Guidelines on mobile money data protection

September 2018

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

About this report

Authored by Juliet Maina

Acknowledgements

The author would like to thank the teams from MTN, Orange, Telenor and Vodafone for their time and guidance on the development of these guidelines. The author would also like to extend their thanks to fellow GSMA colleagues, in particular Jade Nester, Brian Muthiora, Nathan Naidoo and Saad Farooq, for sharing great insights and feedback.

Published September 2018

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

Contents

Introduction

Over the past decade, mobile money has emerged as the leading financial service in a growing number of countries. More than one billion dollars is transacted every day, across 276 live deployments in 90 countries.

The business is also changing as it evolves into a payment platform based, in part, on strong data analytics and partnerships with third-party providers. This shift is one of the most significant developments in emerging market financial services since the arrival of mobile money over a decade ago.

More effective use of data represents a substantial opportunity to advance not just access to financial services but economic digitisation more broadly. Data analytics can unlock better fraud detection, improve agent liquidity management, and incentivise businesses to shift from cash to digital. It can also spur the growth of new sectors, for example by providing a digital means of paying for e-commerce goods or facilitating sharing economy services that rely on credit scoring. This is especially significant for low-income consumers, as mobile money emerges as a mechanism through which these consumers can access the wider digital economy.

In this context, it is crucial to ensure that data is not only fuelling innovation, but also that it is handled in a safe and responsible manner. To that end, mobile operators are building on the technical and compliance capabilities of the core GSM business to advance data protection in mobile money. In emerging market countries where data protection regulations are either outdated or yet to be introduced, there is also an active dialogue about how future rules can both ensure consumer protection and facilitate broad access to the digital economy.

The practices outlined below show how leading mobile money providers around the world are approaching the privacy, security, and integrity of consumer data.[1] They reflect initiatives spearheaded by the GSMA and its members since 2009, including the GSMA Mobile Privacy Principles, which is the basis of the Privacy Design Guidelines for Mobile Application Development, the Accountability Framework for the implementation of the GSMA Privacy Design Guidelines for Mobile App Development[2] and the GSMA Mobile Money Certification.

As part of the development of these Guidelines, the GSMA sought input from a range of privacy experts and mobile money providers. The precise implementation of best practice will vary, of course, according to factors such as the nature of the mobile money service and local regulatory requirements. Any practices must also evolve with the release of new technology and the emergence of new risks or service offerings. Nevertheless, those outlined below are rooted in the longstanding OECD privacy principles and in mobile operators' decade of experience in providing mobile money services. The resulting Guidelines aim to inform discussions regarding the protection of mobile money data, today and in the future.

1. None of these initiatives or the principles outlined in this document are intended to replace or supersede applicable law, which varies across different jurisdictions.
2. GSMA. (2016) "Mobile Privacy Principles".

1 Data governance

Providers typically use an overarching framework to shape how data is managed. A clear governance structure and the codification of internal policies and processes are crucial elements of this.

Guiding principles for data governance include:

1.1. Define and implement a privacy policy that commits to fair usage and protection of consumer data, and outlines how access, collection, disclosure, sharing, and retention of personal data are managed.

1.2. Appoint a specific individual or team to oversee good practice in customer data privacy, including through employee awareness programmes and training. This individual/team will undergo relevant training to adequately oversee the implementation of data protection principles in the organisation.

1.3. Develop a strategy that clearly sets out the data protection journey, and the steps to be taken to improve the organisation's data governance framework, including a roadmap with timelines for implementation.

1.4. Implement a risk management approach to data that involves the regular evaluation of risks, including through privacy impact assessments.

2 User choice and control

Users should be provided with information about their personal data. Mobile money providers therefore take steps to provide users with meaningful choice and control over their personal data.

Guiding principles for user choice and control include:

2.1. Limit access, collection, sharing, disclosure and further use of personal information to what is required for legitimate business purposes, such as providing applications or services as requested by users, or as required by legal obligations.

2.2. Ensure users can opt out of the collection or processing of their personal data, where it is not essential to the provision of mobile money services, or to meeting legal requirements.

2.3. Provide customers with the means to access and to amend their data to ensure completeness and accuracy.

2.4. Ensure that these options are made available to consumers in both rural and urban areas and that they account for varying levels of literacy.

3 Data minimisation

A central aspect of best practice by mobile money providers is the minimisation of data. Only the minimum personal information necessary to meet legitimate business purposes and to deliver, provision, maintain or develop applications or render services should be collected and otherwise accessed and used. Personal information should not be kept for longer than is necessary to fulfil legitimate business purposes or legal obligations.

Guiding principles for data minimisation include:

3.1. Carefully consider what personal data will be needed to realise a particular purpose before proceeding with the collection of personal data.

3.2. Document the type of personal data collected, as well as the justification for doing so, as part of information handling policies and practices.

3.3. Minimise the number of people to whom personal data is disclosed or by whom personal data is accessed.

3.4. Once personal information is no longer required to meet a specific legitimate business purpose or legal requirements/obligations, it should be destroyed or anonymised. Truly anonymous data may be retained indefinitely. To anonymise data, remove any information that could be used to identify a specific individual, ensuring it is not possible to re-identify the individual, and ensure that the data cannot be related to a single, unidentified individual by unique identifiers.

3.5. Ensure the proper sanitisation of old devices so that retired hardware does not inadvertently contain personal data, in order to prevent breaches.

4 Openness, transparency and notice

Openness, transparency and notice are key to ensuring that users have a clear understanding of how their data used, enabling them to make informed decisions about whether to use a service.

Guiding principles for openness, transparency and notice include:

4.1. Have an external privacy policy which outlines the purpose of collecting personal data and the data retention and disposal policy for personal data, as well as an indication that personal data will not be shared with third parties unless for a legitimate purpose or business use.

4.2. Through the use of notices, provide users with sufficient information to know how to access and correct their personal information. These notices typically account for varying literacy levels among consumers, and therefore adopt creative means of communication through the training of agents and customer call centre support.

5 Data and information security

Security of personal data is critical to data privacy. Mobile money providers typically implement a number of mechanisms to ensure the security of data. For mobile operators, this effort builds on deep expertise from the core GSM business and is designed to protect mobile money data from loss, or unauthorised access, destruction, use, modification or disclosure.

Guiding principles for data and information security include:

5.1. Develop, implement and regularly review a formal security policy for mobile money services, outlining the organisation's approach to managing its information security objectives.

5.2. Set out clearly the roles and responsibilities of information security teams, including security risk assessments, controls and mitigations. This will also include data breach response plans as well as a designated contact person for all regulatory notifications in the event of a breach.

5.3. Design and develop secure systems, applications and networks for mobile money services in accordance with privacy requirements.

6 Data sharing

As mobile money services continue to evolve, the ecosystem is growing to include more players, such as financial ecosystem partners, or outsourced service providers for systems. The transfer of personal data between third parties is critical, as is the sharing of data within organisations, and this may occur across different national or regional legal jurisdictions. Where a provider permits access to or transfer of personal data through systems external to the organisation, as may be required for legitimate business purposes, mobile money providers must take step to ensure the data remains protected.

Guiding principles for data sharing include:

6.1. Where personal data is transferred (either to third parties, or to other departments within the same organisation) providers set minimum default policies for sharing personal information that may pose risks to customers.

6.2. Written agreements governing data privacy will be in place with all third parties that either process personal data or have access to personal data. These will typically include responsibilities for data privacy as well as further restrictions to personal data sharing.

7 Accountability

Accountability applies to the measures implemented by mobile money providers which will serve to demonstrate adherence to the principles of data protection, as well as compliance with other applicable laws and regulations.

Guiding principles for accountability include:

7.1. Assign responsibility for ensuring the user's privacy is considered and protected throughout the product lifecycle and through applicable business processes.

7.2. Establish an organisational commitment to accountability and to the adoption of internal policies consistent with the Guidelines.

7.3. Introduce systems for ongoing internal oversight and assurance reviews.

7.4. Introduce transparency and mechanisms for individual choice regarding the use of their personal data.

Conclusion

Data protection is critical to ensuring the provision of consistent, high-quality service as the mobile money business evolves. It is a core driver of economic digitisation that promises not only to extend financial inclusion, but also to encourage owners of mobile devices to interact with a diversity of digital services.

We hope that these Guidelines will help to facilitate ongoing dialogue on data protection. Collaboration between mobile money providers, regulators and other relevant stakeholders is critical to the evolution of industry best practice and regulatory frameworks that are fit-for-purpose in a world of rapid technological progress and persistent barriers to universal financial inclusion.

As the GSMA continues to support the industry in implementing appropriate safeguards in the use of personal data, we invite all interested parties to work with us to ensure that personal data is protected, and that the full social and economic potential of mobile money is realised.

For more information on GSMA Mobile Money, visit
gsma.com/mobilemoney

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