Financial Systems Development

Responsible use of personal data and automated decision-making in financial services

Deutsche Gesellschaft
für Internationale
Zusammenarbeit (GIZ) GmbH

As a federally owned enterprise, GIZ supports the German Government in achieving its objectives in the field of international cooperation for sustainable development.

Published by:
Deutsche Gesellschaft für
Internationale Zusammenarbeit (GIZ) GmbH

Registered offices
Bonn and Eschborn

Friedrich-Ebert-Allee 36 + 40
53113 Bonn, Germany
T +49 228 4460-0
F +49 228 4460-1766

Dag-Hammarskjöld-Weg 1–5
65760 Eschborn, Germany
T +49 (0) 6196 79 - 4218
F +49 (0) 6196 79 - 804218

info@giz.de
www.giz.de

Programme/project description:
Sector Programme 'Financial Systems Development'

Author:
Michael Rothe, Alexander Dix and Tim Ohlenburg on behalf of GIZ/BMZ

Responsible:
Judith Frickenstein, Konstantin Pagonas, Sector Programme 'Financial Systems Development'

Design/layout, etc.:
Jeanette Geppert pixelundpunkt kommunikation, Frankfurt

Photo credits/sources:
Cover, p.6 © Wright Studio/shutterstock, © Businessvector/shutterstock

On behalf of
Federal Ministry for Economic Cooperation and Development (BMZ)
Division 114, Cooperation with the private sector; sustainable economic policy
Natascha Beinker
Stresemannstraße 94
10963 Berlin, Germany
Telphone +49 (0) 30 18 535 - 0
Fax +49 (0) 30 18 535 - 2501

poststelle@bmz.bund.de
www.bmz.de

GIZ is responsible for the content of this publication.

Printing and distribution:
Druckriegel GmbH, Germany

Printed on 100% recycled paper, certified to FSC standards.

Eschborn, August 2018

Table of Contents

LIST OF ABBREVIATIONS

AFI	Alliance for Financial Inclusion
AI	Artificial intelligence
ATM	Automated teller machine
BMZ	German Federal Ministry for Economic Cooperation and Development
DIFS	Data-intensive financial services
DFS	Digital financial services
DPRA	Data privacy risk assessment
EU	European Union
FinTech	Financial technology
FSP	Financial service provider
GDP	Gross domestic product
GDPR	European Union General Data Protection Regulation
GPFI	Global Partnership for Financial Inclusion
GSMA	Global System for Mobile Communications Association
ICO	United Kingdom Information Commissioner's Office
IDC	International Data Corporation
IT	Information technology
MFI	Microfinance institution
MNO	Mobile network operator
MoU	Memorandum of understanding
MSME	Micro, small and medium-sized enterprises
OECD	Organisation for Economic Co-operation and Development
REGTECH	Regulatory technology company
RIA	Regulatory impact assessment
UK	United Kingdom of Great Britain and Northern Ireland
URL	Unique resource locator

Acknowledgments

This document has been prepared by the GIZ Financial System Development Sector Programme on behalf of the German Federal Ministry for Economic Cooperation and Development (BMZ) to advance understanding of the usage of personal data and automated decision-making in the provision of financial services. It is based on the report Selected Regulatory Frameworks on Data Protection for Digital Financial Inclusion[1].

We would particularly like to thank the following people for their insights and helpful feedback: Tom Fisher, Privacy International; Jeremy Gray, Cenfri; Louis de Koker, La Trobe Law School; Juliet Maina, GSMA; David Medine, CGA; Zeituna Mustafa, Microsave; Claire Scharwatt, GSM; Mercy W. Wachira, Microsave

This work was led by Judith Frickenstein and -Konstantin Pagonas (Financial Sector Advisors, GIZ) and was authored by Michael Rothe (ConsultColors), Tim Ohlenburg (Consultant) and Alexander Dix (Deputy Chair of the Board of the European Academy for Freedom of Information and Data Protection).

1 https://www.eaid-berlin.de/wp-content/uploads/2017/12/Selected-Regulatory-Frameworks-on-Data-Protection-for-Digital-Financial-Inclusion-GIZ-09-2017.pdf

FOREWORD

The opportunities and risks presented by innovative digital finance solutions are two sides of the same coin, with digitisation holding enormous potential for advancing financial inclusion in innovative ways in developed and developing economies alike. Digital financial services (DFS) are deemed to be a huge game changer, especially in sub-Saharan Africa where the number of individuals making use of digital payments increased by 68.5 million from 2014 to 2017. With the 2030 Agenda acknowledging that financial services are an important driver of sustainable development, the digitisation of financial services are an enabling and powerful way to support the implementation of the Sustainable Development Goals. Digitisation presents an unprecedented opportunity to accelerate access to finance for the financially excluded and underserved.

Digitisation impacts on the financial sector and the business models it uses. Traditional providers of financial services like banks as well as new actors such as the mobile providers or FinTech companies that use technology to make financial services more efficient, are tapping into big data to design financial products and develop innovative ways of bringing their services to market. As a result, even greater volumes of data (big data) are generated on (potential) customers and used by these providers.

Regulatory frameworks on data privacy do advance, but they have not kept pace with the dynamic changes in the financial services industry. They are lagging behind in setting adequate customer protection standards governing the rapidly increasing use of artificial intelligence and big/alternative data. There is also a risk of social or financial exclusion if, for example, an algorithm were to calculate that people living in a specific location are less creditworthy than others.

In an early step, to balance the risks and opportunities of digital financial inclusion, the G20 leaders endorsed the G20 High-Level Principles for Digital Financial Inclusion in Hangzhou in 2016. These principles address, among other things, the balancing of innovation and risks (Principle 2), the provision of an enabling and proportionate legal and regulatory framework (Principle 3), the establishment of responsible financial practices to protect consumers (Principle 5) and the strengthening of digital and financial literacy and awareness (Principle 6).

Discussions at the 2017 G20 Global Partnership for Financial Inclusion (GPFI) Forum and at the GPFI-supported Eighth Responsible Finance Forum on Opportunities and Risks in Digital Financial Services: Protecting Consumer Data and Privacy in Berlin in 2017 focused on how to protect customers through enabling and proportionate legal and regulatory frameworks and responsible digital financial practices. At the 2017 G20 Summit in Hamburg, the leaders present encouraged G20 and non-G20 countries alike to continue promoting digital financial services and to do so in line with the G20 High-Level Principles for Digital Financial Inclusion. In addition, the G20 leaders asserted their support for efforts to develop enabling and responsible legal and regulatory environments for financial services that foster financial inclusion and encourage countries to share their experiences in regulating FinTech.

This paper builds on GIZ's 2016 discussion paper *Data protection in the context of digital financial services and Big Data* and on its 2017 report on *Selected Regulatory Frameworks on Data Protection for Digital Financial Inclusion*. It seeks to provide financial sector policy-makers and regulators with orientation in their work to develop appropriate regulatory frameworks for data-intensive financial services (DIFS) – frameworks that, in the interests of financial inclusion, should ensure to safeguard people's privacy as well as to promote innovation.

Section 1 defines the purpose and scope of this paper, outlining the salient features of financial service provision in the digital age. In particular, it describes the ever-increasing role of personal data, discussing the benefits and risks arising from their use, and it highlights the implications of consumer data use for financial sector policy.

Section 2 sets out six recommendations on data protection in DIFS, which are intended to inform discussions around data protection and DIFS and to support the drafting and implementation of the respective regulations. Under each recommendation, a number of sub-recommendations are put forward, detailing specific actions that can be taken to achieve the overarching recommendation.

I hope that this paper serves its purpose to support the shaping of frameworks that promote responsible (digital) financial inclusion!

Natascha Beinker
German Co-Chair G20 Global Partnership for Financial Inclusion
German Federal Ministry for Economic Cooperation and Development (BMZ)

1 | INTRODUCTION

1.1. Background

The financial sector is undergoing fundamental changes, which are being driven by advances in technology and the proliferation of mobile and digital devices. These changes have significant implications for financial sector policy and regulation, including financial inclusion. Two key waves of innovation have impacted on the financial landscape:

The first wave: delivery channels for financial services

Ubiquitous mobile technology and innovative business models such as 'mobile money' and 'agent banking' can reduce the cost of financial service delivery by up to by 90% (McKinsey Global Institute, 2016). These innovations, initially referred to as 'branchless banking' and more recently as 'digital finance', have made it economically viable to service customer segments that, through traditional means, could not be served profitably.

Consequently, digital finance has become central to financial inclusion in developing and emerging markets, a fact reflected in the financial inclusion commitments made by developing- and emerging-country governments: 70% of all Maya Declarations include commitments on digital finance.[2] These commitments have largely already been realised – for example, according to the GSMA, 52 markets now have enabling regulatory environments for mobile money (GSMA, 2018).

Digital finance is provided by 'traditional' financial institutions such as banks and microfinance institutions (MFIs), by mobile network operators (MNOs) from the telecommunications sector (often providing financial services through subsidiaries), and by third-party technology providers set up specifically for digital finance. All these digital finance providers are typically regulated by the authorities tasked with governing the financial sector.[3]

2 The Maya Declaration is the first global commitment by policy-makers from developing and emerging countries to unlock the economic and social potential of the poor through greater financial inclusion. For more information, see https://www.afi-global.org/maya-declaration

3 Commonly-regulated activities/sub-sectors differ between jurisdictions and include electronic money, mobile money, mobile payments, agent banking and branchless banking.

The second wave: data-intensive financial services (DIFS)

This second wave is being driven by the increasing amount of available data and the ongoing advances in the new technologies that make sense of this data. Digitisation generates unprecedented amounts of information on people and businesses: digital payments, text messages, social media messages, cloud-based services, etc. all leave data trails that can provide important insights into people and businesses. According to the International Data Corporation (IDC), 'the world's stock of digital data will double every two years through the year 2020' and 'by 2020, 60 percent of this digital data will come from developing economies' (Owens and Wilhelm, 2017).

At the same time, data storage and processing capabilities are rapidly becoming cheaper and more powerful, and data-related technology such as machine learning and artificial intelligence (AI) is now central to global scientific research and investment trends. The combination of these factors opens up vast opportunities for innovation in financial services. 'End-to-end' systems that use data to autonomously make decisions are spreading across industries. For example, loans can now be appraised and disbursed without any human intervention, within seconds and at extremely low cost. Data is the common denominator of what is referred to as FinTech (i.e. financial technology), a term used to describe the wide variety of technology-based start-ups in the financial services sector.[4]

The use of personal data in itself is nothing new in financial services. For decades, financial institutions across the globe have used electronic core banking systems and the personal data they store. What is new, however, is the intensiveness of data use and data's rapidly increasing prominence in new services and business models. New models such as digital credit are based entirely on the use of personal data and would not exist without them.[5] This paper will use the term 'data-intensive financial services' (and its abbreviation 'DIFS') to refer to all financial services that intensively use personal data.

4 https://www.investopedia.com/terms/f/FinTech.asp

5 For more information on digital credit, read 'The Proliferation of Digital Credit Deployments', available at http://www.cgap.org/web-publication/proliferation-digital-credit-deployments

The table below summarises the characteristics of the two waves of innovation:

	FIRST WAVE: DELIVERY CHANNELS	SECOND WAVE: DATA
DRIVERS	Proliferation of digital technology and mobile phones, and increasingly enabling regulations	Increases in the availability of data, advances in data analytics, machine learning, AI
IMPLICATIONS	The economics of service delivery is enhanced, which means vast numbers of people can now be served profitably	The capacity to tailor products, quantify risks and automate processes is enhanced, which makes operations to assess credit-seeking customers low cost
KEY INSTITUTIONS	Banks, MNOs, MFIs, some FinTechs	FinTech firms, data analytics firms, companies from any sector that gather personal data (e.g. social media)
POLICY AND REGULATION	Core part of financial inclusion policy, now generally regulated	Policy discussion in early stages, sparse regulation, regulatory uncertainty

In developing and emerging markets, second wave innovations such as digital credit often ride on the back of the first wave. For example, a digital finance provider that already has contractual relationships with customers for basic digital payment services (e.g. mobile money) may team up with a FinTech or data analytics company and with a capital provider to offer a digital credit service. The emergence of new players and ways of doing business has both potential upsides and potential downsides.

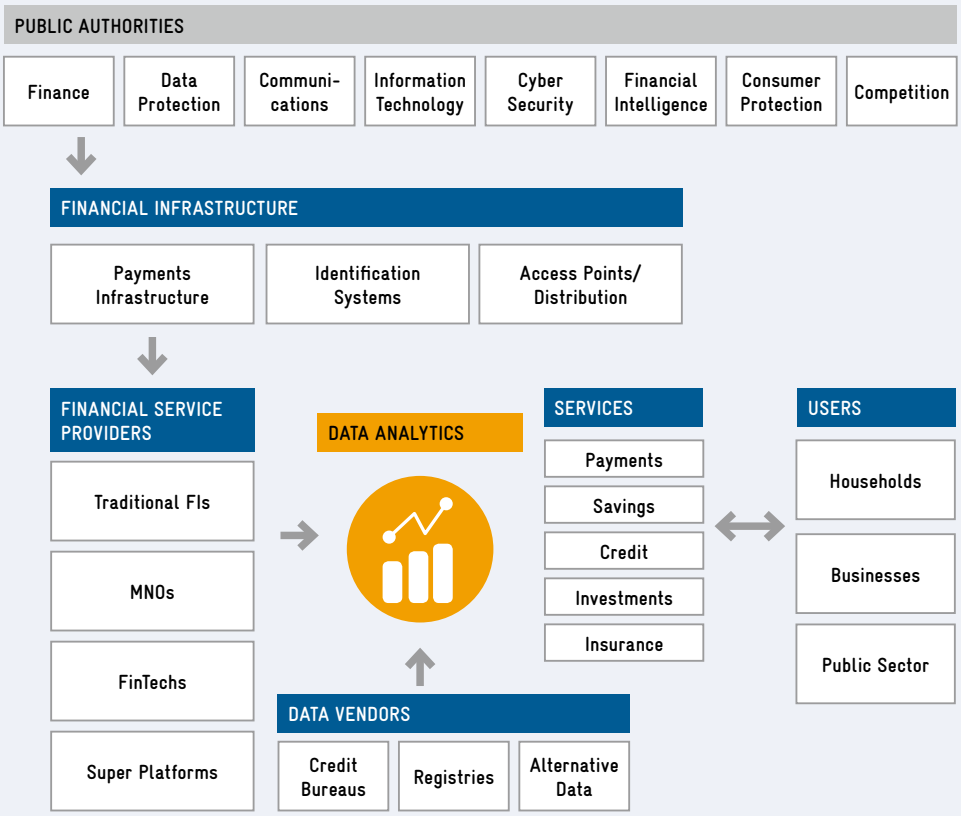
DIFS ecosystem

One key characteristic of the digital age is that the lines between sectors are blurring. DIFS are a direct result of the growing convergence of the financial, telecommunications and technology sectors. DIFS are delivered through complex value chains and within ecosystems comprising large numbers of stakeholders. Data are gathered, stored and processed at different points and by different stakeholders.

Figure 1 below illustrates a stylised DIFS ecosystem. All stakeholder groups marked in blue may store, process or have viewing rights to personal information.

FIGURE 1: A DIFS ECOSYSTEM

SOURCE: SOURCE: AUTHORS' OWN WORK



Public authorities

Policy-makers, regulators and supervisors for the sectors of finance, data protection, communications, information technology, cyber security, financial intelligence, consumer protection, and competition (antitrust) all may play a role in protecting privacy in DIFS.

Financial infrastructure

Financial infrastructure includes payment infrastructure (e.g. switches), identification systems, and access points (e.g. agents and ATMs). For example, retail payment switches process at a central level the transactions made by individuals and small businesses and in so doing capture data on spending patterns.[6] Identification systems, such as the Aadhar[7] system in India, capture sensitive personal data including biometrics.

Financial service providers

It is financial service providers (FSP) that most commonly have the contractual relationship with the customer. In the context of running even a basic service, FSPs capture important personal data on their customers including identification information (proof of identity, address, phone number, etc.) and account transaction data. FSPs also have access to personal data kept by third parties, such as credit reference bureaux, and often report specified sets of data to third parties, such as the aforementioned bureaux. Different types of FSPs use intensive data-driven approaches. These currently include 'traditional' financial service providers such as banks and microfinance institutions (MFIs), mobile network operators (MNOs) and FinTechs. In some countries – most notably China – FSPs also operate online 'super platforms',[8] market places that leverage existing customer relationships and data to provide financial services.

6 One example of this kind of centrally processed system is Jordan's JoMoPay mobile payments platform.

7 To find out more about Aadhar, visit http://indiastack.org/about/

8 For a discussion of the potential role of super platforms in financial inclusion, see the Financial Inclusion on Business Runways (FIBR) Project's 2017 white paper on Inclusive digital ecosystems of the future, available via http://www.fibrproject.org/news-events-list/2017/12/8/fibr-project-white-paper-no2-inclusive-digital-ecosystems-of-the-future

Data vendors

'Data vendor' is the industry term for an organisation that specialises in or generates revenue from the provision of data, such as credit reference bureaux, collateral registries, asset registries and vendors of alternative data sources. The data they own may have been gathered in the context of financial activities as well as non-financial activities. While DIFS naturally use traditional credit reference data (i.e. data on the repayments [or defaults] of past loans), they also use 'alternative data', which include the following:

» Digital payment transaction data: mobile money payments, card payments.

» Deposit/current account information: recurring payroll deposits and payments, average balance, etc.

» Traditional credit-reference data: loan repayment records.

» Telecommunications data: phone records, text messages, airtime top-ups, data volume top-ups.

» E-commerce transactions: online purchases and sales, bookings (in the case of hospitality sector transactions), loyalty programmes.

» Cloud services: accounting services, inventory management, business intelligence, training.

» Social media data: personal networks (contacts), activities on social media (e.g. posts).

» Utilities: gas, water, electricity.

» Property/asset records, including the value of owned assets.

» Rent: past payments.

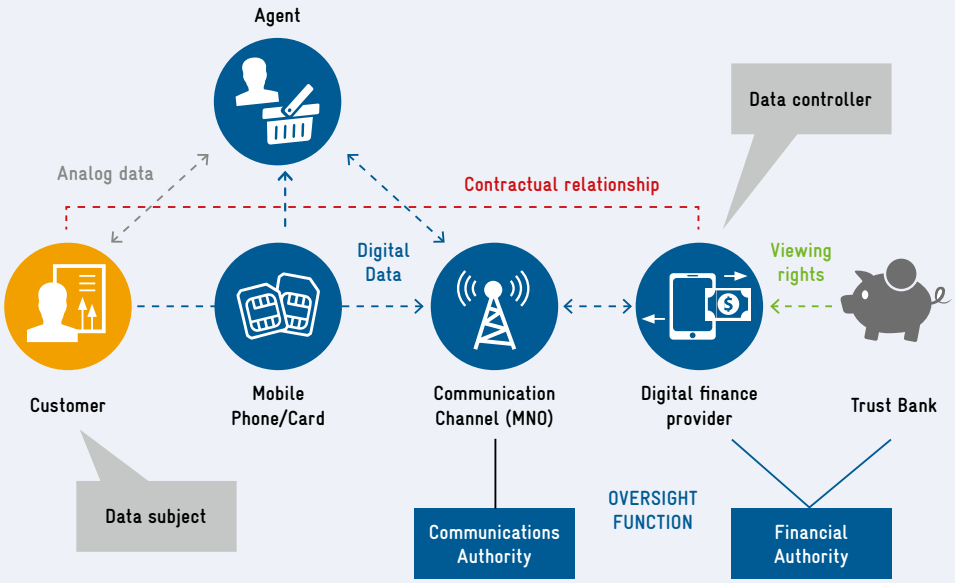
» Public records: beyond the limited public records information already found in standard credit reports.

Data analytics

Data analytics involves combining insights from raw information sources with human knowledge. Many data-analytics techniques and processes have been automated using mechanical processes and algorithms that prepare raw data for human consumption. Data analytics techniques can reveal trends and metrics that would otherwise be lost in a morass of information. These trends and metrics can then be used to optimise processes and increase the overall efficiency of a business or system, while simultaneously adding value to customers by providing tailor-made products based on the data held on them. Data analytics is central to DIFS and is conducted either by the financial service provider itself or by an external specialist service provider (e.g. a data analytics firm, a FinTech company, or a consumer reporting agency).

Figure 2 below illustrates data flows in an exemplary digital finance set-up:

FIGURE 2: EXEMPLARY DATA FLOWS IN DIGITAL FINANCE — SOURCE: AUTHORS' OWN WORK



» Customers have a contractual relationship with the digital finance provider. They make transactions remotely using a digital device (mobile phone, card) or through an agent (mainly the case for paying in or withdrawing cash).

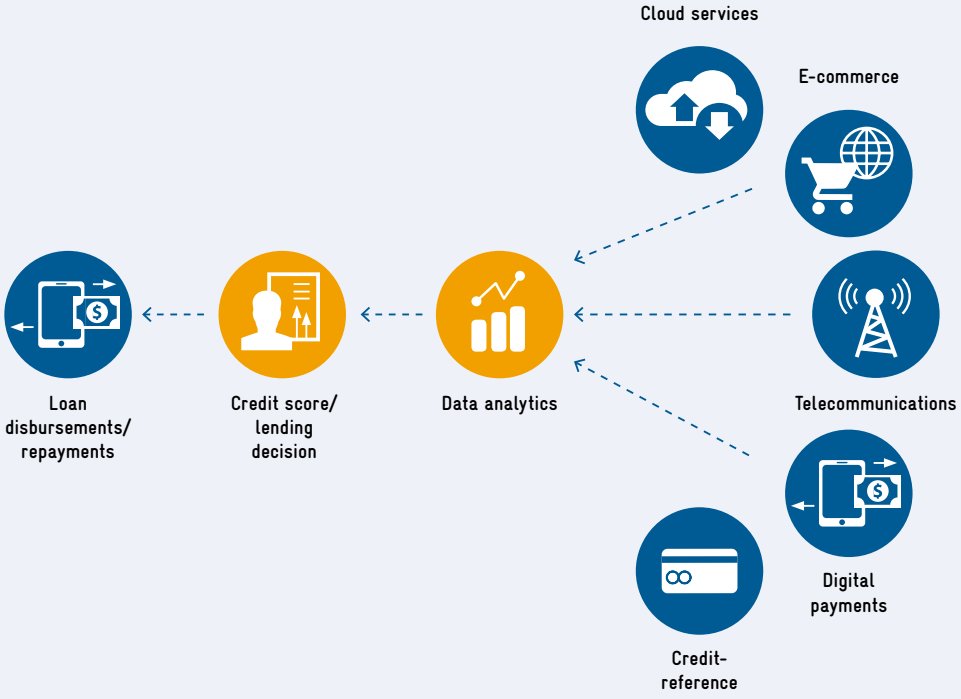
» The digital device (phone or point-of-sale terminal) communicates via the mobile network with the core technology system of the digital finance provider.

» The digital finance provider is regulated by the competent financial authority.

» If the digital finance provider is a non-bank (i.e. not a fully licensed) financial institution, the regulations commonly require this provider to collateralise in a fully licensed bank (the 'trust bank') the funds it issues to customers in the form of electronic money. In such cases, the trust bank will have viewing rights.

Figure 3 below shows the potential data sources and typical data flow of a digital credit model.

FIGURE 3: DATA FLOWS IN DIGITAL CREDIT — SOURCE: AUTHORS' OWN WORK



1.2. Benefits and risks associated with using consumer data

It is a golden era for innovation in financial services for the unbanked, as the economics of new technologies allows established firms and new entrants to expand coverage, better assess risk, and create new services. The rapid evolution of financial services presents great opportunities and **benefits**, but regulators must also consider and mitigate the associated **risks**.

BENEFITS

INCREASED ACCESS TO BETTER FINANCIAL SERVICES	The potent combined forces of the unfolding consumer, data and digital revolutions are changing the landscape of inclusion and the reach of financial services, offering the promise that billions of individuals and businesses will be able to access affordable financial services for the first time (Costa et al., 2015). In particular, with lenders able to use personal data to better assess risk, the individuals and businesses that have historically been locked out due to a lack of formal credit history, bookkeeping or collateral will find it much easier to access these services. McKinsey estimates that this could unlock USD 2.1 trillion in credit for MSMEs and individuals in developing and emerging economies (McKinsey Global Institute, 2016). While most of the innovation involving the intensive use of personal data has been witnessed in the areas of credit, financial planning and insurance, other types of financial services, including savings and investment, are set to follow.
HIGHER-QUALITY, MORE-TARGETED PRODUCTS	High-quality financial products and services are those that meet customer needs, which are as diverse as individuals' and MSMEs' economic activities, financial behaviours and income patterns. Personal data presents a significant opportunity to tailor products and services to the specific needs of customer segments or even to individual customers. For example, a data-intensive lender may analyse the digital payments records of a small shopkeeper to determine tailored loan sizes.
INCREASED OVERALL EFFICIENCY, AFFORDABLE PRODUCTS AND SERVICES	Automated decision-making that leverages data provides opportunities for significant cost savings. For example, using advanced analytics and non-traditional, large data sets to assess credit worthiness can offer a substantial cost advantage when it comes to providing credit in emerging markets (Costa et al., 2015). In a competitive environment, these savings can benefit consumers in the form of lower prices or wider access.
BUSINESS GROWTH, EMPLOYMENT AND ECONOMIC DEVELOPMENT	All of the above-mentioned benefits lead to business growth, which in turn leads to employment opportunities and economic development. For example, better access to finance will lead to job creation within the MSME sector. Lower operational costs will enable FSPs to serve more customers. McKinsey estimates that that widespread use of digital finance could boost the total annual GDP of the group of emerging economies by USD 3.7 trillion by 2025, a 6% increase on the business-as-usual scenario (McKinsey Global Institute, 2016).

RISKS

LOSS OF PRIVACY	Non-transparent collection and processing of personal data diminishes the ability of the customer (commonly referred to as 'data subject' in modern data protection regulations such as the GDPR) to decide upon the use and flow of his or her data. Consequently, he or she may find it difficult to challenge any decisions taken by the digital financial service provider, such as denial of credit on the basis of false data used for scoring. Furthermore, the use of alternative data such as social networks leads to the capture of far-reaching personal profiles on the behaviour, preferences and movements of the data subject. The use of such profiles for purposes unrelated to credit provision and to the detriment of the customer is difficult to monitor and prevent. Excessive collection of personal data without the necessary regard to privacy considerations will lead to a loss of trust and therefore may eventually lead to the economic failure of some digital financial services.
UNFAIR DISCRIMINATION (INCLUDING PRICE)	The use of personal data to inform decision-making in financial services presents the risk of discrimination. For example, there have been reports that people are being denied credit due to their sexual identity or political views (Privacy International, 2017). The use of sensitive personal data such as race, ethnic or tribal origin, sex, religion or political opinion is (subject to strict exceptions) illegal not only under EU data protection law (GDPR), but also under international conventions dealing with race discrimination even if the data only concern groups of people rather than individuals. These legal limitations are relevant in the financial inclusion context because such practices (e.g. excluding or preferring certain individuals or groups seeking financial services or providing discriminatory interest rates) would run counter to financial inclusion.[13] However, discriminating between customers on the basis of facts that help determine their risk profiles (e.g. their credit scores) is not an illegal or unethical form of 'discrimination' as long as it does not factor in characteristics that have been deemed unethical/illegal by lawmakers (e.g. tribal origin, race, religion, gender, sexual orientation).
FRAUD (IDENTITY THEFT)	The more that personal data is collected and stored outside the control of the customer/data subject, the greater the risk is that this data will be used by unauthorised persons (inside or outside the DIFS provider or MNO) for identity theft or other criminal purposes. This is especially true if IT security is insufficient.
UNLAWFUL ACTIVITIES EXECUTED BY MACHINES	Automated decision-making and machine learning exacerbates risks to privacy and equal treatment and can diminish transparency, in particular in cases where decisions on access to financial resources are taken exclusively by machines without any realistic intervention and control by humans.

1.3. Implications for financial sector policy

How do the potential benefits and risks relate to policy objectives?

Financial sector authorities traditionally pursue the core policy objectives of financial stability, financial integrity and consumer protection. More recently, financial inclusion was added to the global policy agenda, with 115 financial regulatory and policy-making institutions from 94 developing and emerging countries (representing 85% of the world's unbanked population) joining the Alliance for Financial Inclusion (AFI, 2017), a global advocacy network for financial inclusion policy and regulation. The use of personal data in digital finance has specific implications for these different policy objectives, as illustrated in the table below:

POLICY OBJECTIVE	IMPLICATIONS OF THE USE OF CONSUMER DATA
FINANCIAL INCLUSION	The responsible use of consumer data has great potential to advance financial inclusion. Promoting it would therefore contribute to this policy objective.
MARKET CONDUCT/CONSUMER PROTECTION	The use of consumer data entails various consumer risks (see 1.1.2), which must be addressed if this specific policy objective is to be delivered.
FINANCIAL INTEGRITY	Consumer risks associated with the use of data include fraud, which must be minimised to maintain financial integrity. On the other hand, the use of data can increase integrity through better fraud and risk control. For example, the use of consumer data can lead to improved know-your-customer checks, thus preventing fraud and improving financial integrity.
FINANCIAL STABILITY	Studies on the systemic importance of digital finance and FinTech institutions have largely suggested that these do not pose a risk to financial stability due to their moderate (though growing) size and prudential policies.

In light of the vast potential of using personal data for financial inclusion, it is worth taking a closer look at its specific implications for the key drivers of financial inclusion. In a 2016 white paper (GPFI, 2016), the G20 Global Partnership for Financial Inclusion defined financial inclusion as follows:

> Financial inclusion means that all working-age adults (persons at the age of 15+) have effective and quality access to and usage of – at a cost affordable to the customers and sustainable for the providers – financial services provided by formal institutions. "Effective access" involves convenient and responsible delivery of services that are responsive to the needs of financially excluded and underserved customers, at a cost affordable to the customers and sustainable for the providers. The demonstration of effective access is usage. The fact that a customer can access services offered by a formal financial service provider does not mean she or he is "financially included." For this, the conditions of "effective access" must be met.

As stated above, the use of consumer data presents opportunities for enhancing access, quality and sustainability, but also entails risks. Financial sector policy in general and financial inclusion policy in particular must therefore meet the dual objectives of promoting and enabling the responsible use of data and associated innovations (automated decision-making, AI, etc.), while mitigating the consumer risks associated with these innovations. Effective privacy protection is therefore an essential part of financial inclusion in the age of DIFS.

Striking the balance between regulatory openness and security is nothing new for financial inclusion policy-makers. Financial services commonly present opportunities and risks at the same time. For example, access to (micro-)credit provides individuals and MSMEs with the opportunity to enhance their economic situation through higher profits, while also presenting the risk of worsening it through over-indebtedness, etc. Most financial inclusion commitments explicitly acknowledge this dichotomy: 70% of all Maya Declarations include specific commitments on 'consumer empowerment and market conduct' (AFI, 2017).

Which data fall within the remit of the financial sector authorities?

As described above, DIFS use data that originate both in the financial sector and in other sectors. It is clear that, in the absence of a general data protection authority, the financial sector authority's remit would cover activities related to data collected in the context of financial services use.

Furthermore, given the central function that data originating in other sectors can have in DIFS business models and value creation, the use of these data also falls within the remit of the financial sector authority. As such, the use of data gathered by providers outside of the purview of financial sector regulators (e.g. call records collected by MNOs) must also be regulated by these authorities. What this means in practice is that providers using data for financial services must comply with all relevant requirements, including in situations where they obtain data from other providers such as data vendors.

1.4. Purpose and scope

The intensive use of data presents unprecedented opportunities as well as risks, including for financial inclusion. Policy-makers and regulators across the globe must enhance regulatory frameworks to account for this new reality. Important work at the global, regional and national levels has already been done, and the report *Selected Regulatory Frameworks on Data Protection for Digital Financial Inclusion* (Dix, 2017) summarises selected existing initiatives and regulatory frameworks that address this theme.

Building on this earlier report, the recommendations set out below aim to provide concrete guidance to support policy-makers and regulators in establishing enabling regulatory frameworks for the responsible use of personal data and automated decision-making in financial services. Regulatory frameworks for DIFS should seek to enable innovation while safeguarding consumer inclusion.

Blockchain and other distributed ledger technologies may give rise to innovations in the protection of personal data and privacy in the digital space, with new applications that go beyond crypto-currencies. However, a discussion of these technologies and their potential applications is beyond the scope of this paper.

Furthermore, it should be kept in mind that many state and non-state actors may have access to personal data – from the data gathered by state intelligence agencies from telecommunications providers or the information held by humanitarian agencies on their beneficiaries, to the data collected by financial intelligence units. This paper, however, focuses on those issues that currently are most relevant to and can be addressed by financial sector authorities and other authorities working on policy and regulation that affect the use of data in financial services.

2 | THE RECOMMENDATIONS

1. Demonstrate leadership in data protection
2. Collaborate to uphold privacy in the digital age
3. Enhance data awareness
4. Empower customers to be the sovereigns of their data
5. Hold providers accountable
6. Enforce secure data storage

This paper outlines six recommendations to address data protection in data-intensive financial services (DIFS). The recommendations are targeted at financial sector policy-makers, regulators, and other authorities working on policy and regulations that affect the use of data in financial services. They are intended to inform discussions around data protection and DIFS and to support the drafting and implementation of respective regulations.

In light of the complexity of evolving business models and the variety of stakeholders involved, a well-designed policy process is paramount. Therefore, recommendations 1, 2 and 3 provide guidance on process-related issues, while recommendations 4, 5 and 6 go on to provide orientation on the potential content of regulatory frameworks for DIFS. Given that the extensive use of data and new tools such as automated decision-making are still new phenomena across the globe, some of these principles remain untested. The recommendations are therefore drafted in a way that provides orientation for discussions on developing a solution for a given jurisdiction, rather than suggesting a solution.

Each recommendation comes with a number of suggested sub-recommendations for specific actions that can be taken to achieve the overarching recommendation. For each sub-recommendation we outline why addressing the issue at hand is important and how it can be implemented. Where relevant, we also describe the specific recommendation's relationship to and implications for financial inclusion.

As approaches to addressing data protection must be tailored to the specific context of any jurisdiction, all the recommendations presented herein should be understood as suggestions and orientation on how to address these new regulatory issues, and not as 'best practice'.

2.1. Demonstrate leadership in data protection

2.1.1. Clearly define the role of the financial sector authority

It is likely that data protection in DIFS will involve more than one regulator and, as stated in section 1, financial sector authorities have a clear role to play. The nature of this role will depend on the existence and mandate of other authorities, in particular on whether there is a general data protection authority and/or whether general data protection regulations have been instituted.

In jurisdictions where no general data protection authority exists, the mandate for overseeing the use of personal data in financial services will clearly fall to the financial sector authorities. Even in jurisdictions that have a general data protection authority and regulations, there will still likely be a role for financial sector authorities. This is because financial sector regulators have clear assets regarding the regulation of data protection in this space, including direct and established licensing relationships with financial institutions, deep understanding of financial sector issues and direct access to financial service providers' data.

To ensure effective implementation of any policy/regulation, the role of the financial authority and its partner institutions should be clearly defined. This will include developing internal consensus regarding the role of the financial authority. The respective roles of different authorities, and potentially the 'division of labour' between the authorities, should be defined in dialogue (e.g. through a working group or taskforce). A memorandum of understanding (MoU) could be adopted to formally define key roles and responsibilities as well as modes of cooperation. Legislation can also resolve the roles of different regulators.

Given that financial inclusion is an explicit policy objective of most financial authorities, it is important that financial authorities assume a key role in the discussion around regulating DIFS. This will ensure that any policy or intervention reflects the nuances relating to financial inclusion.

2.1.2. Demonstrate leadership on data protection

Achieving effective data protection in DIFS will likely require public intervention, which in turn requires actions by a variety of public bodies. Strong leadership is therefore required to initiate and champion a discussion around data protection for the jurisdiction in question. Policy-makers and relevant authorities can start by outlining high-level data protection principles.[9]

The country context will determine which institution takes on the leadership role in data protection for DIFS. In countries that have a data protection authority, the role will fall to the champion for data protection across sectors, including the financial sector. In countries without a data protection authority and with a limited or no effective data protection regime, leadership will mean championing the discussion and subsequent initiatives to enhance data protection in the respective sectors. For the financial sector, it is the financial sector authority that must take on this work.

Due to the dynamism of the sector, data protection in DIFS will require agile public authorities and continuously evolving regulation. Leadership will therefore also mean initiating a discussion around assessing the effectiveness of existing regulatory frameworks for data protection in the specific field of DIFS.

It is important for this leadership to be conscious of the potential impact of data protection on financial inclusion. From an institutional perspective, this may mean that financial sector policy-makers as well as representatives of private financial institutions and consumer groups or civil society should represent the 'voice of financial inclusion'.

9 See the annex for more on the data protection principles.

Finally, authorities have to be aware of the broader social implications of the use of personal data. All credit scores change behaviour; however, as scoring extends beyond the traditional financial sector (into social media, etc.), it runs the risk of changing behaviour more broadly. Regulators must be mindful of this risk and explore the implications of the development of DIFS and the FinTech sector beyond its impact in the financial sphere.

2.1.3. Rule-makers should regulate to ensure that DIFS are developed and delivered in a responsible and sustainable manner

Safeguarding privacy and minimising other consumer risks in DIFS will likely require regulatory intervention. However, regulation is not an end in itself. Rule-makers must ensure that regulation is as effective as possible and weigh the expected benefits of regulation against the likely costs. Regulation will be deemed effective if its total benefits – for all members of society – are greater than its total (financial and social) costs (OECD, 2008). In the context of financial inclusion, regulatory intervention to protect consumers' personal data may mitigate consumer risks while compromising data-driven opportunities to advance financial inclusion. That said, clear rules on data may also create a level playing field and thereby foster competition and innovation. Data protection rules and their enforcement will also increase consumer trust in the DIFS services offered. 'Smart policies' may also help to level the playing field and reduce the costs of compliance. For example, over the long term, the financial costs will be lower if the policy-makers and regulators adopt the principle of 'privacy by design and by default'.[10]

To determine whether regulatory intervention is justified, policy-makers can conduct regulatory impact analysis (RIA), which is defined as follows:

> RIA is a process of systematically identifying and assessing the expected effects of regulatory proposals, using a consistent analytical method, such as benefit/cost analysis. It is based on determining the underlying regulatory objectives sought and identifying all the policy interventions that are capable of achieving them. These 'feasible alternatives' must all be assessed, using the same method, to inform decision-makers about the effectiveness and efficiency of different options and enable the most effective and efficient options to be systematically chosen (OECD, 2008).

10 This principle is related to the principle of data minimisation (see the annex on Data Protection Principles) and stresses taking a pro-active approach when designing products, services and business models. It makes sense from a business perspective to take on board the recommendations and existing regulations on privacy at an early stage rather than bolt them on to existing products afterwards at higher costs.

Financial sector authorities can address DIFS regulation through three different approaches:

SPECIFIC REGULATION FOR DATA PROTECTION IN (DIGITAL) FINANCIAL SERVICES/FINTECH ('SECTORAL REGULATION')	This would be a specific regulation intended to address all personal-data-related practices across the financial services sector and would form part of the licensing requirements for financial service providers.
INTEGRATION OF DATA PROTECTION PROVISIONS IN OTHER REGULATIONS	This would involve including data protection provisions in the regulations governing related financial sector activities. Regulators can use digital finance regulation to address data in areas such as electronic money, mobile money, mobile financial services, agent banking, and branchless banking. For instance, in many countries, regulations governing electronic money or mobile money include provisions on the use of personal data, albeit limited ones.
INPUT INTO THE GENERAL DATA PROTECTION FRAMEWORK	Where a general data protection framework (cross-sectoral) is being developed, financial sector authorities can provide advice to ensure financial sector issues are covered.

Assessing the costs vs the benefits of regulating the use of data in digital financial service provision is a complex task. The wrong regulatory intervention may have negative consequences for financial inclusion, including stifling innovation, introducing barriers to entry and creating regulatory arbitrage. In many developing and emerging markets, the increased access to alternative data constitutes a fundamental shift from previously limited data availability. Also, the implementation of data protection principles in the FinTech space remains untested, even in more mature markets. At the same time, the DIFS and the emerging FinTech companies should clearly follow the same basic legal and ethical requirements with regard to privacy and non-discrimination that have been adopted in other areas of economic activity.

2.1.4. Supervisory bodies should build the internal capacity required to effectively foster compliance

Any regulation is only worthwhile if it is effectively implemented and monitored. Effective implementation requires capacity at the level of the 'controllers'[11] and the supervisory authority, and it requires specific skill sets. For example, supervisors will need to understand business models and data flows. Controllers and the responsible authority should therefore hire staff with the relevant skills in, for example, IT, data analytics, digital finance/FinTech, data protection, anonymisation, encryption, etc. Existing staff should receive on-the-job training and work on gaining qualifications in the fields of privacy, non-discrimination and consumer protection.

11 Here, 'controller' means the natural or legal person, public authority, agency or other body that determines the purposes and means of the processing of personal data (see Article 4[7] of the GDPR).

Regulators should engage in awareness raising, skills development and capacity building for providers/controllers and customers. In addition, regulators should encourage and support self-regulation, whether in the form of codes of conduct or otherwise (OECD, 2013). Finally, they should promote technical measures and tools that help to protect privacy.

Financial regulators and, where established, data protection supervisory authorities may make a stronger uptake of DIFS more likely if they promote privacy-friendly services and products. This will contribute to more widespread forms of financial inclusion and to enhancing consumers' trust in digital financial products.

2.1.5. Public authorities should lead by example by practising high levels of data protection

Like private financial service providers, public authorities collect personal data, and these data require at least the same level of protection as they receive in the private sector. A data breach in public sector authorities will not only compromise the data of affected consumers as citizens, but also diminish trust in the data protection regime in general. In addition, by complying with data protection, authorities gain practical direct experience and in so doing enhance their own internal capacity in this area.

In countries that already have data protection laws in place, it is generally the case that the public authorities charged with monitoring compliance with these rules are themselves subject to strict rules regarding the handling of citizens' data. Financial or other specific regulators (e.g. in the telecoms sector) will be subject to oversight by the data protection authority, where such exists. Law enforcement agencies should only be permitted to access data stored by providers or regulatory authorities in so far as it is provided for in national law (e.g. for crime prevention or prosecution). In any case, all existing public authorities should be subject to judicial review if they process personal data unlawfully or are responsible for data breaches.

The success of financial inclusion will largely depend on the relevant public authorities taking an active role, in so doing leading by example and promoting the adoption of privacy-friendly business models and processing practices (OECD, 2013).

2.2. Collaborate to uphold privacy in the digital age

2.2.1. Public authorities should work together to protect personal data

Given that DIFS span various sectors – in particular the financial, telecommunications and technology sectors – consumer risks, including risks to privacy, can only be addressed if all the relevant authorities collaborate effectively. For example, FSPs may use personal data that were originally gathered in other sectors, such as call records and social media activity, to determine credit scores. In addition, the level of protection applied to consumer data should be the same regardless of where they are processed (be it in the jurisdiction where the consumers reside, in the cloud or in another country). As mentioned in 2.1.1, financial regulators may also play a role in enforcing overarching data protection regulations.

Collaboration is therefore required between all authorities – at both the national and international levels – that have a mandate to address consumer data risks and uphold privacy. These include but are not limited to financial, consumer, antitrust, regulatory, cybersecurity, data-protection and human-rights bodies or their equivalents. This collaboration can start out in the form of a working group or committee on data protection in financial services. Where working groups on digital finance or FinTech already exist, a sub-group can be established.

Collaboration may be required by the context: should, for example, a FSP offer DIFS (e.g. credit) based on telecommunications data, the use of these data may need to be overseen by both the financial and telecommunications regulators. The Digital Clearinghouse set up by the European Data Protection Supervisor is an interesting example of how cooperation between oversight bodies could be intensified.[12]

2.2.2. Industry cooperation should be promoted to achieve industry-wide standards and best practices

All industry actors must adhere to privacy rules, and if these actors work together, economies of scale and a level playing field can be achieved. In addition, self-regulation may reduce the cost of regulation to society. Industry actors can agree on common standards and best practices for both the domestic and international levels. At the international level, GSMA Mobile Money Certification[13] is a broad self-regulation initiative designed to ensure safer, more transparent and resilient mobile financial services. The Certification is assessed using 300 criteria, which include data privacy and data security requirements in addition to other core risk management and consumer protection principles.

The financial regulator can support industry cooperation and compliance by providing orientation on how to interpret and implement data protection regulations (be they general or specific to the financial sector). For example, the Financial Conduct Authority in the UK holds surgeries for businesses experiencing specific and common issues working with the regulatory framework. The support offered in these surgeries includes Q&A sessions to explore problems and coaching sessions to build attendees' capacities (Cambridge Centre for Alternative Finance, 2018).

2.2.3. Regulatory frameworks for data protection should be developed through consultative processes

A consultative process in the context of regulation is one that allows all key stakeholders to make their voice heard regarding the topic at hand. In addition, consultation helps to establish the legitimacy of regulation by allowing stakeholders to raise concerns and participate in the regulatory process before regulation is implemented. This, in turn, can improve the extent of voluntary compliance with regulation.

12 (accessed on 19 June 2018).

13 For more information, see https://www.gsma.com/mobilefordevelopment/mobile-money/certification/

Consultation is especially important in a new and innovative (sub-)sector such as DIFS, because it is impossible for authorities to anticipate all the implications that a regulatory intervention may have. To effectively protect privacy and personal data and, at the same time, promote innovation, any regulatory intervention must be tailored to the specific context of the country in question. This will require detailed consultation with all key stakeholders, which include but are not limited to

» relevant public authorities (see Figure 1 for more detail),

» financial service providers,

» data analytics firms,

» telecommunications providers, and

» consumer representatives.

A consultative approach to regulatory intervention is extremely important for financial inclusion, as it provides parties with the opportunity to put forward and discuss any negative implications of regulatory intervention and to generate new solutions that regulators may not have thought of. The consultation should be led by the institution in charge of protecting privacy in DIFS (e.g. the financial sector authority or, where it exists, the general data protection authority). Different methods can be used for consultation such as workshops, roundtables and written comments.

2.3. Enhance data awareness

2.3.1. Policy-makers should work to improve the public's digital data literacy

While data collection and processing are increasing at an exponential rate, people's awareness of the implications of these developments is often limited or insufficient. People are often unaware of the data trace they leave when using digital services and of the implications this may have. This is true across the globe, and arguably more so among unbanked populations with comparatively low education and literacy levels. To fully exercise their rights under any data protection framework and to make informed decisions about the use of DIFS, customers must be capable of fully appreciating and weighing up the risks and the benefits.

Policy-makers should make use of effective communication channels to enhance consumers' awareness of data risks and should demand that financial service providers do the same. Awareness of data issues should be part and parcel of any campaign on digital literacy, financial literacy or digital financial literacy. Any such campaign should include efforts to raise awareness about the 'personal data trail' that people leave behind when using digital financial services and about the data-related rights of consumers in the jurisdiction in question. To convey this message, effective communication techniques should be used. These may include visual representations and educational videos. In terms of content, the following ideas could be highlighted:

» Any digital transaction leaves a data trail. Consider this fact – and consult the providers' privacy policy – before using a service.

» Some financial service providers read more of your data than just your financial transactions. Therefore, consider whether accessing the service (e.g. obtaining credit) is sufficiently beneficial for you.

» Some financial service providers read more of your personal data than do others. If your privacy is important to you, compare the providers' privacy policies.

» Your personal data are an asset. They are your asset. Consider what you are prepared to trade your data for.

» Many financial services contracts are basically transactional: you provide access to your data, they provide a service on this basis. Before trading your data in this way, consider whether the benefits of doing so are sufficient.

Enhancing consumer awareness will incur initial costs. However, these will pay off in the long-term as consumer education, if done right, will stimulate effective and informed demand. Better-educated/more-capable consumers will support innovation by generating effective demand for innovative services. Whether consumer education requirements are met can be verified through mystery shopping. Data protection will only be effectively implemented if consumers fully appreciate the implications of using a given service and understand the risks associated with the irregular use of their personal data. Greater consumer awareness will result in more informed decision-making and, in so doing, may stimulate competition based on the customer-friendliness of privacy practices.

2.3.2. Financial service providers should increase internal awareness of data protection issues

Data protection will only be achieved if all those with access to data handle them with due care. Experience shows that many data breaches are the result of internal fraud or negligence. Ensuring compliance therefore includes making all relevant staff fully aware of their duties in this regard. Indeed, any regulatory framework adopted should include this activity as a requirement.

In addition, policy-makers should promote general data ethics among financial service providers, FinTech firms and data analytics companies that store and analyse personal data. These companies could be asked to publish information on their 'company values' and/or privacy policy on their website and in their other prominent communications media.

2.4. Empower customers to be the sovereigns of their data

2.4.1. Customers should be notified about the nature and purpose of the personal data stored

Providers store and process data that consumers generate when using a service. Storage and processing may be necessary for the running of the core business, including the performance of credit contracts. Credit agreements do not serve as a carte blanche to use personal data in any way they please. Only under certain conditions can providers process data or pass them on to third parties for the purpose of offering additional services. The nature and purpose of data storage is not always clear to customers (see Whitley and Pujadas, 2018). When consumers provide their data, they are handing over a key asset. This handover must be a conscious decision and should not happen unknowingly. Furthermore, FinTech companies sometimes use personal data gathered on an individual that might include other people's personal data (e.g. social media feeds, emails, money transfers to contacts). Companies processing extraneous persons' data must respect these people's rights and should put relevant protections in place. This is particularly important given that we already know this is the type of data being used to judge creditworthiness (e.g. the social graph used by companies like Lenddo).

Regulators should ensure financial service providers comply with the requirement to explain (a) what personal data are being collected for what purpose and (b) in cases where data are being collected from third parties (e.g. MNOs) or individuals, why these are necessary for the performance of the contract. These communications should be conducted in a language that the customer can understand and possibly should be supported by pictures, diagrams, flowcharts or videos.[14] Information material should be provided in local languages.

Transparency, fairness and measures to rectify information asymmetry are essential for providing the conditions required for equal access to financial resources. This, in turn, is a cornerstone for sustainable financial inclusion that avoids the exclusionary effects caused by a lack of information.

2.4.2. Consumers should be asked to provide consent when data is processed for a purpose different to that of the original contract

Providers of digital services, such as digital finance, e-commerce and telecommunication providers, capture personal data when providing their core services and these data are sometimes processed for purposes different to those planned or anticipated at the outset. Take the example of telecommunications data: most of these data are not collected for the purpose of supporting credit assessments, yet they are now a mainstay for assessing the credit worthiness of customers lacking other data. While the opportunities are significant, such data should only be employed with customers' informed consent.

Consumers and providers of financial services should meet on equal terms; there should be no information asymmetries that prevent consumers from making informed decisions. Consumers should be informed when their personal data are used for purposes different to those stated in the initial contract. In cases where a financial service (e.g. credit, insurance) requires the processing of personal data that was captured in another context (e.g. mobile phone call data), consumers should be able to make informed decisions on whether or not to provide the personal data required to obtain the service. As a minimum, they should be notified of any intention to use such extraneous data and have the option to opt out.

Policy-makers and competent authorities can make a start by clearly outlining this policy goal and asking financial service providers to come up with solutions. In cases where these providers fail to offer satisfactory solutions, those in power should intervene by imposing relevant regulations.

14 See p. 27 of the World Bank's Good Practices for Financial Consumer Protection – 2017 Edition (World Bank, 2017), and Articles 12, 13 and 14 of the EU GDPR (European Parliament, 2016).

2.4.3. Customers should be able to access, copy, correct and delete their data

Customers have a legitimate right to see what data a provider is holding on them.[15] In addition, when data are stored and processed errors can happen, in which case the controller is obliged to correct the mistakes. Customers are entitled to have wrong or outdated data deleted, and they may even be given a right to data portability, which will enable them to transfer data to another DIFS provider if they wish.

Regulators should consider obliging FSPs as controllers of personal data to comply with these duties. The benefits of providing customers with these rights will need to be weighed against the cost implications for FSPs, which will have to introduce new tools to implement these rights and train their staff accordingly. Regulators can start by outlining this policy goal and asking FSPs to suggest solutions for achieving this goal in the most cost-effective manner. It is in the interest not only of customers but also of DIFS providers to take decisions on access to credit on a sound factual basis in order to avoid exclusionary effects.

2.4.4. Customers must be able to make their voice heard should data issues arise

Financial consumer protection, which is a policy objective in most countries around the world, dictates that financial service providers put in place mechanisms to handle any customer complaint. Complaints in relation to data are therefore simply a specific category of complaint.

Effective complaints-handling mechanisms for data-related issues should therefore be implemented in the context of existing general complaints-handling procedures. The procedure must make sure that complaints-handlers receive all the information required to respond to a complaint. There should also be an escalation procedure for cases where the consumer is not happy with the response (e.g. ombudsperson, central bank).

There may be additional costs, but these should not be too high in the context of general complaints-handling. Ensuring that effective complaints-handling mechanisms are in place will contribute to building trust in the financial sector and specifically in digital/data-driven financial services. While there will be a cost, effective complaints-handling will, in the long-term, foster customer trust and thereby support adoption, innovation and financial inclusion.

15 See Article 13 on the Individual Participation Principle in the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (OECD, 2013), and Articles 15–21 of the GDPR (European Parliament, 2016).

2.4.5. Personal data should be deleted once its purpose is fulfilled

To minimise risks to data subjects, the FSP should delete personal data for which it no longer has a legitimate use when the financial service has been delivered or terminated for other reasons. 'Legitimate use' could include the analysis of data generated on the firm's systems for process optimisation or other legitimate business reasons, where this does not impinge on the rights of data subjects. In some cases, regulators may need to determine whether the risk to data subjects outweighs legitimate use for business reasons and, where it does, must stipulate the deletion of the data in question.

In the absence of legitimate uses, further storage of the data in an identifiable form should require the customer's explicit and informed, freely given consent. While anonymised data may be stored, the type of data used by DIFS often allows for easy reidentification, which means anonymising the data is not a trivial matter.

There may also be a legitimate public interest for retaining personal data in cases where the provider is obliged by law to do so for a specific time period. Such requirements are common for telecommunications and financial services firms, but data held for recordkeeping may not be processed unless there is a legitimate reason to do so. This guideline, rather than negatively affecting financial inclusion, will serve to promote it. If customers are assured that their data are not being retained without legitimate purpose or without their consent, they are more likely to trust the same lender when in need of more financial resources.

Implementation tools

To empower customers to be sovereigns of their data, DIFS providers and the public authorities in this sector should have a privacy management programme in place that:

» gives effect to this recommendation – and indeed to all the other recommendations and principles listed herein;

» is tailored to the structure, scale, volume and sensitivity of its operations;

» makes provision for appropriate safeguards based on a privacy risk assessment (see recommendation 5);

» is integrated into its governance structure and establishes internal oversight mechanisms;

» is updated in the light of ongoing monitoring and periodic assessment.

The OECD's 2013 Guidelines on the Protection of Privacy and Transborder Flows of Personal Data include a requirement for a privacy management programme.21 The level of protection applied to consumer data should essentially be the same, regardless of where the processing takes place (e.g. in the cloud or in another country).

A possible internal oversight mechanism could be the appointment by the DIFS provider of a data protection officer who would serve as a point of contact for customers requiring, for example, access to or the correction of their data. European law provides for such officers for companies and public authorities of a certain size.[16]

2.5. Hold providers accountable

2.5.1. Make automated decision processes interpretable

The growing prevalence of digital services that can function without human intervention means that algorithms make more and more decisions that affect livelihoods. Previously, many of these decisions would have been made by humans, making it possible to assign the responsibility for a specific decision to an individual. Personal assignment of responsibility is, however, difficult where computer code determines outcomes.

Notwithstanding the technical complexity, regulators must be able to hold organisations to account for their automated decision-making if they are to properly discharge their supervisory duties. Accountability in this context refers to the general requirement for DIFS providers to demonstrate compliance with laws and regulations (with or without automatic decision-making).[17] Providers must document decision-making processes in a way that enables supervisors to assess compliance. In the context of supervision, regulators gain access to confidential information that represents business secrets. Such privileged access is warranted by the need to ensure lawful behaviour, but it also constitutes a confidential relationship that imposes a responsibility on the regulator. In this light, the transparency requirements outlined above can be viewed as the provision of information to customers, whereas accountability means the provision of information to regulators. This section focuses on accountability rather than transparency.

Statistical models for large and high-dimensional datasets, also referred to as 'big data', often have complex functional forms. It is commonly the case that the inner workings of machine learning models that turn data into decisions cannot be explained in an intuitive, direct manner. However, interpretability need not imply a logical if-this-then-that decision framework, or a linear boundary that 0.4 of one factor and 0.6 of another determine the decision, or the like. With the development of new methods, tools that can provide insights into complex algorithms are advancing. For instance, it may be deemed sufficient to identify the three most important factors that shaped a decision in an individual case, rather than to know the entire decision function. Even notoriously complex tools such as neural networks can be interpreted in some circumstances. Whether such tools offer sufficient interpretability is a context-specific question that cannot be answered upfront for all situations. However, regulators must be satisfied with a level of interpretability that allows them to perform their oversight function on the basis of reasonably clear evidence about the automated decisions of a given system.

In the DIFS realm, decisions that affect livelihoods and rules around financial inclusion must be enforced. Black box algorithms that preclude interpretation may violate anti-discrimination laws or take otherwise untenable actions. Compliance with rules and regulations can be verified if decision-making processes are sufficiently clear. In some cases, such as decision trees or linear models, interpretability is inherent in the method. A lot of research has been carried out on neural network interpretability, with a high level of success in the image domain. A recent example, the LIME tool (Tulio Ribeiro et al., 2016), is an approach that works for several types of models. The state of the art is developing quickly, and regulators should be open to new methods if they meet their objectives. While the onus should be on DIFS providers to demonstrate that their methods are interpretable, the regulators will need to verify such claims critically and thoroughly, testing results not just for interpretability but also for evidence of prohibited discrimination and other unlawful practices. One idea for implementing interpretability in an auditable fashion is to require the construction of sandboxes for regulators (see annex).

It can be difficult for many modern statistical architectures to fulfil the demand for interpretability in automated decision-making processes. Methods and therefore products or even providers may be excluded from the market, leading to a more limited offering. If it causes some households to miss out on products, then the interpretability requirement has negative consequences for financial inclusion. The trade-off

16 Articles 37, 38 and 39 of the EU GDPR (European Parliament, 2016).

17 In the annex on Data Protection Principles, see principle 6 on Accountability.

between a well-regulated industry and broadest possible access may be insurmountable in some cases, leaving each country to decide where to draw the line between these two possibly conflicting objectives.

2.5.2. DIFS providers should document their decision processes clearly and comprehensively

DIFS providers should produce clear documentation for their automated decision-making processes. DIFS are offered on the basis of customer data. In addition, DIFS providers and their business partners, such as analytics firms, may themselves produce data. Accountability of the DIFS decision-making process implies accountability about the nature and sources of data used and produced. DIFS providers should produce an exhaustive and detailed listing, herein called a 'data map'. This map should show the origins and uses of inputs, the processes that lead to outputs, the nature of these outputs and their intended uses. The documentation should include related processes, data sources and groups of algorithms, or should simply be a straightforward input-to-output process. Either way, the documentation should clearly explain each part of the decision-making process drawing on the results of the algorithmic interpretability exercise as well as on the data map.

A clear understanding of the sources, nature and uses of data items is necessary for compliance and oversight. Only when an organisation has a full picture of the data it holds, can it verify that it is meeting its obligations. In the same vein, supervisors need to be able to audit the comprehensive data archive of a regulated DIFS provider, a task that can be executed much more efficiently and thoroughly where full descriptive information is available. The verification of compliance in the DIFS space implies an inspection of computer systems. Such systems, especially when run on a large scale, can be difficult to understand for anyone not involved in their construction. A system inspection can be made vastly easier when such supplementary information is available. In turn, the inspection is necessary to regularly ascertain whether DIFS providers are complying with laws and regulations, and it represents the starting point for a detailed audit.

Regarding the data mapping, the items detailed should include, for example, the data sources and the variables they contain, and their data types and formats, storage locations, version control, parties responsible for management, metadata category encodings and units, sensitive and personal aspects of the dataset, and access rights. Equipped with such information, regulators can readily verify that data-focused rules and regulations are being followed. A flowchart of the decision-making process can visualise the flow of information through the process. When it is combined with the data map and the interpretability results, the resulting document gives an initial insight into the decision-making process. However, more context-specific details are likely to be required for an in-depth assessment of regulatory compliance.

Two aspects with a bearing on financial inclusion stand out. One is the administrative cost of producing and updating the information, which may be burdensome for a small firm and thus represent a risk to fragile early-stage finances. However, financial services are a regulated industry and such costs are simply the cost of a ticket to access the financial opportunities of this space. The second aspect is quite simply that good documentation supports procedural quality. A firm may benefit from reviewing its operations and perhaps learn so much that it becomes better at what it does. Overall, these effects are likely to be small in both cases.

2.5.3. DIFS shall not discriminate according to inadmissible criteria

Many financial services involve payments made from one party to another now, in return for repayments made in the future. Loans, savings and insurance are variations on this theme. The ability and willingness of the contracting party to honour the future leg of the deal determine whether it will be an economically viable transaction. This reality makes discrimination an inherent and essential aspect of DIFS; firms need to discriminate between customers if they are to offer their services on a sustainable basis.

Discrimination on the basis of income and assets is generally accepted in the credit industry. Other criteria may function as proxies for such fundamental determinants, but not all criteria are deemed acceptable bases for decisions. Many societies do not allow discrimination on the basis of sex, race, religion or disability. The determination of permissible criteria for discrimination is a political decision shaped by cultural, social, moral and religious values, and each society needs to make its own decision on what it deems acceptable. For example, the Ghanaian Data Protection Act of 2012 restricts the processing of 'special data', namely data on children under parental control and on an individual's religious or philosophical beliefs, ethnic origin, sex, trade union membership, political opinions, health, sexual life or criminal behaviour.

As discrimination by DIFS providers entails decisions that affect the economic life of households, it can have important effects on households and communities. Discrimination along specific lines will result in a reduced choice of services for the affected groups. On the flipside, prohibition of discrimination will reduce the profitability of DIFS providers if the discrimination is economically justifiable. To maintain a given rate of return, the providers will then need to charge higher prices to their other customers. Such are the real costs of anti-discrimination policies, which need to find their expression in DIFS regulation as in other areas of public policy. The USA serves as a good example here, because its federal law forbids discrimination on the grounds of race, age, sex or marital status when giving access to credit, even if these categories are statistically predictive of future repayment behaviour.[18]

The regulators' primary task is to codify and enforce prohibitions on discrimination. This may include guidance on how non-discrimination legislation is to be interpreted in the DIFS context, such as the mapping of legal groupings onto measurable indicators used in decision-making processes. Discrimination according to characteristics such as disability, race, religion or sex may be prohibited, in which case these criteria should also be factored into the work of the DIFS regulators. In addition, the regulators need to test whether DIFS providers are complying with the relevant laws and regulations. The documentation of decision-making processes, including the inspection of the variables used and their interaction in algorithmic processes, is the main feature of the regulator's supervision. A sandbox approach, described in the annex, is a practical tool for testing whether prohibited systematic discrimination occurs in a given decision process.

Decisions on what constitutes permissible discrimination is an outcome of the political process that goes beyond the technical implementation of regulation. The resulting costs and benefits may vary from one group to the next, and the regulator can provide information on its estimate of these effects. Most obviously, permissible discrimination excludes certain groups from accessing DIFS. However, in situations where such discrimination is economically beneficial but not allowed, the costs of the non-discrimination policy then need to be borne by the remaining customer base. The higher expense may make participation unviable for some and reduces the overall benefit to all. In extreme cases, the entire business model may become unviable, leading to financial exclusion for all potential customers. Morality-based choices of the kind mentioned above may have undesirable economic consequences, but ethical values may well override narrow economic concerns.

18 See p. 16 of Carroll and Rehmani, 2017. http://www.oliverwyman.com/content/dam/oliver-wyman/v2/publications/2017/may/Alternative_Data_And_The_%20Unbanked.pdf

2.5.4. All providers and stakeholders seeking to use automated decision-making should consider the impact of and assess the risks involved in the data processing they envisage

A data privacy risk assessment (DPRA) is a structured approach to evaluating the possible adverse effects that a proposed DIFS system can have on individuals' privacy.[19] A DPRA contains several components, namely it should (a) describe the nature, scope, context and purposes of the processing, (b) assess necessity, proportionality and compliance measures, (c) identify and assess risks to individuals, and (d) identify any additional measures to mitigate those risks. It should be conducted whenever the processing poses a significant risk and should be undertaken as a matter of course for major projects.

The DPRA is the culmination of the documentation efforts proposed in this and other guidelines, for instance those governing safe data storage. It summarises the risks that data storage, processing and use pose for individuals, such as the possibility of unfair discrimination, loss arising from inadequate security practices, etc. In so doing, it offers a useful overview of regulatory risks to individual interests. A comprehensive overview of this sort provides a useful basis for discussions between regulators and DIFS providers and gives the supervisors an opportunity to consider the adverse consequences that a business process poses in all aspects of the DIFS providers' relations with customers. While not a sufficient basis for regulatory clearance, the DPRA can go a long way to assessing conditions for lawful and fair processing.

The responsibility for carrying out[20] a DPRA lies with the DIFS provider. The regulator is responsible for ensuring that DPRAs are carried out where necessary and for evaluating whether the assessment is correct. An in-depth assessment is particularly called for during the licensing or approval stage of a new service, with the assessment focusing on any changes that have greater relevance for regulator reporting requirements. Importantly, supervisors should verify that risks are correctly identified and that mitigating measures are appropriate and proportionate.

19 In Germany for example, even before the GDPR came into force, such privacy risk assessments were obligatory in cases where the automated processing of personal data entailed specific risks. The discrimination risk assessment is a new concept.

20 A good example of practical guidance for organisations preparing a DPRA is provided by the UK's ICO. https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

A DPRA may identify activities for which the proposed mitigating measures are insufficient to allay risks to individuals. Steps taken in response to a DPRA failing to gain regulatory clearance may involve an adjustment of the process, an upgrading of the mitigation strategy or an outright prohibition of the activity. In each case, the regulatory framework is strengthened and inappropriate operating procedures are rooted out. More broadly, this is an example (a) of the compliance measures suggested in this guideline that also impact on financial inclusion indirectly by influencing levels of consumer trust in the industry, and (b) of the regulatory framework that guarantees the safeguarding of rights and the meeting of obligations. The DPRA should be extended to include possible illegal discriminatory and financial exclusion effects felt not only by individual customers, but also by groups of individuals.

Implementation tools

Here again, it is recommended that each DIFS provider and public authority establish a privacy management programme (see section 2.4 above). Indeed, the *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (OECD, 2013) explicitly favour this approach as a way to implement accountability.[21] Documentation can be described in a data map that provides an overview of the sources and outputs, allowing for the targeted auditing of compliance for specific data categories. The interpretability of the decision-making process needs to be addressed with method-specific tools, such as the LIME tool mentioned above, which is an approach that works for several machine learning methods. Sandboxing, as outlined in the appendix, provides a framework for verifying whether the decision-making process can be replicated, interpreted and adjusted according to the documentation provided.

2.6. Enforce secure data storage

2.6.1. Strict data security should be maintained in all DIFS systems

Information on livelihoods, such as details on income and assets, is a highly sensitive data category. Leakage of this kind of information to the public can have adverse social, economic and even security implications for the data subjects. Secure storage of the data gathered by DIFS providers is a fundamental duty of those accumulating and using such data. It is not enough for regulators simply to ensure that the firms they oversee follow adequate security procedures; they should themselves lead by example and implement their own stringent procedures. Up-to-date security protocols, access rights within the organisation and verification of third-party standards are key aspects of secure data storage.

Secure data storage comprises several components, and the maintenance of high technical standards in this area is as integral a component of good management as physical safety or accounting standards are. Data is the raw material of DIFS and we can say that secure data storage is to digitally native businesses what physical security is to bank vaults. Bank robbers are something of a rarity now, but crime in cyberspace is growing and the risks of careless behaviour grow in accordance with the value of information resources. Data loss and theft are major operational risks in the digital economy, so they need to become supervisory priorities as well.

One aspect of data security is to protect the resource – data – on which DIFS propositions are built. Data pertinent for DIFS decisions are not just of economic value, they also comprise sensitive personal information on individuals and thus require special protection. Unauthorised access to data, their abuse by insiders or outsiders, not only affects the individuals whose data get sold in shady corners of the web, but also hinders the acceptance and uptake of new technologies. Particularly in countries with fragile banking systems and volatile market conditions, a major data breach has the potential to undermine systemic confidence in the financial sector and trigger a crisis with real macroeconomic effects.

Technology standards move fast, but principles remain stable. For instance, data security starts with the internal procedures of organisations storing information. Limiting access to individuals who require specific data items lowers the risk of data loss, theft and manipulation. Data access policies should specify who has access to each item listed on the data map described above. Aspects of the policy include password-protected storage; segregation of users into groups with varying rights, data access and modification logs; and clear staff guidelines that detail both operational procedures and expectations around responsible data use. Other dimensions of secure storage include such diverse areas as password policy, software maintenance, network administration, cryptography, device management, and cloud service restrictions.

21 See Article 15 in OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (OECD, 2013).

To protect data subjects, both the hardware and software used for their data need to be of a modern standard. Physical security is similarly important and includes premises access controls, disposal protocols for expired storage devices, back-up policies, guidelines on portable media and laptop use, etc. For this, a flexible regulatory approach[22] is required, drawing on private sector expertise and coordination. Encouraging codes of conduct and industry self-certification may be an effective way to ensure compliance with the principle of secure data storage. The onus of supervision rests with the authority that regulates the activities of the data processor; this authority may need to bring in data security experts to become routine contributors to overall regulatory compliance assessments.

When compared against the limited market opportunities present in smaller economies, the high fixed cost of compliance with modern data security measures may appear prohibitive. To encourage innovation, regulators might prefer a light touch regime that avoids 'throwing the baby out with the bathwater' – i.e. missing out on valuable opportunities in an attempt to avoid the downsides of compliance costs. Nonetheless, regulators need to consider that the protection of customer data is not merely a matter of company interest; it is also important to the development of the wider sector. A graduated regulatory approach that adjusts its requirements to reflect the risks arising may be advisable when seeking to create a vibrant DIFS ecosystem built on the basis of consumer trust.

2.6.2. Companies should limit third-party access to their data

Data is a special kind of resource: it may be valuable, but it can be duplicated at little or no cost. Organisations may be tempted to share data when an opportunity arises, opting for the chance to profit in return for exposing their data subjects to risk. Once the data is handed over, internal policies that protect data subjects from prying eyes can lose their effect if the right safeguards are absent. Organisations should only hand over data to third parties that have strong and effectively enforced policies on data access and secure storage. Ensuring equivalent standards when sharing data is as important as maintaining high standards in-house. Third-party sharing should be clearly highlighted in financial services' terms and conditions so that consumers can consider whether to give consent.

Much of the innovation witnessed in digital financial services is the result of alliances between firms. A prime example is mobile money, where MNOs work with banks to provide the unbanked with financial services. With the digital platform in place, other companies can then use it to provide additional services, such as third-party loan or savings products. Start-ups and alliances emerge quickly, which is largely good news for consumers. However, data security standards must be maintained. The sharing of customer information – be it intended for targeted marketing by third parties, for third-party product development on behalf of incumbents or for any other relationship – must not be used as an excuse to lower data protection standards.

As happens with firms' internal access policies, organisations should define the conditions under which they are prepared to share data with third parties and the standards they expect from these parties. The outsourcing of data functions should not be an excuse to reduce standards. Consequently, the third party should be able to demonstrate an equivalent level of data security, meaning it should have a similarly stringent internal access policy and should limit its own information sharing with third parties.

While the sharing of data between organisations carries risks, it also promises to make DIFS-enabling customer data available in situations where traditional information sources are lacking. Consistent data-sharing policies are therefore necessary to support a healthy DIFS ecosystem that can maximise opportunities for the financially excluded.

Implementation tools

Today's arms race between computer hackers and IT administrators means that resources on data security and sharing are both extensive and under constant development.[23] How to put these resources to good use is best judged by experts on the ground who are familiar with the technology and skills available and the risks present in their regulatory domain. Technical guidance that sets out minimum security standards and prescribes measures can be formulated as regularly updated guidelines and then published on the regulator's website. Similarly, third-party data sharing needs to be couched within the terms of country-specific conditions, with existing data protection legislation especially relevant. The publication of specific implementation instructions that draw on the legal framework helps to clarify regulatory requirements.

22 The UK's now-defunct Financial Services Authority published Data Security in Financial Services (Financial Services Authority, 2008), which provides a useful overview of the important topics to address when designing a secure DIFS system.

23 A list of key issues can be found in the report by the UK's now-defunct Financial Services Authority, Data Security in Financial Services (Financial Services Authority, 2008).

3 I CONCLUSION

Given that the best approach to addressing data protection is one that is tailored to the specific context of a given jurisdiction, the different recommendations offered above should not be treated as 'best practice'; rather, they should be understood as suggestions and orientation on how to address new regulatory issues arising in relation to the responsible use of personal data and automated decision-making in financial services. In this way, the recommendations can be used to inform discussions and support the drafting and implementation of respective regulations.

With this publication, targeted at financial sector policymakers, regulators, and other authorities mandated with creating policies and regulations that affect the use of data in financial services, we hope to have contributed to future discussions around data protection in DIFS. In return, we would very much welcome readers' comments and feedback by email at sv.fse@giz.de

ANNEXES

1 Definitions[24]

PRIVACY is 'the presumption that individuals should have an area of autonomous development, interaction and liberty, a "private sphere" with or without interaction with others, free from state intervention and from excessive unsolicited intervention by other individuals'.

INFORMATION PRIVACY OR DATA PRIVACY is the right of natural persons to control and determine freely and on the basis of sufficient information if, how, to what extent and for what purposes information about his or her person are to be collected and used by others.

PRIVACY-ENHANCING TECHNIQUES are techniques that minimise or eliminate the collection of personal data.

DATA PROTECTION has generally come to mean information privacy, decision on usage plus access and correction rights of the data subject, security and integrity.

PERSONAL DATA is defined as including information relating to an identifiable individual including but not restricted to address, national identification number, date of birth, facial image, vehicle registration number, fingerprints, a computer's IP address and CCTV video footage. 'Personal data' also applies to the ability to combine different categories of information to identify a person.

SENSITIVE PERSONAL DATA OR SENSITIVE PERSONAL INFORMATION is a subset of personal data requiring stricter protection than non-sensitive data. Sensitive personal data are data like racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual identity.

BIG DATA describes primarily extremely large data sets (structured or unstructured, from public or internal sources such as mobile communications networks) which are characterised by their huge volume, the velocity with which they are accumulated and their variety.

BIG DATA ANALYTICS is used to identify computational technologies that analyse large amounts of data to uncover hidden patterns, trends and correlations.

DATA SECURITY describes the requirements on controllers to protect data from unauthorised attack, theft or manipulation. These data are not necessarily personal data or data in a digitised format.

CYBER SECURITY entails data security – again not limited to personal data – and the security of information technology. It includes the ability of network and information systems to resist, at a given level of confidence, any unauthorised access or misuse that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data, applications or the related services offered by, or accessible via, those network and information systems.

24 All these definitions are taken from the GIZ publication Selected Regulatory Frameworks on Data Protection for Digital Financial Inclusion (Dix, 2017).

2 Data protection principles

Data protection laws and regulations are typically derived from general principles that provide direction and guidance. Here we review one such list of principles – that contained in article 5, paragraphs 1 and 2, of the European Union's General Data Protection Regulation (GDPR) – and discuss the extent to which the principles it contains provide unequivocal guidance. In many cases, we also refer to the tensions inherent in digital financial services. The following comprises a brief summary of the seven principles laid down in Article 5 of the GDPR. The primary aim of this summary is to situate the principles in our context of digital financial services in low- and middle-income economies.

As of 2018, the EU's GDPR is probably the most ambitious, stringent and wide-reaching data protection legislation to have been passed anywhere in the world. The 'Brussels Effect' means that it is likely to find widespread adoption beyond its legal remit as multinationals seek to adhere to the highest standards of any major market in order to provide consistent processes across their global operations. It is neither the only nor necessarily the best example of data protection legislation, but it is likely to set standards.

For each principle, we outline its meaning and then interpret its application to a DIFS context. The thoughts presented draw on the tensions developed and highlight areas where cautious implementation is desirable to mitigate the risk of imposing disproportionately restrictive regulation. It should also be pointed out that the principles are not absolute but must be weighed against other rights. The most likely friction in this area is between the legitimate commercial interests of firms and the valid data-protection interests of individuals. Regulators may wish to provide guidance on appropriate policies in situations where such a tension is likely to emerge.

1) Lawfulness, fairness and transparency

Meaning ›› Lawfulness means that there must be a legitimate reason, also known as the 'lawful basis', for processing the data. Data subjects' consent constitutes a possible legal basis. In addition, the consent it must not violate any laws in the process. Consent needs to be informed, explicit and freely given. Besides consent, the necessity of data for the performance of a credit contract is another and, in this context, more important legal basis. Unlike with consent, the data subject cannot prevent (or later revoke her or his consent to) the collection and processing of personal data that are necessary for this purpose. However, as in the case of consent, the customer seeking access to financial resources must be fully informed before he or she can enter into a contract that could form the legal basis of data processing. **Fairness** means that processing cannot be unduly detrimental, unexpected or misleading to the individuals concerned. **Transparency** refers to being open and honest towards the data subjects, making it clear for what purposes the data is being used.

Thoughts regarding financial inclusion ›› Fairness and transparency are key requirements for entering into a valid contract. When entering into a financial agreement on the basis of adequate information, the customer explicitly agrees to the processing of all relevant personal data. The question as to whether an opt-out rather than an opt-in should suffice to provide for valid consent arises in the use of personal data for marketing purposes. In contrast, as financial inclusion involves offering credit facilities on a contractual basis, explicit and informed consent on data use is required. Financial inclusion does not justify the lowering of consumer and data protection standards for unbanked people.

2) Purpose limitation

Meaning ›› The purpose of the processing must be clearly stated at the outset. In cases where personal data are used for a different purpose that is not compatible with that stated at the outset, there must either be a lawful basis or consent for this different use.

Thoughts regarding financial inclusion ›› DIFS providers often wish to inform their decision-making using data that were collected for a different purpose. For instance, telephone records are used in Kenya to establish creditworthiness for small-scale mobile money lending. Given the paucity of data with which individuals can establish credibility vis-a-vis DIFS providers, any data that can yield insights into people's (likely future) behaviour can be a game changer when it comes to enhancing access to finance. However, when people feel their privacy is being compromised, they may lose trust in the financial system.

3) Data minimisation

Meaning ›› Only personal data that are relevant and necessary for a specified purpose can be collected and used.[25] Both this principle and principle 2 on purpose limitation are intimately related with the maxim of 'privacy by design and by default', which conveys the need for data protection and privacy safeguards to be considered at each stage of the design and construction of a data processing system. Instead of treating privacy and data protection as hurdles to be surmounted once a system has been built, they should be considered upfront and throughout. What is required is the treatment of data protection as an inherent characteristic rather than as a bolt-on feature.

Thoughts regarding financial inclusion ›› In a similar vein to the points raised before, it may not be in individuals' interest to minimise the data that service providers hold on them. If such data can be used to facilitate financial inclusion, then the collection and storage of additional data points may actually be helpful. However, national legal restrictions on the collection and use of sensitive data, such as race, ethnic or tribal origin, sex, marital status or age, must be taken into account.

4) Accuracy

Meaning ›› Organisations should take steps to ensure that the personal data they hold is factually correct, that these data are corrected where mistakes become known, and that accuracy-related complaints are carefully considered. This also applies to situations where a mobile money provider accumulates inaccurate information on a customer.

Thoughts regarding financial inclusion ›› In some countries, consumer protection standards are lacking and, compared with big business, individuals can be relatively powerless. The complaints-handling procedures (including those in relation to requests for data correction) that regulators should institute therefore carry special weight.

5) Storage limitation

Meaning ›› Personal data must not be kept for longer than is necessary for legitimate purposes. A policy on retention periods should be implemented and providers should be obliged to delete the data once this period has expired. Furthermore, individuals should have a right to have their data deleted if they have been unlawfully collected.

Thoughts regarding financial inclusion ›› As with lawfulness and data minimisation, there is a case for nuanced enforcement of storage limitation. At the time when data are collected, novel uses for a given item of data may not yet have been foreseen. Given the fast pace at which new DIFS are emerging, past data may provide the evidence needed to facilitate access to financial services. Their secure storage should therefore be permitted in cases where customers have consented to such extended storage. In addition, just as there are other legal bases for data processing in addition to informed consent, there are also other legal grounds for data retention besides the requirements of contract-specific consent. Regulators may need to weigh legitimate interests, in particular regarding the use of data generated by a firm's own systems, against the storage limitation principle. Storage beyond contractual needs that is in the public interest (e.g. for law enforcement, crime prevention, etc.) may also be prescribed by law, as is the case for telecommunications and financial service providers in a number of jurisdictions.

6) Security

Meaning ›› Personal data must be protected with appropriate security measures.

Thoughts regarding financial inclusion ›› Due to the non-traditional origin of DIFS-relevant data, a common data security framework is paramount for a trust-based, inclusive industry that supports the needs of individuals and companies. Even if compliance costs in this area are high, regulators should lead by example and ensure that their own efforts are copied throughout.

7) Accountability

Meaning ›› The storage and use of personal data implies taking responsibility for their processing, which includes compliance with these principles. Compliance includes the existence of appropriate measures, policies and processes, as well as recordkeeping to document said compliance.

Thoughts regarding financial inclusion ›› As with privacy by design, we recommend 'accountability by design' as a maxim to apply to the architecture of digital systems. It is essential for the success of accountability-enhancing rules and regulations that they be matched with regulatory resources. To be accountable for their own policies, regulators should put in place sufficient labour resources to audit and supervise the DIFS providers from whom they demand accountability. Note that actioning these recommendations will place extensive demands on DIFS providers to provide information on their activities.

25 See, for example, section 19 of the 2012 Ghana Data Protection Act (Republic of Ghana, 2012).

3 Sandboxing

Inspired by the methods used for testing new software in a secure, stand-alone environment, sandboxes are an approach for safely trialling new products and services and therefore serve as a versatile tool for regulators in the digital age. Regulators such as the UK's Financial Conduct Authority and the Bank of Sierra Leone have used sandboxes with the main aim of supporting **FinTech** (financial technology) development. Using this approach, FinTech firms can test new business ideas in a secure environment with lower regulatory requirements, combined with close oversight and advice. One variation on the sandbox concept is for the regulator to provide access to restricted personal or market data within an isolated development environment.

The term **RegTech** (regulatory technology) may be used to describe firms or public sector organisations that explore solutions to public policy and regulation problems. For start-ups and new initiatives, a sandbox can overcome the chicken-and-egg problem of achieving accreditation without a proven technology platform, and vice versa. However, a level of caution is required when implementing sandboxes. One concern is that they may give the participating firms an unfair advantage. Sandboxes should therefore only be employed for services that are unlikely to emerge in their absence, and the participant selection process should be transparent, open and accessible to avoid accusations of preferential treatment. In addition, only services designed to respect privacy principles when implemented outside the sandbox should be considered.[26]

A third sandbox option for regulators is to turn the idea on its head and ask regulated firms to set up a sandboxed version of their automated systems. This kind of **inverse sandbox**[27] provides a practical testing environment for supervisors to verify rule-compliant software and system design. Examples of tests could include the systematic variation of the input data to test for prohibited discrimination in decision outcomes, or the closer inspection of the algorithmic decision criteria with the help of interpretation methods. Testing the procedural regularity of the system (i.e. whether it performs its functions in a consistent, repeatable manner) is another example of where a sandbox approach is more helpful than looking at components in isolation. Given the compliance cost of building an automated system, regulators need to be confident, before commissioning the system, that they will make enough use of it to justify the expense.

26 The 2017 CGAP paper Regulatory Sandboxes and Financial Inclusion (Jenik and Lauer, 2017) contains useful international evidence on the implementation methods, risks and opportunities of sandboxes.

27 This idea is described in Nesta's blogpost 10 principles for public sector use of algorithmic decision making (Copeland, 2018).

4 Digital lockers

Governments and public authorities may choose to consider tools other than regulation to empower consumers in the digital age. India's digital locker or 'DigiLocker', which forms part of the IndiaStack[28] initiative, is an example of a public initiative aimed at supporting consumers in deciding how parts of their documents are shared with whom. DigiLocker is a publicly-owned centralised data storage and verification system and, as its data can be linked to one of the 800 million or so 'Aardhar' unique personal identification numbers, it is the prime example of large-scale personal data storage. As part of the IndiaStack project to digitise government operations, DigiLocker allows users to store, sign and share personal documents via the cloud. By June 2018, DigiLocker users had uploaded and e-signed 16 million documents.

The concept of giving public bodies the authority to issue official documents directly into a digital locker could be extended to include other (possibly accredited) data providers such as MNOs. DIFS providers could request access to specific data from users that are required for the provision of their services, perhaps via standardised procedures that facilitate proper notification, explanation and thus informed consent.

Although early experiences with DigiLocker have been promising, the system has had its share of critics. Most seriously, a number of data breaches were reported, which arose due to lax data security at the public bodies entrusted with access to the data. The strength of having centralised personal data storage is also its weakness: by collecting important, verified information in a single place, a single data breach is sufficient to expose individuals to a major loss of privacy. Nonetheless, the potential benefits appear substantial for countries where consumers struggle to establish a digital track record that facilitates financial inclusion.

28 See http://indiastack.org/about/

BIBLIOGRAPHY

AFI (2017), 2017 Maya Declaration Progress Report – Commitments to impact, Alliance for Financial Inclusion, Kuala Lumpur, Malaysia, retrieved on 22 June 2018 from www.afi-global.org/sites/default/files/publications/2017-09/2017_MAYA_progress%20report_digital.pdf

Buttarelli, G. (2017), 'The Digital Clearinghouse gets to work' (2017), European Data Protection Supervisor, accessed on 24 June 2018 at edps.europa.eu/press-publications/press-news/blog/digital-clearinghouse-gets-work_en

Cambridge Centre for Alternative Finance (2018), Guide to Promoting Financial & Regulatory Innovation – Insights from the UK, Cambridge, UK, accessed on 4 July at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/701847/UK_finanical___regulatory_innovation.pdf

Carroll, P. and Rehmani, S. (2017), Alternative Data and The Unbanked, Oliver Wyman, retrieved on 22 June 2018 from www.oliverwyman.com/content/dam/oliver-wyman/v2/publications/2017/may/Oliver_Wyman_Alternative_Data.pdf

Copeland, E. (2018), '10 principles for public sector use of algorithmic decision making', Nesta, London, UK, retrieved on 24 June 2018 from https://www.nesta.org.uk/blog/10-principles-for-public-sector-use-of-algorithmic-decision-making/

Costa, A., Deb A. and Kubzansky, M. (2015), Big Data, Small Credit: The Digital Revolution and its Impact on Emerging Market Consumers, Omidyar Network, retrieved on 24 June 2018 from www.omidyar.com/sites/default/files/file_archive/insights/Big%20Data,%20Small%20Credit%20Report%202015/BDSC_Digital%20Final_RV.pdf

Dix, A. (2017), Selected Regulatory Frameworks on Data Protection for Digital Financial Inclusion, GIZ, Eschborn, Germany, retrieved on 24 June 2018 from https://www.eaid-berlin.de/wp-content/uploads/2017/12/Selected-Regulatory-Frameworks-on-Data-Protection-for-Digital-Financial-Inclusion-GIZ-09-2017.pdf

European Parliament (2016), Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), retrieved on 22 June 2018 from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

Financial Services Authority (2008), Data Security in Financial Services, London, UK, retrieved on 24 June 2018 from https://www.fca.org.uk/publication/archive/fsa-data-security.pdf

GPFI (2016), Global Standard-Setting Bodies and Financial Inclusion: The Evolving Landscape, G20 Global Partnership for Financial Inclusion, Washington DC, available at http://www.gpfi.org/sites/default/files/documents/GPFI_WhitePaper_Mar2016.pdf

GSMA (2018), 2017 State of the Industry Report on Mobile Money, London, UK, retrieved 24 June 2018 from https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2018/05/GSMA_2017_State_of_the_Industry_Report_on_Mobile_Money_Full_Report.pdf

GSMA (2018), 'About the certification', GSMA Mobile Money Certification website, accessed on 24 June 2018 at https://gsmamobilemoneycertification.com/about-the-certification/

Hwang, B.-H. and Tellez, C. (2016), The Proliferation of Digital Credit Deployments, CGAP, Washington DC, retrieved on 24 June 2018 from www.cgap.org/sites/default/files/Brief-Proliferation-of-Digital-Credit-Deployments-Mar-2016_1.pdf

IndiaStack (2018), 'What is IndiaStack?', accessed on 24 June 2018 at http://indiastack.org/about/

Information Commissioner's Office (2018), 'Data protection impact assessments', Guide to the General Data Protection Regulation, London, UK, pp. 186–192, retrieved on 24 June from https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf

Jenik, I. and Lauer, K. (2017), Regulatory Sandboxes and Financial Inclusion, CGAP, Washington DC, retrieved on 3 July 2018 from http://www.cgap.org/sites/default/files/Working-Paper-Regulatory-Sandboxes-Oct-2017.pdf

Jentzsch, N. (2016), Data protection in the context of digital financial services and Big Data, GIZ, Eschborn, Germany, available at http://www2.giz.de/wbf/4tDx9kw63gma/Datenschutz-Diskussionspapier_E_140416_Internet.pdf

McKinsey Global Institute (2016), Digital Finance for All: Powering Inclusive Growth in Emerging Economies (2016), retrieved on 24 June 2018 from https://www.mckinsey.com/~/media/McKinsey/Featured%20Insights/Employment%20and%20Growth/How%20digital%20finance%20could%20boost%20growth%20in%20emerging%20economies/MGI-Digital-Finance-For-All-Executive-summary-September-2016.ashx

OECD (2008), Introductory Handbook for Undertaking Regulatory Impact Analysis (RIA), Organisation for Economic Co-operation and Development retrieved on 24 June 2018 from https://www.oecd.org/gov/regulatory-policy/44789472.pdf

OECD (2013), OECD Guidelines Governing the Protection of Privacy and the Transborder Flow of Personal Data, Organisation for Economic Co-operation and Development, retrieved 24 June 2018 from www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf

Owens, J. and Wilhelm, L. (2017), Alternative Data Transforming SME Finance, G20 Global Partnership for Financial Inclusion, Washington DC, retrieved on 22 June 2018 from www.gpfi.org/sites/default/files/documents/GPFI%20Report%20Alternative%20Data%20Transforming%20SME%20Finance.pdf

Privacy International (2017), Fintech: Privacy and Identity in the New Data-Intensive Financial Sector, London, UK, retrieved on 22 June 2018 from https://privacyinternational.org/sites/default/files/2017-12/Fintech%20report.pdf

Republic of Ghana, Data Protection Act, 2012, retrieved on 24 June 2018 from www.dataprotection.org.gh/sites/default/files/Data%20Protection%20Act%20%2C%202012%20%28Act%20843%29.pdf

Tulio Ribeiro, M., Singh, S. and Guestrin, C. (2016), Model-Agnostic Interpretability of Machine Learning, University of Washington, Seattle, USA, accessible via arXiv:1606.05386

Whitley, E. and Pujadas, R. (2018), Report on a study of how consumers currently consent to share their financial data with a third party, Financial Services Consumer Panel, London School of Economics and Political Science, UK, retrieved on 29 June 2018 from https://www.fs-cp.org.uk/sites/default/files/fscp_report_on_how_consumers_currently_consent_to_share_their_data.pdf

World Bank (2017), Good Practices for Financial Consumer Protection – 2017 Edition, Washington DC, retrieved on 24 June 2018 from https://openknowledge.worldbank.org/bitstream/handle/10986/28996/122011-PUBLIC-GoodPractices-WebFinal.pdf

Deutsche Gesellschaft für
Internationale Zusammenarbeit (GIZ) GmbH

Registered offices
Bonn and Eschborn

Friedrich-Ebert-Allee 36 + 40
53113 Bonn, Germany
T +49 228 4460-0
F +49 228 4460-1766

Dag-Hammarskjöld-Weg 1 - 5
65760 Eschborn, Germany
T +49 6196 79-0
F +49 6196 79-1115

E info@giz.de
I www.giz.de

On behalf of

Federal Ministry
for Economic Cooperation
and Development