Data protection in mobile money

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 the industry-leading MWC events held annually in Barcelona, Los Angeles and Shanghai, as well as the Mobile 360 Series of regional 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

Published March 2019

Author:
Juliet Maina, Advocacy & Regulatory Manager, GSMA.

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

Contents

Introduction

The provision of mobile money services requires the collection and generation of significant amounts of consumer data, both personal and non-personal. When leveraged effectively, this data can drive operational efficiencies in the provision of mobile money services by improving fraud detection mechanisms, and can support the broader economy through the provision of other financial services to the previously underserved.[1]

The mobile money industry recognises that when used responsibly, data can bring fundamental changes to traditional solutions, drive long-term impact by improving access, and develop insights on opportunities for increased financial access. In the context of mobile money, responsible use of data is critical to ensuring customers have sufficient control over their personal data. With this in mind, consumer protection remains a critical focus area for mobile money providers, as they recognise the need to empower consumers and protect their personal data in this increasingly digital age.

As appreciation for the value of data grows, several governments in developing countries are now considering the creation or revision of data protection laws to preserve citizens' privacy rights.[2] The Alliance for Financial Inclusion has recognised the importance of proportional data protection regulation that protects consumer data while also boosting innovation in the financial services industry. They state:[3]

"Proportional data protection regulations must protect customer data while enabling innovation based on digital data. The ability to collect, analyze and share personal data responsibly is critical to client-centric product development. At the same time, customers should be entitled to privacy, confidentiality, protection from excessive collection, unauthorized use and disclosure of their data and meaningful consent for data collection and use." [3]

In countries where consumer and data protection legal frameworks are underdeveloped, protecting personal data can best be achieved through appropriate organisational data governance mechanisms focused on the provision of mobile money services. This will protect users from the risk of cyber breaches, and ensure that there is a level of uniformity across countries where mobile money operates. The ability to build up trust and confidence among users will safeguard the providers' reputation, and boost the growth and sustainability of the mobile money industry as a whole.

This paper aims to provide an overview of data protection practices that will have a significant impact on the provision of mobile money services in the years ahead. It focuses on four key areas that mobile money providers need to address; data processing, data security, data sharing and data localisation, and considers some of the main implications for the provision of mobile money services.[4]

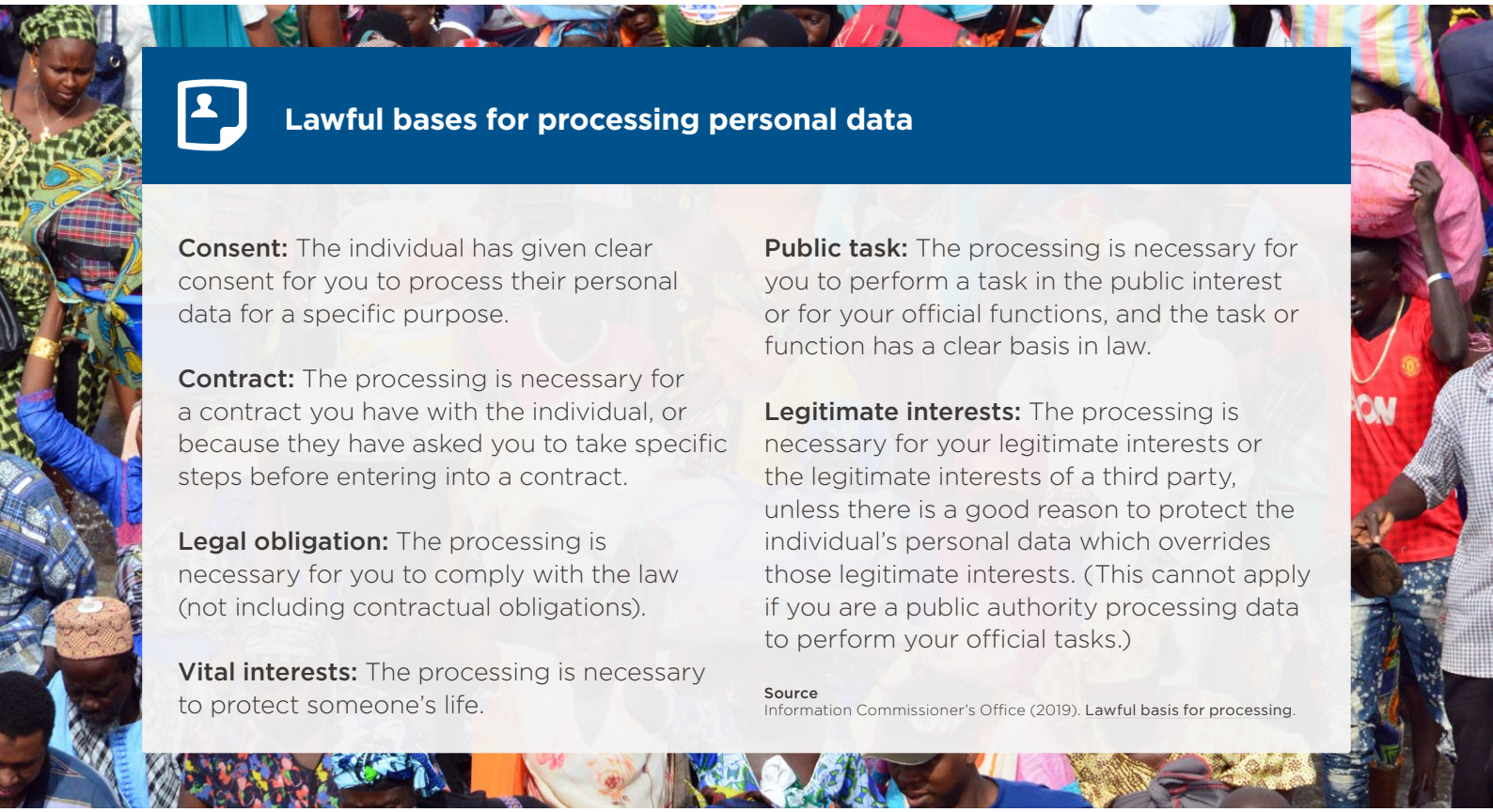
1 Gidvani, L. (2018). Opportunities to leverage mobile money data to improve access to the digital economy. *Mobile for Development Blog*. GSMA.
2 As of 2018, 17 countries in Africa had data protection legislation with several others in the process of developing or revising theirs. See: Deloitte (2017). Privacy is Paramount: Personal Data Protection in Africa.
3 Alliance For Financial Inclusion (2018). Digital transformation of microfinance and digitization of microfinance services to deepen financial inclusion in Africa.
4 It is key to note that these topics are addressed in various global laws and policy initiatives such as the Council of Europe Convention 108 on Automated Processing of Personal Data; the Organisation for Economic Co-operation and Development (OECD) Privacy Guidelines; the EU General Data Protection Regulation; the US Federal Trade Commission's Fair Information Practice Principles, and the APEC Privacy Framework. These widely considered principles and frameworks form the foundation for exploring the privacy issues impacting mobile money.

Data processing

What is data processing?

Data processing refers to any operation or set of operations carried out on personal data or sets of personal data. These operations can be automated or manual. Examples of data processing include: collecting, recording, organising, structuring, storing, adapting, altering, using, disclosing by transmission, disseminating, erasing and destruction of data.[5]

Laws today increasingly stipulate that there must be a lawful basis for all processing of personal data. Where the data controller does not have a lawful basis for processing personal data, then that processing and the associated activity is *prima facie* unlawful.[6] The consent of a data subject typically provides the most common lawful basis for processing of that subject's data. For mobile money services which are geared towards the underserved, consent may be less effective as users are new to the technology and in some instances uneducated. This may act as a deterrent where additional steps are required for the provision of these services. However, it is important to note that there are other grounds upon which lawful processing can take place (see text box below). By taking one or more of these approaches, mobile money providers can avoid the shortcomings of the consent model, protect citizens' personal data, promote trust and confidence in their services and still leave plenty of room for innovation.[7]



Lawful bases for processing personal data

Consent: The individual has given clear consent for you to process their personal data for a specific purpose.

Contract: The processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

Legal obligation: The processing is necessary for you to comply with the law (not including contractual obligations).

Vital interests: The processing is necessary to protect someone's life.

Public task: The processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

Legitimate interests: The processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

Source
Information Commissioner's Office (2019). Lawful basis for processing.

5 European Commission (2019). See: What constitutes data processing?
6 Gabel, D. & Hickman, T. (2017). Chapter 7: Lawful basis for processing – Unlocking the EU General Data Protection Regulation.
7 CGAP (2019). 3 Data Protection Approaches That Go Beyond Consent. *CGAP Blog.* CGAP.

Contracts, legal obligations and legitimate interests are lawful bases for processing personal data which are particularly relevant to the mobile money industry. In each instance, mobile money providers will need to document the particular basis for processing personal data. It is also critical to ensure users are made aware of the avenues for recourse in the event of data breaches such as customer service and support mechanisms, as well as any available dispute resolution mechanisms. Transparency will be crucial in building and maintaining consumer trust and confidence.

Why is lawful data processing important for mobile money providers?

Collection of personal data is essential in providing mobile money services. Personal data is necessary to meet Know Your Customer (KYC) requirements as well as Anti-Money Laundering/Countering the Financing of Terrorism (AML/CFT) provisions. The personal data collected and subsequently generated by mobile money providers may include telephone numbers, call data records, identity information, mobile usage history, transactional history and location data, among others.

Additionally, ensuring a lawful basis for the processing of personal data is essential for data protection as it provides consumers with the required choice and control over their data. User choice and control constitutes one of the key principles of data protection, as addressed in the GSMA Mobile Privacy Principles and the Guidelines for Mobile Money Data Protection.[8] Fundamentally, it requires that users are given opportunities to exercise meaningful choice and control over their personal data, thus putting the consumer at the centre of service delivery.

The aforementioned Guidelines and Principles provisions are grounded in international standards such as the OECD privacy principles, which articulate that data should be collected by lawful and fair means, and with the knowledge or consent of the data subject where appropriate.[9] As part of the Use Limitation Principle under the same OECD privacy principles, it is further required that data should not be used for any purpose other than that which it was collected for, unless consent is given. In the context of service provision, users should either be able to consent to the use of their personal data, or there must be evidence that the processing of data is necessary to the benefit of the consumer.

How does lawful data processing impact the provision of mobile money services?

Based on the above, it is clear that ensuring a lawful basis for processing personal data is critical as it will impact mobile money services at various points of service delivery, starting at the point of on-boarding a customer or registering new services where personal data is collected. In mobile money, the risk to data protection is increased as mobile money agents are responsible for collecting personal data from customers on behalf of the mobile money providers. Agents typically operate as third parties and are therefore not subject to the same licensee or authorisation obligations as the mobile money provider. As mobile money providers strive towards empowering their users and giving them increased control of and access to their data, the customer journey will need to adapt to incorporate these principles. This will begin at the point of on-boarding, with the agent interaction, to ensure that data is collected and processed appropriately.

Mobile money providers may also consider adopting a 'privacy-by-design' ethos or methodology by which privacy and security safeguards are considered and designed into products, services, processes or projects at each stage of the lifecycle, thus affording consumers better transparency over the use of their data.[10] At the on-boarding stage, these would be most impactful in the contractual agreements, as well as in the terms and conditions for the various products and services.

> **"Privacy-by-design advances the view that the future of privacy cannot be assured solely by compliance with legislation and regulatory frameworks; rather, privacy assurance must become an organization's default mode of operation."**[11]

Ensuring the lawful basis for processing of personal data will therefore require awareness campaigns for employees, users and third parties (agents). This will ensure that a) users have a sound understanding of how their data is collected and why it is shared, if at all; and b) that third parties apply the same measures as the mobile money provider when collecting and handling personal data from users. Employees will also be required to understand and adequately handle personal data in accordance with the company's requirements.

8 GSMA (2016). Mobile Privacy Principles: Promoting consumer privacy in the mobile ecosystem. Maina, J. (2018). GSMA Guidelines on mobile money data protection. GSMA.
9 The OECD principles are found in Part Two, paragraphs 7 through 14 of Annex to the Recommendation of the Council of 23rd September 1980: Guidelines Governing The Protection of Privacy and Transborder Flows of Personal Data. See: http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#guidelines
10 GSMA (2017). Mobile Privacy and Big Data Analytics.
11 Information & Privacy Commissioner of Toronto (2013). Privacy by Design.

Data security

What is data security?

Data security refers to the physical and logical security controls used for the protection of personal data guarding against risks such as loss, unauthorised access, use or disclosure, modification or destruction.[18] Ensuring the confidentiality, integrity and availability of personal data through sufficient security controls is critical to protect against data breaches which result in compromised, corrupted or deleted data, thus leading to a violation of privacy and, in some cases, financial harm.

The financial services sector is typically highlighted as one of the largest sectors at risk of cyber breaches.[13] This, coupled with the customer mobility that is promoted by mobile devices, heightens the risk of data breaches in the mobile money industry.[14] The mobile money industry therefore recognises data security as key to building trust and maintaining the growth and sustainability of mobile money services.

Why is it important for mobile money providers?

As cybercriminals become more sophisticated, the nature of cyber breaches continues to evolve, thus putting consumers at more risk. Previously, cyber breaches in the financial services industry would be associated with financial loss, however today there are further implications with breaches increasingly characterised by the loss of personal data. These are then used to perpetuate identity theft and carry out fraud and other financial crimes. Additionally, the reputational damage that emanates from cyber breaches may have more adverse effects on the organisation than financial loss. Loss of consumer trust and confidence could lead to loss of market share, and a lack of trust in new technologies that would otherwise lead to improved financial access. Beyond this, with the development of data protection legislation that requires entities to implement appropriate security measures, the risk of non-compliance in the event of breaches also presents a further risk to mobile money providers.

For mobile money to continue to grow and protect the gains in financial inclusion already achieved, it is critical that the providers implement appropriate security controls that will guard against cyber-attacks. Mobile money's financially underserved customers may be new to the technology that underpins the service. Awareness and education campaigns are therefore even more critical for this group, to ensure that they have an understanding of the associated risks, and are able to secure themselves.

How does data security impact the provision of mobile money providers?

Legal and regulatory frameworks are evolving, and mobile money providers are now subject to new obligations around cybersecurity. Mobile money providers therefore need to introduce technical and organisational measures to ensure that they are able to address these. One such requirement is the notification obligation which is quickly becoming the norm in data protection law. This obligation stipulates that data controllers must report cyber breach incidents to the relevant authorities, and in some instances must report these directly to the affected individuals. The purpose of this is to increase the accountability of data controllers and, through increased transparency, to empower consumers to take steps to protect themselves from harm in the event of a breach.

From a practical perspective, this will require that mobile money providers look beyond the introduction

12 The security safeguards principle requires that personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data. See: http://oecdprivacy.org/#safeguards. This is also provided for in Maina, J. (2018). GSMA Guidelines on mobile money data protection. GSMA.
13 Lagarde, C. (2018). Estimating Cyber Risk for the Financial Sector. *IMF Blog*. International Monetary Fund.
14 In addition to the financial losses incurred by the industry and consumers, cyber incidents and data breaches harm consumers' trust and confidence in the financial system or individual institutions. Cyber risk therefore is a financial consumer protection concern. See: CGAP (2018). Cybersecurity in emerging financial markets.

of appropriate technical systems and consider a holistic approach which looks at people, processes and technology. Data security for mobile money providers will require the formulation of organisational policies which provide appropriate incident response plans and mechanisms in the event of a breach, as well as the appointment of an accountable person for the implementation of these processes and controls.[15] These will enable providers to meet their data protection obligations, as required by an increasing number of data protection laws.

Today, data security is such a critical matter that it needs to be addressed at the management and board level to ensure the successful implementation of data security strategies and policies. The human element of cybersecurity provides the weakest point of data security, as staff and users operate as the most vulnerable targets for cybercriminals. Additionally, insider threats are ever possible, as employees with access to systems have the capacity to collaborate directly with cybercriminals.[16] Capacity building and awareness initiatives across the entire supply chain of these services, including end users, will therefore be fundamental to ensuring the security of customer data. Establishing appropriate security measures, both organisational and technical, will support scalability and help ensure the business maintains enterprise-wide compliance, in keeping with the pace of regulatory change.[17]

15 The Central Bank of Kenya issues draft Cybersecurity Guidelines for payment service providers which, among other things, mandate the appointment of a Chief Information Security Officer who is responsible for all cybersecurity related matters within the organisation. See: Central Bank of Kenya (2018). Guidelines on Cybersecurity for Payment Service Providers. Under the GDPR, the Data Protection Officer also has a role to play in ensuring that data breaches are managed, and that the organisation remains accountable to consumers.

16 In a 2018 survey, it was found that 90% of organisations feel vulnerable to insider attacks. The main enabling risk factors include too many users with excessive access privileges (37%), an increasing number of devices with access to sensitive data (36%), and the increasing complexity of information technology (35%). See: CA Technologies (2018). Insider Threat Report.

17 IT Pro Portal (2019). Critical data security trends for 2019 and beyond.

Data sharing

What is data sharing?

Data sharing models refer to a service, platform, or product that collects and/or creates digital records for individuals including financial history and alternative data (e.g. web history or phone records); and allows individuals to determine when and how this data will be made available to multiple third parties offering products and services.[18]

Why is data sharing important to mobile money providers?

Data sharing has been integral to the development, evolution and success of the mobile money industry. Aggregation, analysis, monitoring and automation of payment requests creates convenience, speed and simplicity for end users.[19] Additionally, individuals who previously could not access certain services due to their lack of financial history are now able to gain access based on alternative sources of data such as social media interactions, call records and geographical location.[20] The ability to share data between various players therefore breaks down data silos which would otherwise limit the potential of data trails to further transform financial inclusion.

However, if not sufficiently controlled, mobile money providers recognise that increased data sharing may also be accompanied by a reduction in customer privacy and security. The implementation of appropriate data governance mechanisms, with accountability mechanisms and transparency for the user, is therefore critical to ensure that personal data is shared in a responsible manner.

18 Mazer, R. (2018). Emerging data sharing models to promote financial service innovation: global trends and their implications for emerging markets. FSD Kenya.
19 Barclays (2017). Open banking: A consumer perspective.
20 The simple fact that mobile and internet penetration have surpassed financial services penetration in most emerging markets hints at a big opportunity: many people who have had no meaningful access to formal financial services are creating digital footprints financial service providers can capture and analyze to reach them with commercially viable services that help them improve their lives. See: Sanabria, R. (2018). To Bank the Unbanked, Start Using Alternative Data. *Center for Financial Inclusion Blog*.

What is the impact of data sharing on compliance mechanisms?

If done well, data sharing can reduce risks through enhanced KYC capabilities, identity validation, and fraud detection.[21] In the context of mobile money, customer data may be shared between organisations to meet certain statutory requirements that relate to AML/CFT procedures including, for example, watch-list screening. In keeping with these requirements, some mobile money providers have established centralised fraud detection and AML/CFT facilities. In such cases, the cross-border sharing of information between different entities within the same group entity is required to ensure the necessary checks are executed. This is in line with Recommendation 18 of the Financial Action Task Force (FATF) Guidance on private sector information sharing, which requires that financial groups implement group-wide programmes against money laundering and terrorist financing, including policies and procedures for sharing information within the group for AML/CFT purposes.[22] At the group level, these procedures must comply with core data protection principles and lead to an effective group-wide compliance programme.

How can data sharing improve financial deepening?

Data sharing presents an opportunity for mobile money providers to offer a range of products and services to underserved groups. Digital identity and authentication can play a vital role in bringing billions of people into the financial system swiftly and securely.[23] One of the main ways in which this is possible is through data sharing between the entity providing digital identity and the service provider, allowing them to offer more financial services. This, in turn, leads to improved financial access, as providers generate more easily accessible data on consumers and businesses that helps to identify and qualify these consumers and businesses.[24] This is especially so in underserved regions. For this to be successful, however, it is imperative that consumers are given access to and control over the sharing of their data in accordance with internationally accepted best practices.

The implementation of appropriate data governance mechanisms and data handling procedures can complement and even enable data sharing in the provision of financial services. The importance of mitigating risk, especially in countries where there are no data protection frameworks, cannot be over-emphasised. An open, consumer-friendly data environment will benefit consumer welfare, competition and providers' risk management strategies, allowing mobile money providers to diversify their product offerings and reach more users.[24]

How can data sharing lead to increased customer confidence?

To improve consumer trust and confidence in digital financial services, there must be clear accountability for the mobile money providers. Ensuring consumers have transparency into the use of their personal data through the implementation of appropriate procedures and measures is crucial. These measures include record keeping and the establishment of appropriate contractual agreements between parties, and should be accompanied by modes for redress for the consumers.

Privacy notices drafted in plain and simple language will be also critical to ensuring that consumers understand how their data will be used and the extent to which is it will be shared. To foster consumer trust and engagement, it is important that privacy policies are read and clearly understood by consumers. Concerns have been raised that privacy policies and terms and conditions are not easily understood, and this may form a basis for lack of trust in mobile money services.[25] Ultimately, data sharing can be an effective means of improving trust among consumers towards mobile money services. Incorporating data governance measures and safeguards throughout the customer journey will greatly benefit the industry, as consumers gain access to a wider range of digital financial services.

21 McKinsey & Company (2017). Data sharing and open banking.
22 Financial Action Task Force (2017). FATF Guidance: Private sector information sharing.
23 Wilson, M. (2016). Digital Identity: A prerequisite for financial inclusion? *Mobile for Development Blog*. GSMA.
24 FSD Kenya (2018). Emerging data sharing models to promote financial service innovation: global trends and their implications for emerging markets.
25 Murthy, G. and Medine, D. (2018). Data Protection and Financial Inclusion: Why Consent Is Not Enough. *CGAP Blog*. CGAP.

Data localisation

What is data localisation?

Data localisation refers to the mandate that the personal data of a country's citizens must be stored within the borders of that country. These requirements vary between different jurisdictions so that it applies either to the storage or the processing of data, or in some instances to both.[26] Essentially, these requirements seek to limit the transfer of personal data, with the aim of improving privacy and security, improving the enforceability of consumers' rights with respect to data privacy and, ultimately, boosting local economy by supporting local innovators.[27]

Countries including China, Russia, India, Nigeria and Rwanda[28] have adopted data localisation requirements relating to the cross-border transfer of personal data, demonstrating the increasing need for the industry to explore the implications of these requirements on mobile money services. Cross border data flow is critical for the growth of the digital economy as it provides the foundation for innovation and leads to improved productivity and growth in traditional industries. The freedom to move personal data without restriction between countries generates positive outcomes not only for organisations, but for citizens and countries as well. However, as governments continue to appreciate the value of data, there has been a growing trend of the data localisation requirements in a number of jurisdictions.[29]

What is the impact of data localisation requirements on costs for mobile money providers?

For financial service providers, data localisation requirements stipulate that personal data is stored (and at times processed) within national borders, and in some instances will also require international organisations to set up storage facilities in these countries. The rationale behind this is the desire to attract investment, fuel innovation and create competitive advantage for local companies. Additionally, there is a belief that this will boost employment in the country.[30] However, the real impact of this would be increased infrastructure costs for providers, as was the case in India where the Reserve Bank of India introduced data localisation requirements for payment system providers.[31] While larger players may be able to comply with these requirements, the added obligation may force smaller players out of the market.[32] Therefore, while data localisation is geared towards the protection of the local economy, the reality is that this will have adverse effects for service providers, and potentially lead to increased costs for the consumer.

"In India, [data localisation] will undermine firm productivity and competitiveness, and ultimately the economy's productivity, by forcing firms to spend more than necessary on IT services," "This cost is not only borne by those firms directly impacted by the data localisation requirements, such as financial payment processors, but all IT service users, as it forces everyone to pay more for these services."
Nigel Cory, Associate Director of Trade Policy at Washington-based think-tank Information Technology and Innovation Foundation[33]

26 Reinsch, W.A. (2018). A Data Localization Free-for-All? Center for Strategic & Internal Studies.
27 GSMA (2017). Cross-border data flows.
28 Servers.Global (2016) Meeting the Challenge of Data Localization Laws.
29 GSMA (2018). Cross-Border Data Flows: Realising benefits and removing barriers.
30 Servers.Global (2016). Meeting the Challenge of Data Localization Laws.
31 Facebook, Mastercard and PayPal fear the new law in India, which follows similar measures in China and Vietnam, would increase their compliance and infrastructure costs, and affect planned investments. See: ET Tech (2018). Global tech firms gear up to fight India's planned data law. Reserve Bank of India (2018). Storage of Payment System Data.
32 The Economic Times (2019). Proactively storing all Indian users' data locally, says Truecaller.
33 South China Morning Post (2018). Why Facebook bet US$1 billion on Singapore data centre.

What is the impact of data localisation requirements on data protection and security?

Data localisation requirements are viewed as an opportunity to enhance citizens' privacy and security. While keeping personal data within a country's borders may seem like an appropriate approach to achieving privacy and security standards, there are other implications that compromise the security and privacy of a citizen's personal data. Security in itself has little to do with physical location and more to do with the systems and processes that organisations have in place.[34] The skill and capacity of security experts therefore play key roles in improving security, and there is a stark and noticeable skill shortage in the area of data security which inevitably impacts mobile money providers.[35] In addition to increased infrastructure costs, this will also lead to increased costs for security for each local area, which in itself does not translate to improved security. Centralised security within a group is therefore more cost effective as it leverages a wider range of infrastructure and skill, and results in better investments for business efficacy.

Furthermore, the inability to share personal data limits the country's capacity to respond to threats in a timely manner and effectively apply international cooperation mechanisms that seek to facilitate prompt and timely cyber threat responses.[36] Limiting the free flow of data ultimately creates siloes between authorities in different countries in the fight against cybercrime, and allows cyber criminals free reign as they are not subject to similar restrictions. Fragmentation through localisation may also create barriers that make investments in security protection prohibitively expensive.[37]

Additionally, one of the key requirements for data protection is accuracy of personal data. Fragmented storage facilities could potentially lead to incorrect data in different jurisdictions where data is stored. In the mobile money context, this will impact providers' ability to conduct adequate KYC checks, and may impede providers' ability to meet AML/CFT requirements. Ultimately, while data localisation seeks to provide better security and protection, the reality is that the diffusion of data increases the risk of cyber breaches, while simultaneously hampering the cyber threat response process for these countries.

Cloud-based solutions to security are deemed to be more effective.

"In reality, ring-fencing data to a locality actually narrows the point of attack and creates more security vulnerabilities," he says. "Cloud-based storage ensures that data is distributed at different points of the network, across multiple geographies, to minimise the risks from a single point of failure or breach."[38]

34 Baur-Yazbeck, S. (2018). 3 Myths About Data Localization. *CGAP Blog*. CGAP.
35 Forbes (2018). The Cybersecurity Talent Gap Is An Industry Crisis.
36 Effective mechanisms and institutional structures at the national level are necessary to reliably deal with cyber threats and incidents. The absence of such institutions and lack of national capacities poses a genuine problem in adequately and effectively responding to cyber-attacks. National Computer Incident Response Teams (CIRT) play an important role in the solution. See: ITU (2019). National CIRT.
37 GSMA (2017). Cross-border data flows.
38 South China Morning Post (2018). Why Facebook bet US$1 billion on Singapore data centre.

Conclusion

Data protection is crucial for protecting the gains achieved to date in the fast-evolving mobile money industry. Furthermore, data protection is necessary in maintaining the market integrity and confidence in mobile money services which will prove vital for future growth and sustainability.

Data processing, security, sharing and localisation impact key aspects of the delivery of mobile money services, and necessitate flexibility and adaptability among mobile money providers to keep up with these evolving requirements and meet their consumers' demands.

As mobile technology continues to revolutionise the ways in which users access financial services, the mobile money industry remains committed to meeting the highest standards of responsible business practice in the handling of users' personal data. The industry is at a crossroads concerning data and its protection, and this should be viewed as an opportunity, rather than a hindrance, to increased uptake of mobile money services.

The GSMA remains committed to providing support to our key stakeholders in realising this opportunity. Going forward, we will continue to conduct research to develop practical approaches to the protection of personal data for the mobile money industry, including specific recommendations for mobile money providers and other stakeholders to improve their data protection landscapes. As we continue on this journey, we invite all interested parties to join forces and to work with us to offer best-in-class safeguards to personal data protection for all mobile money users.

Glossary

This Glossary only contains definitions necessary for the context of this report.

Data subject
An identifiable natural person who can be identified, directly or indirectly.

Personal data
Any information relating to an identified or identifiable natural person; an identifiable person is one who can be identified, directly or indirectly, by reference to an identifier: ID number, location data, online identifier, or one or more factors specific to physical, physiological, genetic, mental, economic, cultural or social identity of that person.

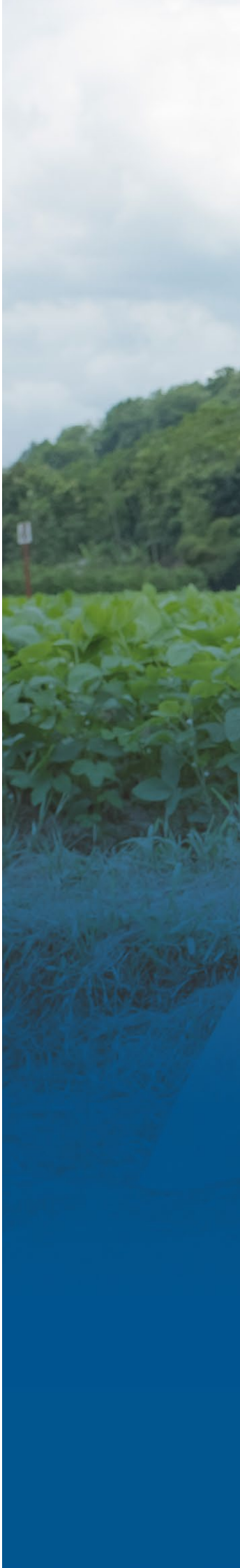
Data controller
The natural or legal person, public authority, agency or other body which alone, or jointly with others, determines the purpose and means of the processing of personal data.

Data processor
A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Data processing
Any operation or set of operations performed upon personal data, or sets of it, be it by automated systems or not. Examples of data processing explicitly are: collection, recording, organising, structuring, storing, adapting, altering, retrieving, consulting, using, disclosing by transmission, disseminating or otherwise making available, aligning or combining, restricting, erasure or destruction.

Data subject's consent
Any freely given, specific, informed, unambiguous indication of which the data subject by statement or clear affirmative or action, signifies agreement to his or her personal data being processed.

Personal data breach
Breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.



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