerian Content in ICT.
6. Russia's Federal Law No.242-FZ which has been in effect since September 2016, requires that all databases containing the personal data of Russian citizens should be located in Russia.
7. In Rwanda, the concept of data sovereignty has be at the core of the government's National Data Revolution Policy and requires that national data should be hosted locally. Ministerial order N°001/MINICT/2012 of 12/03/2012 law provides that all critical information data within Government should be hosted in one central national data centre.
8. In Vietnam, the Parliament is currently reviewing a draft cybersecurity law which requires all foreign online service providers to store the personal data of Vietnamese citizens in local data centres.

# The implications for mobile money-enabled remittances

Over the past few years, mobile money services have evolved to become the leading platform for domestic payments in a number of emerging markets. More recently, a number of mobile money services have expanded to facilitate cross-border transfers and today, there are 184 unique corridors where mobile money can be used to send and/or receive international remittances, connecting 35 sending countries and 40 receiving countries.[9] This represents a major revolution and it has allowed providers to drive down remittance costs significantly, positioning mobile money as a key tool to achieve Sustainable Development Goal target 10.c which aims at reducing the cost of remittances below 3 per cent by 2030.

However, the safe and secure provision of remittances relies on strict anti-money laundering (AML) and combating the financing of terrorism (CFT) processes, which typically involve the sharing of data across borders.[10] There are three main ways in which data localisation requirements impact the effective provision of mobile money-enabled remittances, posing a direct threat to the growth of the sector:

- **Exchange of data with partner remittance companies for customer screening purposes** - Cross-border data sharing of personal customer data is necessary to allow the company receiving the remittance (and the hub where a hub is involved) to check the identity of the sending customer, who will be screened against domestic and international sanctions lists. FATF recommendation 16[11] on wire transfers requires financial institutions to share information about the remittance sender and recipient including their names and account number (or a unique transaction number) at minimum for low-value transactions, as well as the sender's address, national ID number, date and place of birth for higher-value transactions.

- **Exchange of data between different entities within the same group for effective AML/CFT and fraud detection purposes** - A number of mobile money providers belong to international groups that have invested in centralised fraud detection and AML/CFT facilities. In such cases, the cross-border sharing of information between different entities within the same group is necessary to ensure proper checks are carried out. This is in line with recommendation 18 of the FATF around internal controls and foreign branches and subsidiaries, which requires that financial groups implement group-wide programmes against money laundering and terrorist financing (ML/TF), including policies and procedures for sharing information within the group for AML/CFT purposes.[12]

9. Nika Naghavi and Scharwatt, C., (2018). Mobile money: Competing with informal channels to accelerate the digitisation of remittances. GSMA.
10. "Information sharing is critical for combatting money laundering, terrorist financing and financing of proliferation. Multinational money laundering schemes do not respect national boundaries. Barriers to information sharing may negatively impact the effectiveness of AML/CFT efforts and conversely, inadvertently facilitate operations of such criminal networks. This underscores the importance of having rapid, meaningful and comprehensive sharing of information from a wide variety of sources, across the national and global scale." "FATF Guidance: Private sector information sharing", FATF (2017). Available here: http://www.fatf-gafi.org/media/fatf/documents/recommendations/Private-Sector-Information-Sharing.pdf.
11. FATF (2012). International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation.
12. FATF (2017). FATF Guidance: Private sector information sharing and and Maina, J. (2019). Guidelines on mobile money data protection. GSMA.

- **Exchange of data with partner remittance companies to facilitate effective customer protection** - The transmission of financial information is also needed for the transaction to be processed effectively and to support customer redress mechanisms when needed, including in the case of transaction reversals.

As such, data localisation requirements may directly conflict with AML/CFT requirements around international remittances, making it impossible for providers to comply with both regulatory frameworks. In certain cases, exemptions may allow cross-border data sharing for the prevention of crime, as well as money laundering and terrorism financing. Companies are then typically required to document what information is being shared, with whom, and under which circumstances in order to provide sufficient justification to the data regulatory authority. As a general principle, mobile money providers should evaluate whether the cross-border transfer of data required to conduct international remittances is compliant with local regulations.[13]

In many countries however, a lack of clarity and guidance around how to align data localisation requirements with AML/CFT requirements has created uncertainty among mobile money providers. For anti-money laundering measures, the European Data Protection Supervisor (EPDS) has suggested 'necessity for compliance with a legal obligation' as an appropriate legal basis.[14] However, with the lack of harmonisation in laws governing the cross-border transfer of data, we may see discrepancies across borders.

Data protection laws may also limit the transfer of personal data to only countries or territories that meet certain standards. This is the case for example within the ECOWAS region, where cross-border data transfers can only happen with countries that provide "an adequate level of protection for privacy, freedoms and the fundamental rights of individuals".[15] In Ghana, while companies do not need to obtain prior authorisation for transferring data across borders, they need to have assessed and documented the data protection legal environment of other countries where data is being exchanged, which can be difficult.[16] In Côte d'Ivoire, prior authorisation from the regulator is required for the processing of personal data outside of the ECOWAS region.[17]

Finally, in some markets regulation requires prior consent from individuals before their personal data can be transferred cross-border. This is the case for example in Mexico[18] with the exception of when the transfer is made to a subsidiary or affiliate company operating under the same processes and internal policies.

13. This is one of the criteria under the GSMA Mobile Money Certification under Principle 8 around data privacy: "Has an assessment been made to ensure that any international transfer of personal data (e.g. for data processing in another country) is compliant with regulations)?" See: www.gsma.com/mmc.
14. The European Data Protection Supervisor (EPDS) is the EU's independent data protection authority with the responsibility for monitoring the processing of personal data by the EU institutions and bodies, advising on policies and legislation that affect privacy and cooperating with similar authorities to ensure consistent data protection.
15. Supplementary act A/SA.1/01/10 on personal data protection within ECOWAS (2010). Available here: http://www.statewatch.org/news/2013/mar/ecowas-dp-act.pdf.
16. Data Protection Act (2012). Data Protection Act, 2012.
17. Loi n° 2016-412 du 15 juin 2016 relative à la consummation. Available here: https://www.unodc.org/res/cld/document/civ/loi-no-2013-450-relative-a-la-protection-des-donnees-a-caractere-personnel_html/06192013_loi_donne_es_personnelles.pdf.
18. Ley Federal de Proteccion de Datos Personales en Posesion de los Particulares. Available here: http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf.

# What has been the impact so far?

The introduction of data localisation requirements is usually justified through four main arguments:

- Improved data security;
- Stronger protection of privacy for citizens' personal data, including protection from foreign governments' access;
- Easier access to data and control for national regulators and supervisors; and
- The creation of local jobs by necessitating the establishment of domestic data centres.

These are legitimate concerns for policy makers. However, there is little evidence that data localisation have led to these outcomes. Moreover, there is a risk that such measures can even have the opposite effect. When it comes to data security, investment in infrastructure and maintenance is more critical than the physical location of data.[19] The text box below contains more insights into the mobile money industry's practices to ensure data security.

For example, one of the greatest advantage of storing data in the cloud is data sharding – the fact that information is typically sliced up and distributed among multiple systems rather than kept on a single machine or set of machines.[20] Most importantly, extra costs of domestic data hosting may lead to lower investments in security aspects.

Restrictions around cross-border data flows can also lead to increased risks of money laundering and the financing of terrorism. This is the case, for example, when the reporting ability of mobile money providers is compromised by regulations that restrict cross-border data sharing or make it a more complex and lengthy process, as this can increase the risk that a criminal rejected in one country can open a mobile money account and make transactions in another country.[21]

In addition, the positive impact of data localisation on job creation can be reversed with companies deciding to exit a particular market as a result of increased costs and/or the inability to provide services effectively.

19. EDAM Cyber Policy Paper Series (2016). Cross-border data transfers and data localization.
20. Patrick Ryan, Falvey S. and Merchant R. (2013). When the Cloud Goes Local: The Global Problem with Data Localization. IEEE Computer Society.
21. "For example, some jurisdictions have found that sharing alerts or information about customers who are refused or exited due to ML/TF concerns can prevent arbitrage of the financial system by criminals, who may attempt to engage with many different institutions. Consolidating information on payments by multiple institutions can identify criminals structuring payments using multiple institutions to avoid detection by other means." See: FATF (2017). Guidance on Private Sector Information Sharing.

# Conclusion and recommendations

Cross-border data flows are critical to ensuring the safe and secure provision of mobile money-enabled remittance services. In that context, data localisation requirements can directly challenge emerging markets' ability to unlock mobile money's potential to reduce the cost of remittances, to formalise remittance flows and to empower migrants and their families.[22]

In addition, the implementation of data localisation requirements can have unintended consequences leading to reduced data security, increased ML/TF risks and even the closure of services. Governments can facilitate cross-border flows of data in a way that allows them to ensure data security and data privacy, while maintaining and attractive business environment. To that end, the following points should be considered:

- Only impose measures that restrict cross-border data flows if they are absolutely necessary to achieve a legitimate public policy objective. The application of these measures should be proportionate and not be arbitrary or discriminatory against foreign suppliers or services.[23]

- Where cross-border data transfers are restricted, provide exemptions for the prevention of crime, as well as money laundering and terrorism financing.

- Where cross-border data transfers are limited to countries that meet certain data protection standards, clearly indicate the mandatory criteria and identify the countries wherever possible.

- To enable transfers between countries and regions where privacy frameworks are in place, endeavour to identify common principles between these different frameworks, to enable mutual recognition of different frameworks across jurisdictions. This will help to build confidence between countries, facilitate sharing of best practice between policymakers and allow data privacy regulators to detect and address non-compliance more easily, without resorting to localisation measures.

- Provide clear guidance to financial service providers including mobile money providers on how to ensure compliance with both data protection regulations and AML/CFT requirements, to allow mobile money providers to be effective partners in the prevention of money laundering and financing of terrorism.

- Engage with peer regulators in other countries to develop appropriate intergovernmental mechanisms to enable governments to scrutinise data hosted outside of their national borders for official, legitimate purposes when needed, without restricting data flows.[24]

- Encourage the adoption of industry-led initiatives that promote data security and privacy, such as the GSMA Guidelines on International Remittances through Mobile Money, the GSMA Mobile Money Certification, GSMA Mobile Privacy Principles and the Guidelines for mobile money data protection.

The GSMA and its members believe that cross-border data flows can be managed in ways that safeguard the personal data and privacy of individuals and remain committed to working with stakeholders to ensure that restrictions are only implemented if they are necessary to achieve a legitimate public policy objective.

22. Naghavi N. and Scharwatt, C., (2018). Mobile money: Competing with informal channels to accelerate the digitisation of remittances. GSMA.
23. GSMA (2017). Mobile Policy Handbook.
24. Ibid.

## GSMA Guidelines on International Remittances through Mobile Money: Data security and APIs*

International remittances involve the transmission of financial and personal data to a partner located in a foreign jurisdiction. Complex transactions increase the risks associated with the integration of platforms, creating more potential vulnerabilities for cybercrime and human error. For this reason, it is especially important to ensure the security and integrity of communications. Best practices applied by mobile money providers include ensuring that the protection of the information includes the use of APIs to simplify communications, reducing communication risks, and the use of high encryption standards to prevent cases of hacking or fraud.

Best practices that have been adopted by the industry include:

A. All electronic information exchanges related to transactions with third parties are made through secure channels to ensure the protection and integrity of data. Encryption encompasses global best practice in line with the recommendations of the Cryptographic Technology Group of the US National Institute of Standards and Technology.

B. The use of authentication algorithms for providers' systems ensure data is shared only with trusted parties.

C. The application of the ISO/IEC 27001 standards for information security management systems (ISMS) to ensure the secure management of financial and personal data.

D. The development of channel security policies that describe relevant controls and assign clear responsibilities to each party involved.

E. The use of APIs to improve service functionality and data richness, providing, among other things, sufficient data to relevant parties to ensure best-practice AML/CTF, fraud prevention, and sanctions screening.

* Sanin, J. and Scharwatt, C. (2017). Working Paper: Guidelines on International Remittances through Mobile Money.

**GSMA HEAD OFFICE**
Floor 2
The Walbrook Building
25 Walbrook
London EC4N 8AF
United Kingdom
Tel: +44 (0)20 7356 0600
Fax: +44 (0)20 7356 0601