Responsible Finance Forum

# Opportunities and Risks in Digital Financial Services: Protecting Consumer Data and Privacy

RESPONSIBLE FINANCE FORUM VIII

27-28 APRIL 2017
BERLIN, GERMANY


GPFI

Federal Ministry for Economic Cooperation and Development

giz

IFC International Finance Corporation WORLD BANK GROUP

# CONTENTS


PROTECTING
CONSUMER DATA
AND PRIVACY

# ACRONYMS

| | |
|---|---|
| A2II | Access to Insurance Initiative |
| ADM | Automated decision making |
| AML | Anti-Money Laundering |
| AI | Artificial Intelligence |
| BaFin | Federal Financial Supervisory Authority (Germany) |
| BMZ | German Federal Ministry of Economic Cooperation and Development |
| BTCA | Better Than Cash Alliance |
| CGAP | Consultative Group to Assist the Poor |
| CTF | Counter-Terrorism Financing |
| DFS | Digital Financial Services |
| EU | European Union |
| FI | Financial Institution |
| FinTech | Financial Technology |
| FSP | Financial Service Provider |
| G2P | Government to Person |
| G20 HLP | G-20 High-Level Principles for Digital Financial Inclusion |
| GDP | Gross domestic product |
| GDPR | The European Union General Data Protection Regulation |
| GIZ | Deutsche Gesellschaft für Internationale Zusammenarbeit |
| GPFI | Global Partnership for Financial Inclusion |
| GSMA | Groupe Spéciale Mobile Association |
| IAIS | International Association of Insurance Supervisors |
| IAMTN | International Association of Money Transfer Network |
| IFC | International Finance Corporation |
| ILO | International Labour Organization |
| InsurTech | Insurance Technology |
| IPA | Innovations for Poverty Action |
| IT | Information technology |
| KYC | Know Your Customer |
| MFI | Microfinance Institution |
| MNO | Mobile Network Operator |
| MSME | Micro, small and medium enterprises |

| | |
|---|---|
| MTO | Money Transfer Operator |
| NFIS | National Financial Inclusion Strategy |
| NGO | Non-Governmental Organization |
| OECD | Organization for Economic Co-operation and Development |
| OTC | Over-the-Counter |
| P2P | Person to Person |
| PRI | Principles for Responsible Investment |
| PSD2 | The Second Payment Services Directive EU |
| PSP | Payment service provider |
| RDF | Responsible Digital Finance |
| RFFVIII | Responsible Finance Forum VIII |
| RFID | Radio-frequency identification |
| RM | Risk Management |
| SASSA | South African Social Security Agency |
| SDG | Sustainable Development Goals |
| SMS | Short message service |
| SSB | Standard-Setting Body |
| T&Cs | Terms and Conditions |
| Telco | Telecommunications Company |
| UFA | Universal Financial Access |
| UK | United Kingdom |
| UNCDF | United Nations Capital Development Fund |
| US | United States |
| USAID | United States Agency for International Development |
| WBG | World Bank Group |
| WFP | World Food Programme |

# ACKNOWLEDGEMENTS

The Eighth Annual Responsible Finance Forum (RFF VIII), Opportunities and Risks in Digital Financial Services: Protecting Consumer Data and Privacy, was held in Berlin, Germany and made possible by the leadership of the German Ministry for Economic Cooperation and Development (BMZ) as holder of the 2017 Presidency of the G20 Global Partnership for Financial Inclusion (GPFI) and the German Society for International Cooperation, Deutsche Gesellschaft für Internationale Zusammenarbeit GmbH (GIZ).

This report is a product of the collaborative work of RFF VIII partners and organizers. The report was produced by a core team who provided detailed session notes and critical contributions from the Forum, namely: Momina Aijazuddin, International Finance Corporation (IFC); Joscha Albert, GIZ; Amil Aneja, United Nations Capital Development Fund (UNCDF); Elena Babkova, IFC; Florian Berndt, GIZ; Wolfgang Buecker, GIZ; Lory Camba Opem, IFC; Louis de Koker, La Trobe Law School; Judith Frickenstein, GIZ; Ros Grady, Better Than Cash Alliance (BTCA); Volcker Hey, German Federal Ministry of Economic Cooperation and Development (BMZ); Michelle Kaffenberger, Consultative Group to Assist the Poor (CGAP); Johannes Kinzinger, IFC; Kate McKee, CGAP; Margaret J. Miller, World Bank; Jutta Niemann, GIZ; Konstantin Pagonas, GIZ; Beth Porter, UNCDF/BTCA; Maren Springsklee, GIZ; Boyan Stanoev, IFC; and Malak Yusuf, IFC.

On behalf of the Responsible Finance Forum team, we are grateful to the more than 120 participants and partners[1] who committed their time, imparted their insights, and shared candid experiences during the Forum.

The production and publication of this report was made possible with the institutional support and commitment of the German Ministry for Economic Cooperation and Development (BMZ) and the International Finance Corporation (IFC).

The Forum encourages new and current partners and members to stay engaged.

Visit us at: www.responsiblefinanceforum.org.

## About the Responsible Finance Forum

The Responsible Finance Forum (RFF) has been an annual landmark event in the financial inclusion field since its inception in 2009. Each year, the Forum convenes the private sector, development partners, governments, regulators, practitioners, policymakers, academia, and consumer advocates to exchange insights, innovations, and experiences in identifying emerging best practices, concrete solutions, and ongoing initiatives to broaden responsible financial inclusion on a global level.

The First Annual RFF was hosted in Berlin by the German Federal Ministry for Economic Cooperation and Development (BMZ), and conducted by the Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ). It marked its launch among co-founding partners, the Consultative Group to Assist the Poor (CGAP), and the International Finance Corporation (IFC).

The RFF has since evolved into a virtual Platform dedicated to advancing new innovation, evidence, solutions, and best practices to expand financial inclusion and responsible digital finance. The RFF partner community continues to expand, with over 20,000 unique visitors to its Platform, in addition to a featured Annual Forum delivered in collaboration with Our Partners.

RFF partners have included: the Access to Insurance Initiative (A2II), the Better Than Cash Alliance (BTCA), the Bill and Melinda Gates Foundation, Citi Foundation, the German Federal Financial Supervisory Authority (BaFin), the Financial Times, the International Association of Insurance Supervisors (IAIS), Innovations for Poverty Action (IPA), the International Labour Organization (ILO), MasterCard Foundation, the Microinsurance Network, Munich Re Foundation, Principles for Responsible Investment (PRI), the Netherlands Ministry of Foreign Affairs, the Small and Medium Enterprise Finance Forum, the United Nations Capital Development Fund (UNCDF), and the World Bank Group (WBG).

The Forum encourages new and current partners and members to stay engaged.

Visit us at: www.responsiblefinanceforum.org.

# FOREWORD

Responsible digital finance has continued to be a cross-cutting priority of the G20 Global Partnership for Financial Inclusion (GPFI) since 2014. A cornerstone of the Universal Financial Access (UFA) goals of the World Bank Group by 2020[2], responsible digital finance also seeks to help achieve the United Nations' Sustainable Development Goals (SDGs) by 2030[3].

Representing the G20 Presidency in 2017, Germany heightened the importance of digitization, and the topic of data protection/privacy and security was embraced by key implementing partners and all four Sub-Groups of the Global Partnership for Financial Inclusion[4].

The Responsible Finance Forum (RFF VIII) in Berlin focused on **Opportunities and Risks in Digital Financial Services: Protecting Consumer Data and Privacy.** The event probed more deeply into the dimension of the G20 High Level Principles for Digital Financial Inclusion (G20 HLP)[5], endorsed under China's G20 Presidency in 2016.

This year, the Forum delved into the following areas:

**Identifying opportunities, risks, and policy approaches needed to address data-enabled digital financial services (DFS)**. The Forum provided participants with the opportunity to discover the perspectives of diverse stakeholders, for example, retail providers, FinTechs, regulators, policy makers, consumer advocates, development partners. Discussions revolved around how to most effectively address the risks and opportunities of DFS as the basis for identifying common ground, and defining the roles and responsibilities for each stakeholder profile.

**Unpacking big data innovations and the role of industry**. The question of how various stakeholders (for example, industry, financial providers, FinTechs, banks, Mobile Network Operators, and so on) can acknowledge and respect consumer privacy while simultaneously advancing innovation and inclusion, was explored during the Forum's meetings.

**Translating insights into action.** Focus Sessions captured participant insights and priority actions across four areas: Policy and Regulation, Industry Standards, Consumer Perspectives, and Development Partners. These areas were addressed in relation to issues of privacy and data protection as linked to digital financial services. Remaining gaps in these focus areas were noted, particularly from the various stakeholder perspectives and roles.

**Focus on shared goals and forging partnerships in moving forward.** With increasing digitization, members of the G20, GPFI, and all stakeholders must promote measures that ensure responsible financial inclusion as applied to digital financial services.

We hope this report will serve as a call for action that will resonate among Forum participants and beyond. We invite new and ongoing partners to join us and stay engaged in advancing responsible digital financial inclusion.

# I. OPPORTUNITIES AND RISKS OF DATA-ENABLED DIGITAL FINANCIAL SERVICES: TWO SIDES OF THE SAME COIN

"The data-driven approach offers the opportunity to do digital finance right, especially in applying behavioral insights"

Jonathan Dixon,
Financial Services Board, South Africa

## Overview

In an increasingly digitized world, opportunities for expanding financial inclusion are going great distances to provide access to finance for the world's 2 billion adults without a formal financial account. A recent McKinsey study[6] illustrated that digital finance could increase the gross domestic product (GDP) of emerging economies by 6 percent, or a total of US$3.7 trillion by 2025. This additional GDP could also create up to 95 million potential new jobs across all sectors of the economy. Digital financial services have contributed more to financial inclusion in the last few years than any other business approach. With 700 million new accounts created between 2011 and 2014, it has reached previously unserved consumers, mainly via mobile phones and agents. Governments are also gradually digitizing payments such as social transfers, financially including millions of previously unserved lower-income groups in remote areas.

These figures underline the significant potential of digital finance. As such, this session considers both the opportunities and risks.

## Opportunities

Basic services such as airtime top-ups and person-to-person (P2P) payments are by far the most common use cases in DFS, yet there has also been rapid growth in more complex and value-added services. New uses of data and new types of data have enhanced every stage of the product cycle from customer segmentation to product design, marketing, loan servicing, and insurance claims. Digital financial services providers and their business partners now have

the opportunity to develop new products and services, especially as the field moves beyond payment services such as bill pay, credit for consumers and small businesses, and insurance. Data-enabled DFS can also be better tailored to fit consumers' specific needs. In addition, the use of customer data could help improve consumer awareness, understanding and behavior, for example, by providing "just-in-time" prompts that capitalize on information about consumer preferences and insights regarding how to positively influence consumer financial behavior.

"Particularly for emerging economies, digital technology holds the potential of leapfrogging development"

Thomas Silberhorn, BMZ

## Risks

Data collected through mobile phones and telecommunications—such as call data records, airtime top-ups, transaction data for consumers, and micro, small and medium enterprises (MSMEs)—are exponentially increasing "digital data trails" of customers, including lower-income consumers in developing and emerging markets. The creation and rapidly increasing usage of digital data trails by firms providing digital financial services has raised the issue of consumer risks that are currently not well understood by consumers, industry, or government actors. This is particularly concerning in nascent markets where large numbers of lower-income consumers are accessing services in countries where consumer protection and data protection frameworks, regulation, and supervision are underdeveloped.

Some of the risks stem from demand-side factors, such as limited consumer digital literacy, unfamiliarity with formal finance, and issues of financial capability. There are also critical risks on the supply side. For example, rarely are digital financial services systems in emerging markets encrypted from end-to-end; this weakness raises data security risks—from handset use through to service platforms and networks. Cybersecurity risks can facilitate consumer loss of privacy and inflict financial harm, such as identity theft. In addition, it can put providers at risk and undermine public confidence in the digital finance eco-system. Another example is the use of non-traditional data and advanced data analytics to create proprietary algorithms for credit scoring. Although these developments can facilitate the extension of credit to previously unserved people, they could also lead to exclusion if data is inaccurate or the outcomes of the algorithms about different segments are not monitored carefully. The lack of rules or standards about data collection, usage, storage, accuracy and sharing can create or exacerbate privacy loss and other risks.

In sum, the increased use of and access to customers' digital footprints along the data chain through outsourcing and business partnerships creates the following consumer risks, namely: a) fraud, b) identity theft, c) loss of privacy, d) inaccurate profiling, leading to fewer or costlier offers, e) inaccurate credit scoring and insurance underwriting, f) data breaches and loss of consumer trust, and g) cybersecurity risks including business disruption.

"We need end-to-end encryption for DFS – the processes are insecure at every stage"

Bhairav Acharya, India

## Key Takeaways

- Opportunities and risks exist on every level (consumer, firm, market, country).
- Although not all risks translate into actual harm, inadequate data protection practices, standards, and rules can result in consumers in both emerging and developed markets experiencing financial harm, loss of privacy, and/or reduced trust.
- Informed consent is not enough to mitigate these risks. Product terms and conditions (T&Cs)in user agreements tend to be insufficiently transparent, one-sided to the benefit of the provider, or both. Consumers have limited opportunity to opt out of non-consensual data collection or push marketing through short message service (SMS) messages.
- Self-regulation through industry-driven data protection standards and codes of conduct is still a greenfield topic in digital financial services. In this context, it is important to devise workable standards and actionable guidelines for industry providers and players.
- Create a policy environment that is proportionate to the benefits and risks, that is, enabling yet protective. There is a good case for ongoing consultation between the relevant authorities and industry, as well as the need for close coordination among the multiple authorities responsible for overseeing the market.
- Joint research, learning, and collective understanding of DFS risks are needed to shape guidelines, standards, and regulations. It is also important to build cooperation both domestically and globally, as well as capacities to close the evidence and knowledge gaps.

# II. INNOVATIONS AND PREDICTIVE MODELS FOR BUSINESS GROWTH: ADVANCING DATA PRIVACY AND SECURITY


"The default assumption is that everything is vulnerable"

Martin Holtmann, IFC

## Overview

Innovation in the digital financial services space has naturally put pressure on FinTechs, financial providers, microfinance institutions, and digital financial services providers to swiftly become strategically data-driven—that is, to create more accessible products and services tailored to customers' needs in order to remain competitive. This session presented perspectives from pioneering financial service providers who offered insights from their business models. It also addressed emerging consumer and institutional risk management practices for sustainable development.

## Models for Business Growth

**MicroCred Group**[7] presented its approach to digital transformation, which encompassed three layers: 1) A distribution network, 2) Product creation, and 3) Usage/adoption of digital products. MicroCred launched its digital finance operations in two pilot countries, Madagascar and Senegal. Specifically, it deployed an agent network and introduced a fully automated loan product based on predictive credit scoring, delivered digitally through biometrics. MicroCred's digital transformation generated not only an increase in net income, but also produced a sizeable scale-up of the customer base.

MicroCred only uses its own data (that is, data related to transactions, registration) for scoring and then leverages its customer relationships. MicroCred addressed operational risks with regard to consumer protection and data privacy. It invested in information technology (IT) security infrastructure to ensure the highest security standards. It also reduced costs to deliver services to its clients by developing a fully automated credit scoring model. Customer data is not shared outside of the company, nor does it purchase external data in building algorithms and devising behavioral scoring.

**Equifax**[8] collects data from various external data sources to analyze and establish credit scores for clients across the globe. The company's data is centrally held on behalf of all financial institutions and safe-guarded with security measures to protect consumers' credit score data. Regulatory policies are shaping the lending business, such as "open banking" Application Program Interfaces (APIs), MyData, Payment Services Directive 2 (PSD2)[9] (the new European Union [EU] payment rules that take effect in 2018), and the new data protection law, the General Data Protection Regulation (GDPR)[10], which extends the right of "data portability" to consumers. Customer data is increasingly held almost as a "personal data store" (for example, as in the India Stack digital-locker concept in India)[11].

The fragmentation of data use and storage will require more robust data security protocols. Technology is moving at a startling pace, set against regulation that is falling behind. How can the industry "consent" when data can be transferred instantaneously? The industry is finding that consumers are being left behind because they do not fully understand the advancements in digital security.

**Kreditech Holding**[12] promotes the goal of transforming the traditional method of borrowing by applying an algorithm to customer-informed data. This effort ensures that credit decisions are not biased by guarantor perceptions. For Kreditech, data privacy and consumer protection are imperative, especially in environments where customer understanding is limited. Kreditech's proprietary algorithm analyzes up to 20,000 data points, and it builds country and product-specific algorithms, including "self-learning" algorithms for dynamic scoring. Kreditech is aware of the challenges of obtaining truly meaningful and informed consent as required by the GDPR. As such, it introduces the privacy notice early in the online registration process. Kreditech applies a "privacy-by-design" principle, in which the design, data protection, and IT teams collectively build a privacy notice that contains the most succinct information for the customer. In this context, it clearly outlines what data is collected, why, for what purposes, including also associated security measures. In addition, it provides complaint contact information so that customers can directly contact Kreditech.

**MasterCard** Europe, a global cards and payments company, has observed a lack of harmonization between different countries in advancing data privacy and security. Regulation has to be centrally planned, but locally implemented. Data tends to be stored locally, but moves internationally. The free flow of data is required in order to build trust in financial service providers. MasterCard is also prioritizing the protection of consumer privacy while accelerating financial inclusion. In doing so, a toolbox should be created that goes beyond consent. Many safeguards should be explored and consumers need to be in control of their data. Informed consent is not the only compliance tool.

In Europe for instance, for it to be valid, consent cannot be grouped with terms and conditions (T&Cs). Rather, consent must be freely given. Consent has other limitations as well. Fraudsters will not consent to give up data about their activities. Prospective borrowers cannot choose which data about their previous loan repayment performance will be shown to a lender. The principle of "accountability" needs to be encouraged; companies must demonstrate that they are complying (for example, by adhering to the GDPR).

The distinction between data protection and privacy is quite significant. For instance, the risk of consumers being blacklisted for very small amounts with disproportionate consequences has become a concern in many countries. Recently, over 400,000 Kenyans were blacklisted for loans of US$ $2 or less, without any explanation or recourse.[13] Furthermore, exclusion by complexity, or by any metric — such as digital literacy, demographics, financial experience, or knowledge — all greatly impact a consumer's use of and trust in digital financial services.

Overall, the discussion among these companies illustrated the effectiveness of innovative business model development in financially including the previously unbanked at noticeably lower costs. However, digital business models entail a variety of operational risks, with consumer risks become significantly more important. Regulations are currently decentralized, and there is a universal need for more harmonized regulation. If changes do not occur over time, digital business models may be undermined and consumers will lose confidence in the benefits offered by digital financial services.

## Key Takeaways

- Data science is only half of the picture. Customer service design needs to interact with clients as well. Tailored products also need to be created. Finance needs to become less complex for those with unstable incomes and severe liquidity gaps.
- Regulations are being developed. For example, the PBOC introduced its first major internet finance guidance policy last year to strengthen consumer protection and curb mismanagement and fraud.
- Reduce the risk of digital exclusion for certain segments of the global population. The industry is at risk of disenfranchising those who are digitally less-literate.
- Data protection versus accelerating financial inclusion: How does the industry ensure that consumer data is well protected while not harming digital financial inclusion (which relies on efficient access to data)?
- Regulation has to be harmonized and centrally planned. However, it is implemented locally in accordance with developing country jurisdictions. Data needs to be free flowing to demonstrate its full potential and value. Regulators have to become more technology-savvy and improve their knowledge of digital business models.

“Consumer protection is “the salt in the soup”, because although no one can see it, when eating the soup everyone will taste it. Regulators need to demand that the right quantity of salt is added to the soup, while simultaneously making sure that the salt does not spoil the soup altogether”

Thomas Silberhorn, BMZ

# III. EFFECTIVE DATA PRIVACY REGULATION AND SUPERVISION OF DIGITAL FINANCIAL SERVICES


## Overview

Whereas regulatory frameworks for data privacy have evolved in recent years, emerging market regulations in particular have not kept pace with dynamic changes in the digital financial services industry, including the use of alternative data by FinTechs, InsurTechs and other financial institutions. This session discussed some key challenges and possible solutions to effective data privacy regulation and supervision of digital financial services.

### Consider the vast numbers of public and private actors involved

A challenge for data protection regulation and supervision stems from the many actors involved in handling data—such as traditional financial institutions, Mobile Network Operators (MNOs), Money Transfer Operators (MTOs), and FinTechs. As a result, a range of regulatory bodies are involved. As such, a complex situation has emerged that requires improved coordination and dialogue between multiple regulators, including the formation of new and effective cooperative mechanisms for doing so.

In **Uganda**, GIZ, on behalf of the BMZ, helped to establish a dedicated Financial Innovations Sub-Committee at the Bank of Uganda. A joint Working Group between the Bank of Uganda and the Uganda Communications Commission was created as a platform to share information, define regulatory and supervisory roles, and collaborate on implementing provisions across the two regulators' mandates. This joint effort led to the issuance of Mobile Money Guidelines by the Bank of Uganda. The Guidelines contain a section on consumer protection, including issues related to agent supervision and pricing transparency, particularly for the less literate, low-income poor.

### Keeping up with technological advances

Effective regulations need to enable rather than impede. Therefore, sufficient knowledge will be required to help regulators maintain the right balance between innovation and risk prevention. However, technological advances are evolving faster than the ability of regulators to

enact appropriate regulations. Regulators in the U.S. have addressed this issue by hiring technical staff to initiate discussions with chief technology officers of digital financial service providers regarding technological issues potentially touched by regulations.

## Industrial self-regulation and controlled innovation space to support industry advancement

Innovation is needed to further advance financial inclusion just as much as regulation is needed to secure responsible developments that will benefit and not harm consumers. In order for both to proceed hand-in-hand, while accepting that market development moves rapidly, avenues will have to be found that allow digital innovations in a controlled space. "Sandboxes" or pilot areas/projects have been found to serve as attractive solutions to this problem.

Further, to complement regulatory efforts, self-regulation of the industry remains critical in the digital financial inclusion space. Self-regulation efforts in the insurance sector in Tanzania, for instance, work well. In general, however, successful self-regulation depends on proper incentives combined with market discipline. Industry initiatives can further complement regulatory and supervisory efforts to promote consumer protection and data privacy.

### Key Takeaways

- There is a lack of appropriate regulatory and supervisory tools and checklists that address relationships between actors such as FinTechs and telecommunications regulators.
- There is a need for strengthened coordination between different regulatory/supervisory bodies that are active in a given market.
- Data protection principles need to adapt according to technology changes. Regulators need to improve their technological knowledge to better understand risks, as well as to keep up with the rapid pace of FinTech innovators.
- Industry self-regulation can be effective, given proper incentives and market discipline.
- Industry innovators, providers, and regulators should convene to forge agreements on data protection standards that would serve as an effective model of (self-) regulation. These would be applicable to and localized across different markets.
- There are various possibilities to allow for digital innovation in a controlled space, such as sandboxes or the identification of areas that would not be affected by regulation.

# IV. INDUSTRY APPROACHES TO DATA PRIVACY AND PROTECTION

## Overview

Industry practitioners considered potential industry approaches to data privacy and protection, the consequences of adverse practices, and the limits of informed consent in the digital context—particularly in low-access and low-regulatory capacity environments. Self-regulatory initiatives in digital financial services are accordingly becoming an important industry imperative.

This session presented the Responsible Digital Payments Guidelines developed by the Better Than Cash Alliance (BTCA)[14] as part of the discussion about key consumer and data protection risks facing the industry and its customers. There was a particular focus on BTCA's Guideline #7 concerning the need for data confidentiality and security, while also recognizing the use of client data to increase customer access and usage.

The **South African** Social Security Agency (SASSA) provides social grant payments to about 10 million beneficiaries and reaches remote parts of the country's population across nine provinces. In 2011, SASSA contracted an external, single-service provider to deliver, distribute, and pay out grants to the beneficiaries. With a single provider having access to the social grant beneficiary data, this presented a risk — especially when combined with weak supervisory enforcement to protect consumers and the privacy of their data. Unauthorized deductions occurred, including airtime and digital insurance transactions. Two lessons emerged from this experience. First, all operational and systemic risks and related procurement contracts should be carefully assessed when planning significant payments programs. Second, it is necessary to ensure that the program manager has the required capacity, and that the contractors involved are committed to protecting consumers in line with consumer market and data privacy regulations.

**VEON**[15], a global telecommunications provider, shared its digital transformation projects across countries. Data privacy laws affect the decision-making mechanisms of platform providers and the services they can offer. For example, whereas in some countries it is possible to use air time credits for diverse purposes, in others, it is not. In addition to being used to create credit scores, such data can be used for humanitarian purposes. For instance, following a major storm in Mexico, VEON provided data on airtime use in affected areas, which was then used to focus aid efforts in regions where abnormally low levels of use were recorded. The result was a positive impact of the use of airtime data, which would not have been possible in some countries (such as Pakistan). Algeria and Bangladesh are examples of other countries in which VEON cannot offer digital financial services because of their data privacy laws.

There is a perceived dichotomy between the need for data privacy, and the positive uses of data. However, this is a false idea of how the discussion should be framed. The industry should move toward creating trust and building an environment that takes privacy into account, while also considering the perspectives of both industry players and consumers regarding the proposed uses of data. Furthermore, users should be given the option of whether to consent to available services.

Having industry self-regulatory standards is important, especially in countries where there are no data privacy laws, or where the laws do not apply to or are not being followed by all market participants. Another option (which VEON employs) is to voluntarily follow the new EU General Data Privacy Regulation as a form of self-regulation.

## Informed Consent

Recent research has explored the conceptual meaning of "informed consent". Informed consent is commonly used as a justification for various collection, use, sharing, and data storage practices. It is the subject of diverse standards and provider approaches. The consent approach has its roots in the model of data protection based on the Fair Information Protection Principles developed in the U.S. in the 1970s. The underlying rationale for this approach is that users should have the freedom and autonomy to control the use of their data based on the price they are offered. However, this approach has come under increasing criticism in the world of modern data practices.

The central theme of concern regarding the "informed consent" model is that there is no real notice and no real choice. In recent years, invisible and pervasive data surveillance, collection, analytics, and aggregation of data have been developed. Data can also be stored indefinitely and at low cost. Further, consumers do not know the who, when, why, and what of data practices. Current research also suggests that less than 1 percent of consumers read privacy notices. If they chose to do so, it would take roughly 244 hours a year on average to read these often-complex documents. As an example, it has been suggested that two-thirds of global Facebook users do not understand the privacy settings they have in place. This results in a "take it or leave it" situation because users do not have a meaningful choice if they need the underlying product or service.

The barriers to informed consent are even more acute in developing countries where consumers have low literacy levels, and are dealing with unfamiliar financial products. In addition, there

is often less competition among providers, and few data privacy and protection laws or effective regulations are in place. There are alternatives to the consent model that focus on procedural, rather than substantive, rules which aim to reduce risk while also meeting reasonable consumer expectations.

To further explain variations of consent:

**"Privacy by Design"** is an approach that seeks to embed protection of consumer data as part of the design of any new product, service, or system from the very beginning[16].

**"Data Minimization"** is an approach that requires careful consideration of the purpose for which data is to be used; as such, it minimizes the data collected, and holds it for the minimum time.

## Key Takeaways

- All operational and systemic data risks should be carefully assessed when planning any large-scale public or private payments programs, including the risks with any outsourced service provider.
- Data privacy and protection regimes should be flexible, considering both industry and consumer perspectives and the proposed uses of data.
- Having minimum industry self – regulatory standards is important, especially in countries where there are no data privacy laws.
- An alternative to the current "informed consent" model needs to be developed as forms of consent are often not read or are too complex to understand and the consumer does not in any event have a real choice. These concerns are especially acute for consumers in developing countries.
- Possible alternatives to the consent model are the "Privacy by Design" and "Data Minimization" approaches

# V. ALGORITHMS, ANONYMIZATION, AND APIs: EVERYTHING YOU WANTED TO KNOW ABOUT BIG DATA

## Overview

Industry terminology is not always well and fully understood, or used consistently, in the general discussion surrounding big data. Regarding data ownership, no one owns information from a legal perspective, except for corporate trade secrets. Data architects and engineers discuss "ownership" more in the sense of accountability, that is, who is or should be responsible. Data protection covers more than collection, usage, and storage of private information. It also deals with integrity, access, and security.

## Big Data and Financial Inclusion

Big data is commonly defined as being characterized by the "3 Vs": **Variety** of data types and sources, the accelerating **Volume** of data, and the **Velocity** with which data is being generated. In the context, the industry must add the important development of application of advanced analytic techniques (for example, search optimization engines, automation, machine learning, artificial intelligence) to find, structure, combine, and assess data for various purposes.

The main categories of big data include: human generated data, transactional data, biometric data, and machine-to-machine data (for example, the Internet of Things, Radio-frequency identification [RFID]). Advanced analytics includes (semi-) automated tools to analyze data. Algorithms are rules followed in order to achieve a task. All of these categories of big data are based on models which pose a series of questions to abstract a process. The questions are designed by humans and can reflect human bias. The data chosen as the basis for algorithms does not necessarily represent the real world—indeed, the data is a set of proxies.

"Algorithms are a necessary evil"
Peace Osangir, Kopo Kopo, Kenya

To further address common perceptions surrounding big data and its relevance to financial inclusion, it is important to note that there are doubts about whether meaningful consent in relation to digital financial inclusion is simple to achieve and/or effective in its purpose. Some report that most consumers are not all that concerned with data privacy, and plainly trust the system. Another questionable belief is that algorithms are fairer than human bias, and anonymization works well enough to protect consumer privacy. Further, the question remains whether liability frameworks have the ability to protect consumers if there are data breaches and/or they become exposed to other weaknesses in data protection systems.

Regarding the usage of algorithms, entities can also work on providing supporting evidence about the breakdown of the algorithms they employ. This would provide for added clarity and understanding of data uses and parameters. These steps are critical to ensure that consumers can build and maintain trust in digital financial services as it relates to responsible finance and protection.[17]

## Key Takeaways

- The use of exact terminology and definitions helps to break down complex issues.
- Algorithms use a set of information as proxies to analyze data (for example, to determine credit risk). The selected set of information and indicators are choices, which can be biased by cultural choice and specific beliefs. Wrong choices lead to wrong outcomes, such as racial discrimination.
- Making algorithms public is not a solution that optimizes effectiveness. If companies are required to disclose all the details of their algorithms, investments will likely not suffer, but consumer behavior could be distorted.
- Big data debates tend to break down between the cheerleaders and naysayers. Moving forward, the industry must take a more nuanced approach to identifying and addressing the risks and opportunities by adopting a collaborative approach.
- Further research and consultations are necessary to determine specific recommended actions.

# VI. FOCUS SESSIONS: TRANSLATING INSIGHTS INTO ACTION FOR DATA PROTECTION AND PRIVACY

## 1. POLICY, REGULATION AND SUPERVISION

### Insights

While there is broad agreement that data protection for DFS should be enhanced, there are significant gaps in knowledge and evidence. Policymakers, regulators, and supervisors should gather more **evidence** to inform effective data protection regulation and supervision for DFS. Likewise, supervisors should enhance their data protection **capacity**. Improvements that can be made based on current knowledge and understanding should however be implemented without delay. Indeed, improvements in protection are urgently required. Meanwhile, evidence gathering to inform ideal regulatory approaches will require time. Research agendas should be planned and supported with sufficient resources. They should also allow for the investigation and assessment of the broad range of potential harm that may flow from data and privacy breaches in relation to DFS. Efforts should also address unintended consequences that data protection rules may have on financial inclusion efforts.

Data protection, for example, recognizes the right of an individual to access information regarding the reasons behind any decisions generated by automated-decision-making (ADM) means. While this right of access to information about the use and application of a person's data is valued, it can impact negatively on ADM in such a way that may lower the costs of financial services for lower income persons. For example, disclosure may hinder innovation because disclosing the details of the business model to competitors may render the development of

the system commercially unviable. Transparent ADM systems may also be susceptible to gaming by customers. In this regard, disclosure assumes that users are able to identify and take action in cases in which their data is being used inappropriately. Alternatively, they may have easy access to advisors who can assist them to seek redress. Such assumptions cannot be reasonably made in many developing markets where DFS are currently flourishing. Answers may lie in appropriate transparency vis-a-vis effective supervision rather than exposure to the greater public.

It was agreed that **self-regulation** is influential and may be advisable in some markets. While responsible self-regulation may be particularly helpful where there are no laws or laws only in a nascent stage, they should always be supplemented by appropriate government regulation and supervision. Some countries with DFS models do not have effective data protection laws in place and/or find it challenging to implement these laws. Where laws are absent or dated, institutions should be encouraged to implement compliance processes reflecting accepted core principles (for example, those articulated by the Organization for Economic Cooperation and Development [OECD][14] or the GDPR).

Regulators and supervisors require **human and institutional training** involving technical issues around data protection in DFS. This will help to strengthen their capacity to build and maintain effective and enabling regulatory data protection frameworks. A possible practical measure would be to help regulators analyze their own data protection regulatory and supervisory regimes using a diagnostic toolkit. This could include landscape surveys with the private sector to identify what is occurring in practice, as some of the standards rules and regulations may not be needed in certain markets at certain stages or may need to be modified. Such an approach could also help to address the cross-sectoral nature of data protection issues in DFS, which requires a formalized collaboration between regulatory bodies and other stakeholders at the domestic level.

It is clear that **cooperation** is required between the public and private sectors, but also between the actors within each of these sectors. A key issue in advancing data protection regulation in DFS is the question of **ownership and responsibility**. Which regulatory body will move the discussions forward globally and locally, and coordinate cross-sectoral efforts? While collaboration is essential, at this stage, it does not appear feasible to attempt to work toward a uniform data protection law or detailed set of standards that can be applied globally. It would be more realistic to work toward common terminology and agreement on meta-level principles for data protection that may in turn help inform domestic laws in different countries.

Furthermore, the interplay between Anti-Money Laundering and Counter-Terrorism Financing (AML/CTF) and data protection must be taken into account. The conversation with the Standard-Setting Bodies (SSBs) should also be promoted. Within the **Global Partnership for Financial Inclusion,** this could be advanced within the SSBs Subgroup. As a whole, the GPFI is a key platform to coordinate efforts regarding data protection in DFS globally. It does so by working within and across the Sub-Groups, which include program implementation and collaboration across the public and private sectors.

## KEY ACTIONS

- Build a stronger base of evidence about potential consumer harm and risks.
- Strengthen customer empowerment, knowledge, and risk awareness.
- Streamline global and in-country policies by:
  - Encouraging conversation between SSBs and global bodies for data protection and privacy to identify core principles to be implemented.
  - Encouraging conversation between different regulatory bodies at the domestic level.
  - Supporting capacity-building and peer exchange.
- Developing a diagnostic toolkit to allow regulators to review, assess, evaluate data protection regimes.
- Develop cases relevant to informing and testing areas of regulation.
- Encourage standardization of terminology.
- Obtain sectoral overviews.
- Support GPFI and G20 as fora by which to carry discussions forward.

# 2. INDUSTRY STANDARDS

## Insights

This focus session highlighted several global standards covering data protection and privacy issues, including standards developed by industry and development partners. These include, but are not limited to, the following [19]:

- Better Than Cash Alliance Responsible Digital Payments Guidelines
- EU General Data Protection Regulation (GDPR)
- EU Payment Systems Directive (PSD2)
- G20 High-Level Principles for Digital Financial inclusion
- Groupe Spéciale Mobile Association (GSMA) Code of Conduct for Mobile Money Providers
- OECD Guidelines on Protection of Privacy and Trans-Border Flows of Personal Data
- Smart Campaign Client Protection Principles
- The Windhover Principles for Digital Identity, Trust and Data

Various global standards could be used as a basis for working toward a common global language on data protection that will empower and support industry actors. Clear, universal data protection standards are important for credit bureaus, the development of credit scores, marketing, and product development, especially in a world of big data. They are also important for money transfer operators, given that remittances involve cross-border transactions between countries, which are likely to have a wider range of data protection laws (or perhaps none at all).

**The International Association of Money Transfer Network (IAMTN)** is developing common industry standards for Money Transfer Operators (MTOs) in consultation with members, financial institutions, development partners, and governments. This initiative will bring much needed transparency and integrity to the industry, as MTOs will be audited and certified based on their risk assessment.

Ultimately, the industry needs to recognize the significant variations in country contexts, as well as differences in the nature and size of financial institutions and affiliated partners. Further work also needs to be undertaken to identify the potential consumer benefits and harm resulting from the use of traditional and alternative forms of data. The aim should be to develop risk-based minimum data protection standards that can be applied in all contexts, and to all participants in the market. Such standards should also be adapted and relevant to both developed and developing country contexts. This includes a policy framework on dispute resolution and grievance systems for clients in relation to data protection issues, coupled with a major public awareness campaign.

Data protection authorities have an important role to play, but there needs to be consultation and collaboration with other regulators. Specifically, consumer protection agencies need to be brought into the conversation.

## KEY ACTIONS

- Given the interconnections in the financial services market, the industry needs to adopt one set of common, outcomes-focused standards covering data issues on a global level, that can also be tailored to country contexts. The best approach is to start with minimum standards, and then expand as necessary.
- The new standards should be flexible and applicable to all country contexts. Standards should reflect a careful assessment of actual consumer harm that require mitigation measures.
- A broad view of "industry" should be taken for this purpose. It should include traditional financial service providers, money transfer operators, mobile network operators, FinTechs, and so on.
- Data protection legislation should be the ultimate goal, but only after standards have been piloted and their impact assessed to inform policy work.
- Policymakers need to bring consumer protection authorities, the financial sector, telecommunications companies, and competition agencies into the discussion with data protection agencies.
- Consumer advocates need to help the industry to understand data-related needs and potential risks.
- Development partners and stakeholders can assist with developing client awareness and literacy about data issues. A major investment by all parties is needed for this purpose.

# 3. CONSUMER PERSPECTIVES AND ATTITUDES

## Insights

This focus session highlighted insights about consumer perspectives, attitudes, and concerns related to data privacy and protection. The session explored the role of consumers, consumer advocates, the industry, and regulators in addressing privacy and data security concerns so that consumers can benefit from data-related innovations while also being protected from potential risk and harm of which they may not be aware.

Research shows that customers care about their privacy and their data security. However, they often do not have, or cannot comprehend, all the information needed to make an informed decision. In addition, privacy preferences and concerns differ by culture and context. In this regard, discussions occurred regarding the appropriate approach and protections that may differ somewhat by country and government. Participants discussed whether customers understand the value of their data. They also noted the need to ensure that consumer data is used in ways that benefit the consumer, and not just the provider. Privacy concerns in particular sectors were also highlighted in the session. In **Tanzania,** the insurance supervisor worked to identify risks emerging from new digital insurance products and found that: (1) customers have little knowledge about their rights related to insurance products; (2) SMS messaging did not reveal the insurance underwriter, indicating poor transparency; (3) consumers were often unaware that they were subscribed to the insurance (which often comes bundled with other products); and (4) current approaches to informed consent make it difficult for consumers to understand the policies.

Research in **India** highlighted that many consumers avoid formal financial services because they do not trust the providers with their personal information. In the interest of keeping some of their finances private, consumers often engage in both informal and formal finance. Thus, they may be selective about engaging in informal or formal finance.

To increase the uptake and usage of DFS, especially data-enabled DFS, providers will need to earn and maintain customer trust, including by protecting customer data and privacy. It was recognized that many of the actions that are needed to protect consumers will have to come from regulators, providers, and industry associations. For example, ensuring end-to-end encryption, either by mandating it or through voluntary efforts by providers, was discussed as an action other actors can take to help protect consumers. With the challenges inherent in understanding big data and the associated risks and potential harm, consumers cannot be expected to take all actions needed to protect their data.

## KEY ACTIONS

- Conduct research on what matters to consumers.
- Clarify customer ownership, access, and control.
- Establish market conduct rules specific to data security.
- Clarify provider liability and establish a liability framework.
- Develop clear recourse mechanisms specific to digital finance.
- Develop and enforce cybersecurity guidelines.
- Assess the risk of exclusion caused by the use of alternative data.

# 4. STRATEGIC COLLABORATION WITH DEVELOPMENT PARTNERS AND INVESTORS

## Insights

In this session, development partners and investors delved into areas of potential strategic collaboration to further advance responsible digital finance, particularly in the context of consumer data protection and security. The International Finance Corporation (IFC) introduced its role in operationalizing the G20 High-Level Principles for Digital Financial Inclusion through its due diligence and new Investor Guidelines for responsible digital finance, drafted with a core group of impact investors and innovative digital finance operators. The Investor Guidelines aim to bring greater enforceability of global industry standards and principles through investments and strategic partnerships. Key participant insights and examples of concrete partnership actions were gathered from: CGAP; the Bill and Melinda Gates Foundation; the Smart Campaign at the Center for Financial Inclusion at Accion; the Software Group; and the United Nations World Food Programme (WFP).

Through its Financial Services for the Poor program, the **Bill and Melinda Gates Foundation**'s Level One Project developed a public-private sector model for a country-level digital payments infrastructure framework. The project aimed to reduce costs and increase efficiencies in providing digital financial inclusion products and services in Africa and Asia. Private technology partners are now a critical focus for fostering collaboration and devising an open system for inter-operability. The Gates Foundation is also partnering with the United States Agency for International Development (USAID) on an accelerator program to support the use of technology and data by regulators in developing regulations, such as in Mexico and the Philippines.

The **Software Group**[20] leverages technology solutions to partner with financial institutions through digital transformation processes. It conducts a full risk assessment to build or refine workflows, such as biometric user access to data. As an example, the Software Group defines spe-

cific data that agents should be able to access through an application interface. This requires the consent of the customer to confirm the extraction of that specific data. Their solutions are configurable to different markets. They are also in accordance with business strategy, relevant local consumer protection laws, data privacy, and security regulations.

The **Smart Campaign** shared its latest research about the risks that financial technology companies present to clients. It detailed how the Smart Campaign is pivoting to the FinTech industry in order to mitigate against these risks. For instance, the Campaign partnered with Jumo, a technology platform in Africa, to pilot and enable it to embed responsible digital finance in its operations. Jumo's credit risk and portfolio analytics capacity increased, with 97 percent of its customers perceiving their services as easier to use, and having products they trust.

The **United Nations World Food Programme** presented its humanitarian and social inclusion initiatives using technology, especially in fragile states. Their efforts are supporting forcibly displaced persons, refugees, and at-risk populations. They have implemented privacy by design to address consumer data protection; however, consumer risks stem from data registration issues (Know Your Customer - KYC) as well as from data that must be collected and shared from among multiple partner governments and non-governmental organizations (NGOs). Ensuring consumer ownership and empowerment, especially for at-risk groups, is a pressing concern.

**CGAP**[21] presented its perspectives based on evolving policy research and industry implementation experience from its digital finance and consumer protection initiatives. India Stack was presented as an example of digitizing the government's social safety net payments. Principles of privacy were re-emphasized as key. Yet, an open matter concerning privacy for the end-consumer remains. In addition, it is important to consider privacy as defined from different cultural and personal perspectives.

## KEY ACTIONS

**Partner with regulators and policymakers to balance risk and innovation for appropriate regulations and through the building of public-private partnerships:**

- Implement G20 HLPs at the country level to operationalize the principles.
- Support financial capability, education, and digital literacy.
- Promote regulatory technology and sandboxes to facilitate innovation.

**Partner with industry, providers, and investors:**

- Investor Guidelines: operationalize minimum requirements for the digital ecosystem; enforce existing global industry principles.
- Industry networks: Smart Campaign, BTCA Guidelines, GSMA, G20/GPFI.
- Collaborate with technology partners to localize solutions and ensure transparency.

**Partner with consumer advocacy groups and researchers to:**

- Better understand client risks for digital finance; customer empowerment.
- Research and maximize the value of data for financial inclusion; understand ways to minimize risks.
- Harness lessons from donor-funded programs across developed and developing countries regarding implementation of consumer protection and data privacy principles.


Forum
PROTECTING
CONSUMER DATA
AND PRIVACY
27–28 APRIL 2017
BERLIN, GERMANY
Federal Ministry
for Economic Cooperation
and Development
Responsible Finance
Forum

# VII. WHAT'S NEXT? FORGING A VISION


This session focused on collective action through insights that were developed across each of the Focus Sessions. Germany, as the holder of the G20 Presidency in 2017, emphasized that the RFF actions recommending the advancement of data protection in the context of digital financial inclusion will remain a priority for the G20 Global Partnership for Financial Inclusion (GPFI). Digitization opportunities and risks cut across all four GPFI Subgroups and reinforce the objectives of the G20 High-Level Principles on Digital Financial Inclusion. The urgency to advance data protection continued to resonate, as participants forged a vision for deeper public and private sector collaboration in moving forward.










AVOID
ALIGN
DATA COLLECT
INCENTIVES
CONSUMER IN


Privacy

# ENDNOTES AND REFERENCES

[1] The complete Forum agenda, speaker biographies, and participant details for RFF VIII are available on the RFF online platform at: https://responsiblefinanceforum.org/responsible-finance-forum-viii-2017/.

[2] More information about the World Bank's Universal Financial Access Goals (UFA 2020) can be found here: http://www.worldbank.org/en/topic/financialinclusion/brief/achieving-universal-financial-access-by-2020.

[3] United Nations Sustainable Development Goals (UN SDGs): Financial inclusion is not specifically one of the SDGs. However, it is deemed essential to the achievement of many of the other goals including: the reduction of global poverty and hunger; growth in employment opportunities and economic development; and fostering sustainable industry and innovation.

[4] More information about the GPFI Subgroups and Co-Chairs can be found here: https://www.gpfi.org/subgroups-and-co-chairs

[5] The G20 Global Partnership for Financial Inclusion's (GPFI) G20 High-Level Principles for Digital Financial Inclusion provides resources, information and background material for countries that seek to incorporate responsible digital financial inclusion measures into the creation or revision of their national financial strategy plans. The GPFI's Digital Financial Inclusion: Emerging Policy Approaches provides a synopsis of how countries are incorporating the GPFI G20 High-Level Principles for Digital Financial Inclusion into their national financial inclusion frameworks.

[6] How Digital Finance could Boost Growth in Emerging Economies. McKinsey Global Institute.

[7] MicroCred Group is an investment company that builds and manages an international network of financial institutions in emerging markets. These financial institutions share the common mission of providing quality financial services that are accessible and adapted to the needs of the unbanked and/or under-served people, particularly for MSMEs in Africa.

[8] Equifax is a consumer credit reporting agency serving clients and businesses internationally. Using the combined strength of unique trusted data, technology, and innovative analytics, Equifax has grown from a consumer credit company into a leading provider of insights and knowledge that help its customers make informed decisions.

[9] The Second Payment Services Directive (PSD2) is a fundamental piece of payments-related legislation in Europe that entered into force in January 2016. PSD2 is the product of a review of the original Payment Services Directive and requires payment service providers (PSPs) to make a significant number of changes to existing operations. PSD2 is an important evolution of existing regulation for the payments industry, aiming to increase competition in an already competitive payments industry.

[10] The European Union's General Data Protection Regulation (GDPR) replaces the Data Protection Directive 95/46/EC. It was designed to harmonize data privacy laws across Europe, to protect and empower all EU citizen data privacy, and to reshape the way in which organizations across the region approach data privacy.

[11] India Stack: New Financial Inclusion Infrastructure. CGAP.

[12] Kreditech Holding SSL GmbH is an online lender offering loans to individuals based on creditworthiness. The information is analyzed using their online data instead of using traditional credit rating information. The company focuses

its efforts on emerging markets in particular. Kreditech has developed a globally unique technology for scoring thin-file customers. The company's unique selling points (USPs) are the enablers for becoming the "Digital Bank for the Under-banked".

[13] Pain of Kenyans blacklisted for amounts as small as Sh100 in mobile loans, bank fees. Daily Nation, September 9, 2016.

[14] The Better Than Cash Alliance, Responsible Digital Payments Guidelines identifies eight good practices for engaging with clients who are sending or receiving digital payments, and who have previously been financially excluded or under-served.

[15] VEON has transformed itself from a telecommunications company to a global technology provider by offering a new engagement platform to its users. It re-engineered its legacy systems and data architecture to offer new, personalized, and contextual services. VEON's personal internet platform integrates powerful data analytics and artificial intelligence (AI) to finally put the user in control.

[16] Dr Ann Cavoukian Ph.D., former Canadian Privacy Commissioner, has advocated the use of 7 Privacy by Design Foundational Principles. These principles have been approved by numerous international privacy organizations such as IBM and Deloitte.

[17] Digital Financial Services and Risk Management Handbook: Regarding new risks and opportunities in the space of digital financial inclusion, a notable reference on digital finance and risk management is the Digital Financial Services and Risk Management Handbook, produced in partnership between the MasterCard Foundation and IFC. This Handbook provides benchmarks and guidelines outlining mechanisms to adopt varying forms of risk management and responsible finance measures in DFS and financial inclusion. A Handbook on Big Data Analytics is forthcoming this year. This Handbook will be based on lessons of experience from IFC's partner financial institutions in the Africa region. Stay up to date with the Handbook's release date through the IFC site.

[18] The OECD Guidelines on the Protection of Privacy and Trans-Border Flows of Personal Data (2013) were developed by OECD member countries to support the harmonization of national privacy legislation, as well as safeguard it from interruptions and interference.

[19]

- The GSMA Code of Conduct for Mobile Money Providers identifies principles aimed at promoting mobile money providers' adoption of consistent risk mitigation practices in certain critical areas of business. Principle 8 establishes: "Providers [should] follow good data privacy practices when collecting, processing, and/or transmitting customers' personal data."
- The Smart Campaign Client Protection Principles is an initiative of Accion's Center for Financial Inclusion. The Client Protection Principles are the minimum standards that clients should expect to receive when doing business or accessing financial services from a microfinance institution.
- The Windhover Principles for Digital Identity, Trust, and Data are a set of principles that address: (i) self-sovereign identity and control of personal data; (ii) transparent enforcement and effective governance;(iii3) ensuring trust and privacy; and (iv) open source collaboration.

[20] The Software Group is a global technology company that specializes in delivery channel and integration solutions for the financial sector.

[21] CGAP, The Consultative Group to Assist the Poor (CGAP), is a global partnership of 34 leading organizations that seek to advance financial inclusion.

# RESPONSIBLEFINANCEFORUM.ORG


Program Lead: Lory Camba Opem
Design & Layout: Jeff Frost
Photo Credits: Frederic Schweizer - www.foto-sicht.de
Printing: World Bank Group Printing & Media Services