Financal Systems Development

Selected Regulatory Frameworks on Data Protection for Digital Financial Inclusion

giz 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 'Financal Systems Development'

Author:
Alexander Dix, European Academy for Freedom of Information and Data Protection

Responsible:
Judith Frickenstein, Konstantin Pagonas, Sector Programme 'Financal 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, September 2017

Table of Contents

FOREWORD

Two billion adults globally do not have access to formal financial services and thus cannot fully participate in economic activities that could improve their lives. Likewise, 300 million businesses do not have access to the credit needed to grow and expand, which hinders them from contributing to economic growth and being a job creator. Digitalisation continues to transform the global financial sector and creates good opportunities to foster financial inclusion if the potential risks are well managed. In fact, to add to the tremendous gains in financial inclusion that have already been achieved, digital financial services, together with effective regulation and supervision, are considered essential to close the remaining gaps in financial inclusion.

To balance the risks and opportunities of digitalisation for financial inclusion, the G20 leaders endorsed the 'G20 High-Level Principles for Digital Financial Inclusion' in Hangzhou in 2016. These Principles address, among other issues, the balancing of innovation and risks, the provision of an enabling and proportionate legal and regulatory framework, the establishment of responsible financial practices to protect consumers and the strengthening of digital and financial literacy and awareness.

In 2017, discussions within the G20 Global Partnership for Financial Inclusion (GPFI) and at the 8th Responsible Finance Forum in Berlin specifically targeted enabling and proportionate legal and regulatory frameworks and responsible financial practices to protect consumers in the context of digital financial inclusion. Being highly relevant in shaping further financial inclusion efforts undertaken by policy-makers, development organisations and the private sector alike, the GPFI decided to continue working on these relevant issues.

At the G20 Summit in Hamburg, the G20 leaders expressed their appreciation of, and strong support for, the considerable set of outcomes achieved under the GPFI agenda under the German Presidency this year. Noting the outcomes of the 8th Responsible Finance Forum, G20 Leaders 'encourage G20 and non-G20 countries to continue promoting digital financial services under the guidance of the G20 High-Level Principles for Digital Financial Inclusion'. Further, G20 Leaders 'support the 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', which encompasses new services, business models and financial service providers in the new age of digital financial services.

To put words into action, we commissioned this report to support political and technical discussions among policy-makers, private sector actors, technical experts, and others within and beyond the GPFI. Reporting on selected regulatory frameworks and implementing approaches on data privacy for digital financial inclusion, we aim to contribute to the development of minimum data protection standards for digital financial services for which public and private sector partners had voiced a need during the meetings in Berlin.

We are looking forward to fruitful discussions and meaningful progress.

Natascha Beinker

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

LIST OF ABBREVIATIONS

APEC	Asia-Pacific Economic Cooperation
BMZ	German Federal Ministry for Economic Cooperation and Development
CIC	Credit Information Commission
CISA	Credit Information System Act
DPA	Data Privacy Act
ECOA	Equal Credit Opportunity Act
EU	European Union
FCRA	Fair Credit Reporting Act
FTC	Federal Trade Commission
GDPR	General Data Protection Regulation
GIZ	Deutsche Gesellschaft für Internationale Zusammenarbeit GMbH
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
MSME	Micro, small and medium-sized enterprises
NGO	Non-governmental organisation
OAS	Organisation of American States
OECD	Organisation for Economic Cooperation and Development
PIA	Privacy impact assessment
PSD	Payment Services Directive
SCHUFA	Schutzgemeinschaft für allgemeine Kreditsicherung
UN	United Nations
USA	United States of America

This report was drafted by Dr Alexander Dix, Deputy Chair of the Board of the European Academy for Freedom of Information and Data Protection, supported by Judith Frickenstein and Konstantin Pagonas (both GIZ). Section 2 was drafted with the invaluable contributions of Dr Nicola Jentzsch, German Institute for Economic Research (DIW), Germany; Prof. Louis de Koker, La Trobe Law School, Australia; Marc Rotenberg, President and Executive Director of the Electronic Privacy Information Center, USA; David Watts, Adjunct Professor, Commissioner for Privacy and Data Protection for the State of Victoria, Australia; Dr Thilo Weichert, Deutsche Vereinigung für Datenschutz e. V., Germany. This section is a consolidation of the responses received.

1 | INTRODUCTION

'For any enterprise, confidence is the capital without which no effective work can be carried on.'

Albert Schweitzer, Nobel Lecture 1954

Expanding financial inclusion of the so far excluded and underserved has been an agreed goal of the international community for some time. The rapid expansion of digital technologies is a key instrument to attain this goal. FinTechs and InsurTechs are increasingly offering their services worldwide.

Creditors and insurers have a legitimate interest in evaluating the creditworthiness or insurability of their potential customers. **Responsible lending** includes measures to avoid over-indebtedness (over-borrowing). For these (among other) reasons personal information is collected and processed on an ever increasing scale not only from the data subject but from various other sources. Big data analysis can undoubtedly deliver important social benefits in the area of medical research.[1] Whether big data analysis of, for example, mobile phone metadata can be used effectively to evaluate the creditworthiness of a person may well be debated. For the purposes of this report it is assumed that big data analysis can in certain circumstances be useful for offering financial services.

Credit reports, credit scoring and consumer profiling as a prerequisite for agreeing on a loan or insurance cover[2] can open access to vital financial resources. But they can also have an exclusive effect when credit or insurance are denied as a result of the credit report or scoring. Even if credit is not denied altogether on the basis of a credit report it may lead to a higher interest rate, thereby de facto excluding customers who cannot afford this. Credit reports are required in some countries before access to employment or a profession is granted.[3] Thus, financial credit is often only an example for economic and social credit more generally. Scoring and profiling may therefore be decisive whether the individual's human right to an adequate standard of living is fulfilled.

This report builds on the G20 High-Level Principles (HLP) on Digital Financial Inclusion (2016).[4] The G20 governments have accepted that a balance has to be struck between innovation and risk (HLP 2) to achieve financial inclusion. In their view, the provision of an enabling and proportionate legal and regulatory framework (HLP 3), the responsible delivery of financial services at a cost affordable to customers and sustainable for providers (HLP 5) should be the common goal. The report examines selectively how global, regional and national legal frameworks balance the human right to privacy and data protection with (1) the human right to an adequate standard of living and (2) the goal for more effective financial inclusion of those people who have so far been excluded from access to financial resources. Some of these frameworks are promoting solutions to use innovative big data analytics in line with data privacy.

The remainder of this report is structured as follows: The first section introduces some basic concepts (Section 2), defining key terms. The main part of the report is dedicated to a comparative analysis of global standards for data privacy and of selected legal frameworks in the European Union (EU), the United States of America (USA) and the Philippines (Section 3). Finally, a catalogue of recommendations for possible steps to take in order to create a level playing field for both digital financial services and consumers worldwide (Section 4) is followed by a conclusion (Section 5).

1 Cf. UN Global Pulse, Big Data for Development: Challenges & Opportunities (2012), p. 20 et seq.; Ohm, Response, The Underwhelming Benefits of Big Data, U. PA. L. REV. ONLINE, https://www.pennlawreview.com/online/161-U-Pa-L-Rev-Online-339.pdf (seen on March 16, 2017)

2 In not all jurisdictions may insurers use credit reports. E.g. in New Zealand this is only allowed for insurance of a credit transaction.

3 For the situation in the US cf. Solove, Rotenberg and Schwartz, Information Privacy Law (2006), p. 702

4 G20 High-Level Principles for Digital Financial Inclusion, p. 3 (quoting the GPFI White Paper on Global Standard-Setting Bodies Financial Inclusion: The Evolving Landscape (2016)

2 | INTRODUCTION OF BASIC CONCEPTS

***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'.*[5]

There is as yet no globally accepted definition of the term 'privacy'. One of the first and still the most succinct and vivid definition of the term was given by Warren and Brandeis (1890) who spoke of the 'right to be let alone'.[6] This includes the physical right to keep out trespassers from one's private home[7]. Privacy has therefore been described as a passive or defensive right.[8] Although the right to privacy is derived in certain jurisdictions[9] from human dignity[10] and the right to protect one's personhood, privacy is a broader concept than that of intimacy or dignity. An invasion of privacy may therefore be seen without a person's intimacy or dignity being violated.

The aspect of autonomy (decisional privacy) with regard to the processing of personal information was taken up by the OECD in their Guidelines of 1980, revised in 2013, as well as by Asia-Pacific Economic Cooperation (APEC) in their Privacy Framework (2005). The latter describes the individual as being at risk of losing control over his or her personal information due to the fast development of information and communication technology which allows for the collection, storage of and access to (personal) information from anywhere in the world.

At the same time, 'privacy' is used to overlap with, or even as a synonym for, other terms such as 'information/data privacy' and 'data protection'. However, delineations to these terms are necessary. As was described in the Responsible Finance Forum Report on the recent Berlin Conference[11] (p. 7) the blacklisting of more than 400,000 Kenyans for minimal loans without any explanation or recourse cannot be seen primarily as a privacy problem but surely is a massive data protection issue.[12]

***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.*

This harmonised definition of information/data privacy, flexible enough to be implemented in different jurisdictions with and without legislation on this topic, is based on the OECD Guidelines. The fact that there may be statutory limits to this right (e.g. the legitimate interests of money lenders, credit reference agencies or governments) does not require or justify a more restrictive definition.

In the context of digital financial services (and other digital services), information privacy[13] should be restricted to the processing of data concerning natural persons (personal information). Most international instruments (e.g. the OECD Guidelines and the APEC Privacy Framework) do not address the handling of information concerning legal persons.

***Privacy-Enhancing Techniques** are techniques that minimise or eliminate the collection of personal data.*[14]

5 Report by the Special Rapporteur on the Right to Privacy to the UN Human Rights Council (A/HRC/23/40)

6 Warren and Brandeis, The Right to Privacy, Harvard Law Review 1890, 193 et seq.

7 In the case of Warren and Brandeis, media photographers

8 Cf. Docksey, Four Fundamental Rights: finding the balance, International Data Privacy Law 2016, 195 et seq.

9 e.g. in Germany the 'right to informational self-determination'

10 CF. also Art. 11 of the American Convention on Human Rights (1969)

11 https://responsiblefinanceforum.org/publications/key-takeaways-eighth-responsible-finance-forum/

12 If someone applies for a loan he or she will have to accept that data on his or her solvency may be collected and shared. There is no legitimate expectation 'to be let alone' here. However, if a debtor is put on a blacklist without being told in advance and without any possibility to have the list corrected (in cases of erroneous identification) or updated once the debt has been paid then this is an unacceptable loss of control which the data subject should have over his or her data.

13 The Indian Supreme Court in Puttaswamy v. Union of India (p. 246 et seq.) speaks of 'informational privacy'.

14 Rotenberg, 1993

This concept, as well as the corresponding concept of **privacy by design**, are important in this context since they support and encourage the preventative integration of privacy principles at the design stage, instead of enforcing privacy regulations after they have been violated.[15] It has now been integrated in the EU General Data Protection Regulation (Art. 25).

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

Data protection is a more novel concept and largely (in Europe in particular) used synonymously with **->Information/Data Privacy**. At least, there is a certain overlap between data privacy and data protection.

Some active elements (e.g. the subject's right of access) are already to be found in the OECD Privacy Guidelines. Further active rights give the data subject the option to intervene in the processing of his or her data.[16]

Although a number of national data protection and privacy laws are based on the OECD Guidelines, there is at least one important exception: The European Union has gone beyond this minimum standard by adopting the Data Protection Directive of 1995 and more recently the General Data Protection Regulation (GDPR), which will come into force in May 2018. Since the GDPR contains adequacy rules restricting the export of personal data to non-European countries with an essentially equivalent level of protection the GDPR will have a global impact. Already a number of non-European countries and supranational organisations[17] have adopted European-style laws to gain adequacy status under European law in order to allow for the transborder processing of European personal data. Therefore FinTechs, InsurTechs and other stakeholders in the financial sector would be well advised to adopt the more advanced concepts and regulatory scheme of the GDPR, e.g. by means of self-regulation or binding corporate rules.

The GDPR – in comparison with the OECD Guidelines – provides for more detailed and novel provisions concerning the design of IT systems ('privacy by design') and more far reaching rights of the data subject.

***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.*

The concept of personal data is of key importance for the scope of data protection and information privacy laws. These laws are only applicable to the processing of personal data. However, the term 'personal data' is to be understood broadly.

Both the OECD Guidelines, the EU GDPR and the African Union Convention on Cybersecurity and Personal Data Protection[18] all define personal data as including information relating to an identifiable individual. This includes 'taking into account the ability to combine different categories of information to identify a person...'[19] which is particularly important in the context of **->Big Data**. The Council of Europe also includes in the concept of personal data any information used to single out people from data sets, to take decisions affecting them on the basis of group profiling information.[20]

The GDPR further elaborates on who is identifiable:

'an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person' (Art. 4 No.1).

Therefore, in the discussion on measures such as data minimisation[21] it should be kept in mind that this does not mean to abstain from collecting and processing personal data altogether but to sever the reference to individual persons.

15 The concept of Privacy-Enhancing Technologies and Privacy by Design was developed by Cavoukian and Borking in 1995, cf. Hustinx, Privacy by design: delivering the promises (2010), https://link.springer.com/content/pdf/10.1007%2Fs12394-010-0061-z.pdf (as seen on 31 August 2017)

16 Docksey, International Data Privacy Law 2016, 195 et seq.

17 The African Union Convention on Cybersecurity and Personal Data Protection (2014) in its Chapter II contains a number of provisions closely modelled on the European legal framework.

18 This Convention has not yet entered into force, see below Section 3

19 G20 High-Level Principles for Digital Financial Inclusion, 16

20 Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data, III a), adopted on 23/1/2017 by the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data

21 cf. p. 13 of the RFF Report Berlin: https://responsiblefinanceforum.org/publications/key-takeaways-eighth-responsible-finance-forum/

More generally, concepts of de-personalisation (anonymisation and pseudonymisation[22]) become of crucial importance as methods to ensure effective data and privacy protection. Thus, whenever it is argued that personal data are necessary (i.e. to identify and prevent discriminatory effects of certain services) it should first be ascertained whether this legitimate aim can be achieved by processing de-personalised data. At the same time the term 'personal data/information' is not to be understood in a static way. The risk of identifiability has to be re-assessed from time to time since it is likely to change due to technological changes or developments in the area of **->Big Data**.

***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[23] 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.*

The category was first introduced internationally by the Council of Europe in its Convention 108 (Art. 6)[24] and later broadened and integrated in EU law.

The African Union Convention on Cybersecurity and Personal Data Protection extends this concept to data revealing regional origin and parental filiation.[25] The OECD Guidelines – without defining the category of sensitive data – refer to the sensitivity of personal information in the context of assessing the legality of transborder data flows (No. 18).

*The term **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.[26]*

The term 'big data' is also used to describe advanced software technology to collect and extract from a great volume and variety of data new and predictive knowledge for decision-making purposes regarding individuals and groups. The definition of big data therefore encompasses big data analytics.[27]

*The term **Big Data Analytics** is used to identify computational technologies that analyse large amounts of data to uncover hidden patterns, trends and correlations.*

Big data does not necessarily contain personal data; only if and as soon as it does, privacy and data protection laws come into play.

In a big data context, the concept of sensitive data is particularly relevant since information relating to racial or ethnic origin, political opinions, trade union membership, religious or other beliefs, health or sexual life may be revealed by personal data further processed, or combined with other data using big data analytics.

A special form of big data developing worldwide after the global financial crisis is called 'regulatory big data' in which an institution (RegTech) provides its bulk underlying granular data to regulators for their regulatory, risk assessment, and stress testing efforts.[28] However, these statistical data will not normally refer to individual persons.

Finally, big data and big data analytics may increase the risk of identifiability of data sets, which initially are non-personal.[29] E.g. the more granular statistical information becomes, the greater is the likelihood of singling out individual persons. This is particularly relevant in digital financial services, e.g. in the case of scoring. But this does not mean that in a world of big data anonymisation or pseudonymisation of data is impossible. On the contrary, methods of anonymising or pseudonymising data are likely to become important tools to facilitate big data applications involving raw data which are personal at the point of collection.

***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 digitised format.*

22 Pseudonymisation is defined in Art. 4 No. 5 GDPR as follows: '"pseudonymisation" means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person'. There are some inconsistencies in the international discussion of these terms. The UNDG in its Guidance Note 'Big Data for Achievement of the 2030 Agenda: Data Privacy, Ethics and Protection', p. 11, considers pseudonymisation to be one method of anonymisation.

23 Council of Europe in its Convention 108 (Art. 9 para. 1).

24 Cf. also No. 5 (Principle of Non-discrimination) of the UN Guidelines of 1990

25 This Convention has not yet entered into force, see below Section 3.

26 UN Global Pulse, Big data for development: challenges and opportunities (May 2012)

27 Cf. Council of Europe, Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data, III a)

28 Van Steen, Regulatory Big Data: Regulator Goals and Global Initiatives (May 2015); Heath/Bese Goksu, G 20 Data Gaps Intiative II: Meeting the Policy Challenge (March 2016)

29 Cf. the definition of identifiability in the G20 High-Level Principles for Digital Financial Inclusion, see above note 12

Quite apart from privacy and data protection laws, companies and state agencies have a vital interest in securing their business and official secrets and to protect critical infrastructures. With regard to the handling of personal data, most data protection laws contain data security requirements, which mostly coincide with the security requirements applying to non-personal data as well. Therefore, the question of whether the processed data are **->Personal Data** or not is irrelevant for the need to take security measures. The OECD Guidelines contain the security safeguards principle (**->Information Privacy**) as a minimum standard. The European GDPR (Art. 32) in addition requires controllers and processors to 'implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

» the pseudonymisation and encryption of personal data;

» the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

» the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

» a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

In assessing the appropriate level of security, account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.'

***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 disuse 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.*

The importance of securing data processed in an online environment particularly in the financial sector has been highlighted by the attack on the SWIFT system via the Bangladesh Central Bank causing damage worth as much as USD 81 million.

The African Union Convention on Cybersecurity and Personal Data Protection[30] contains detailed provisions on cybersecurity without specifically defining it. Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive) provides an interesting definition in this context: '"security of network and information systems" means the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems' (Art. 4 No. 2).

By November 2018, EU Member States will have to decide whether financial services such as the SWIFT system qualify as essential (critical) services, the operators of which have to provide for specific security measures under the NIS Directive.

If personal data are processed, the obligations to provide for cybersecurity follow from data protection laws to the same extent as for data security.

The remainder of this paper focuses on **the collection and processing of personal data to assess the creditworthiness or insurability of potential customers (credit scoring)**.

Finally, this paper does not purport to measure the degree of de facto compliance with the law in Europe, the USA or the Philippines. This would require extensive additional research. Although there is always a gap between the letter of the law and how it is applied in practice there is a tendency in the USA and a future potential in Europe towards harsh enforcement by the supervisory authorities to close this gap.[31]

30 This Convention has not yet entered into force, see below Section 3.

31 There is no information available about the factual situation in the Philippines where the relevant legislation only came into force in 2016.

3 | OVERVIEW AND ASSESSMENT OF EXISTING REGULATORY FRAMEWORKS

Having introduced the basic concepts, we will now proceed to have a closer look at existing regulations on the global, regional and national level. As will be seen, the frameworks differ strongly with regards to their content, scope and liability. Table 1 provides a brief overview of the regulations reviewed.

TABLE 1: OVERVIEW OF REGULATIONS

YEAR	BODY	REGULATION	CONTENT (very compressed, not exhaustive)	MONITORING/ENFORCEMENT
GLOBAL				
1948	UN	Universal Declaration of Human Rights	Right of everyone to an adequate standard of living	Hard law', monitored by UN Human Rights Committee (no sanctions provided) and its Special Rapporteur on the right to privacy
1966	UN	International Covenant on Civil and Political Rights	Right to privacy	
1966	UN	International Covenant on Economic, Social and Cultural Rights	Right to protection from unlawful interference with privacy	
1990	UN	Guidelines for the Regulation of Computerised Personal Data Files	• Lawful and fair collection and usage of information • Accurate compilation of files • Purpose specification of personal data collections • Right to know whether information is processed • Non-discrimination • File security • Transborder data flows	'Soft law'
2013 2014 2016	UN	Resolutions on the Right to Privacy in the Digital Age	• Procedures, practices and legislation regarding surveillance by intelligence agencies must be reviewed • Business enterprises must protect and ensure the consumer's right to privacy in the digital age • Information to users about the collection, use, sharing and retention of their data that may affect their right to privacy • Establishment of transparency policies	'Soft law'
1990/ 2013	OECD	Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data	• Collection limitation • Data quality • Purpose specification • Use limitation • Security safeguards • Openness • Individual participation • Accountability	Soft law', monitored by the Global Privacy Enforcement Network (which also facilitates the enforcement of regional frameworks)
2007	OECD	Recommendation on Cross-border Cooperation in the Enforcement of Laws Protecting Privacy	Recommendations to improve domestic frameworks for privacy law enforcement	
2008	ISO/ IEC	Financial Services – Privacy Impact Assessment Standard	• Recognises that a privacy impact assessment (PIA) is a tool to identify and mitigate privacy issues and risks • Describes, defines and provides guidance on PIAs	'Soft law'
2011	ISO/ IEC	ISO 22307:2008	• Consent and choice • Purpose legitimacy • Data minimisation • Privacy compliance	

YEAR	BODY	REGULATION	CONTENT (very compressed, not exhaustive)	MONITORING/ENFORCEMENT
REGIONAL				
1953	Council of Europe	European Convention on Human Rights	Right to respect for private and family life	'Hard law' enforced by the European Court of Human Rights
1981	Council of Europe	European Convention No. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data	• Fair and lawful collection and processing • Purpose limitation • Extent and duration of storage adequate in relation to purpose • Accuracy • Conditions for transborder data flow	'Hard law' but no formal enforcement on the regional level
1995	EU	Data Protection Directive (95/46/EC)	• Lawfulness, fairness, transparency • Purpose limitation • Data minimisation • Accuracy • Storage limitation, integrity, confidentiality	'Hard law' enforced by data protection authorities of Member States and the European Court of Justice (ECJ)
2016	EU	General Data Protection Regulation ((EU) 2016/679)	Reiterating the rights and principles of Directive 95/46/EC and providing in addition for: • privacy by design, • accountability, • portability, • right to be forgotten	'Hard law' enforced by data protection authorities of Member States, the European Data Protection Board and the ECJ
2000	EU	European Charter of Fundamental Rights	Right to respect for private and family life	'Hard law' enforced by the ECJ
2002	EU	Directive 2002/58/EC on privacy and electronic communications (ePrivacy Directive)	• Security and confidentiality of communications • Restrictions on processing of traffic and location data • Regulation of telemarketing	'Hard law' enforced by data protection authorities of Member States and the ECJ
2007/ 2015	EU	EU Payment Services Directive	FinTechs have right of access to customers' bank accounts with their consent	'Hard law' enforced by the ECJ
2008	EU	Consumer Credit Directive	• Restricting the collection of consumer data by creditors • Alternative dispute resolution	'Hard law' enforced by the ECJ
1996	OAS	American Convention on Human Rights	Right to Privacy	'Hard law' monitored by the Inter-American Human Rights Commission

YEAR	BODY	REGULATION	CONTENT (very compressed, not exhaustive)	MONITORING/ENFORCEMENT
NATIONAL				
1970	USA	Fair Credit Reporting Act	Restricts the disclosure (not collection) of personal credit information by credit reporting agencies	'Hard law', enforced by the Federal Trade Commission
1974	USA	Equal Credit Opportunity Act (ECOA)	Restrictions on discrimination not applicable to credit reporting agencies	Enforced by US courts
1974	USA	Privacy Act	Covers only the public sector (federal agencies)	Enforced by US courts
2008	Philippines	Credit Information System Act	Provides for central registry processing credit information	'Hard law', monitored by the Credit Information Commission
2012	Philippines	Data Privacy Act	• Principles and rights following the European model • Applicable to financial institutions except the Credit Information System	Monitored by the National Privacy Commission

3.1 Global Legal Frameworks

The following sections deal with standards and frameworks that have been adopted by international organisations and – theoretically – have a global sphere of application. There is a huge variety of international data protection frameworks. For reasons of scope, this report focuses on frameworks provided by the United Nations (UN), the Organisation for Economic Co-operation and Development (OECD) and the International Organization for Standardization (ISO). The UN and OECD were the first global agencies to address these issues. ISO was chosen as an example of one of the most frequently used non-governmental standards.

3.1.1 United Nations

The international community, represented by the UN, has agreed on several documents, which provide the backdrop against which data protection legislation must be evaluated. In Art. 11 of the International Covenant on Economic, Social and Cultural Rights 'the **right of everyone to an adequate standard of living** for himself and his family, including adequate food, clothing and housing, and to the continuous improvement of living conditions' is recognised. This human right is of particular importance in the context of financial inclusion in countries with high levels of poverty. The **right to privacy** is guaranteed in Art. 12 of the Universal Declaration of Human Rights as well as Art. 17 of the International Covenant on Civil and Political Rights according to which no one shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence. This is linked with the **right to protection** of the law against such interference. The States Parties to this Covenant have agreed to take appropriate steps to ensure the realisation of these rights, recognising to this effect the essential importance of international cooperation based on free consent. The Universal Declaration and both Covenants stress the **principle of non-discrimination**. The two International Covenants have been ratified by most Member States of the UN and together with the Universal Declaration of Human Rights they form the International Bill of Rights. The Covenants are monitored by the UN Human Rights Committee which receives and reviews reports from all signatory states. The International Covenants are monitored by the UN Human Rights Council which receives regular reports from national governments and which in 2015 appointed a Special Rapporteur on the right to privacy.

The UN General Assembly has also adopted more specific Guidelines for the regulation of computerised personal data files (1990).[32] In the wake of Edward Snowden's revelations on mass surveillance, the General Assembly adopted three resolutions on the **Right to Privacy in the Digital Age** (2013, 2014 and 2016).[33] Whereas the first two resolutions primarily addressed surveillance by intelligence agencies, the third resolution is more **relevant for providers of digital financial services**. For the first time, it calls 'upon business enterprises to meet their responsibility to respect human rights in accordance with the Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework,[34] including the right to privacy in the digital age and to inform users about the collection, use, sharing and retention of their data that may affect their right to privacy and to establish transparency policies, as appropriate.'

3.1.2 Organisation for Economic Cooperation and Development

Already in 1980, the OECD Council adopted **Guidelines** governing the Protection of Privacy and Transborder Flows of Personal Data[35], which were revised in 2013.[36] The Guidelines 'apply to personal data, whether in the public or private sectors, which, because of the manner in which they are processed, or because of their nature or the context in which they are used, pose a risk to privacy and individual liberties.'[37] They can be qualified as 'soft law', since they are based on a Council Recommendation and not legally binding for OECD Member States.

Despite the use of the term 'privacy', the Guidelines deal more specifically with 'data protection' (as defined above in Section 2). They contain eight principles to be observed when processing personal data:

» collection limitation,
» data quality,
» purpose specification,

32 Resolution 45/96 of 14 December 1990

33 Resolutions 68/167 of 18 December 2013, 69/166 of 18 December 2014 and http://undocs.org/A/C.3/71/L.39/Rev.1 of 19 December 2016

34 This Framework was adopted by the UN Human Rights Council in 2008 and monitored by a Special Representative of the UN Secretary General, see http://www.business-humanrights.org/SpecialRepPortal/Home

35 At the same time the Council of Europe finalised its Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data. This Convention is open for accession to non-European countries; alongside most members of the Council of Europe Mauritius, Senegal and Uruguay have ratified the Convention.

36 The OECD Privacy Framework (2013)

37 Para. 2 of the Guidelines

» use limitation,
» security safeguards,
» openness,
» individual participation, and
» accountability.[38]

In order to implement accountability, data controllers (including banks and insurance companies) should have a **privacy management programme** in place.[39] Although the Guidelines themselves do not form binding international law, OECD Member States have consistently worked to increase the degree of cooperation. The amended OECD Guidelines also provide for transborder cooperation between supervisory authorities enforcing national data protection laws. In 2007, the Council adopted a Recommendation on Cross-border Cooperation in the Enforcement of Laws Protecting Privacy, the implementation of which was evaluated in a report in 2011.[40] Since 2010 there has been a Global Privacy Enforcement Network using a platform for informal cooperation of national supervisory authorities provided by the OECD Secretariat.[41]

3.1.3 International Organization for Standardization

The ISO is a non-governmental international organisation of 165 national standards bodies which develops and publishes internationally agreed standards.[42] Its objective is the 'use of ISO standards everywhere', but it has no formal powers of enforcement, relying on stakeholders and partners such as the national standards bodies and industry. ISO together with the International Electrotechnical Commission (IEC) has adopted two standards relevant to digital financial services. One is the Privacy Framework Standard ISO/IEC 29100:2011 which not only spells out in greater detail the eight privacy principles contained in the OECD Guidelines (see above), but adds four important additional principles:

» consent and choice,
» purpose legitimacy,
» data minimisation, and
» privacy compliance.

38 Paras. 7–14 of the Guidelines

39 Para. 15 of the Guidelines

40 OECD, The OECD Privacy Framework (2013), p. 137 et seq.

41 www.privacyenforcement.net (seen on 7 April 2017). This follows the example of the International Consumer Protection Enforcement Network (ICPEN), cf. www.icpen.org. (seen on 9 April 2017)

42 Cf. https://www.iso.org/files/live/sites/isoorg/files/archive/pdf/en/iso_strategy_2016-2020.pdf (seen on 9 April 2017)

The second international standard adopted is ISO 22307:2008 on **Financial services – Privacy Impact Assessment**. The standard does not require a privacy impact assessment (PIA) by itself but offers guidance where an institution wants (or is obliged, see below p. 19) to use this 'important financial services and banking management tool'. A PIA is to be distinguished from a privacy compliance audit. The latter is primarily concerned with meeting the legal requirements, whereas a 'PIA is intended to investigate further in order to identify ways to safeguard privacy optimally'.[43]

3.1.4 Conclusion

The global picture in terms of information privacy shows some legal frameworks which may be considered as 'hard law' such as the International Covenants on Civil and Political Rights and on Economic, Social and Cultural Rights. They are monitored by the UN Human Rights Council which cannot, however, impose any formal sanctions in the case of violations. Increasingly the UN is adopting soft law instruments, in particular General Assembly resolutions, addressing privacy in the digital age. OECD and ISO are in turn dealing with privacy issues more specifically with issues of data protection, transborder data flows and privacy impact assessments thereby contributing to the emergence of an international legal framework on privacy. So far no legally binding international convention exists on privacy and data protection in the financial sector.

3.2 Regional Legal Frameworks

In comparison to the global level there are regulatory frameworks in various regions of the world which provide more granular rules on data protection, direct enforceability in the courts, transborder data flows and specific regulation of the credit industry. These can be found in Europe, America, Africa and Asia-Pacific.

3.2.1 Council of Europe

The Member States of the Council of Europe in 1950 adopted the European Convention on Human Rights which contains in Art. 8 a right to respect for private and family life.[44] This Convention is enforced by the European Court of Human Rights as well as by the national courts of Member States. In addition, the Council of Europe in 1981

43 https://www.iso.org/standard/40897.html (last seen on 7 March 2017)

44 47 European States have ratified the Convention, most of them not members of the EU.

adopted Convention No. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data. This instrument can be seen as a precursor of later Directives and Regulations adopted by the EU (see below, 3.2.4). Convention No. 108 contains principles concerning fair and lawful collection and processing of personal data, purpose limitation, adequate extent and duration of storage in relation to purpose accuracy and conditions for transborder data flow.

3.2.2 European Union

The EU is a regional supranational organisation to which the Member States have transferred certain regulatory powers. As a consequence the EU may adopt certain types of so-called secondary legislation. Whereas Directives by and large have to be transposed into national law in order to take effect, Regulations are directly applicable by the courts throughout the Union. In cases of conflict, the European Court of Justice[45] has the final say.

Data privacy framework

Since 1995 the EU has had a general legal framework for data protection, Directive 95/46/EC, which obliges the Member States to harmonise their national laws in order to achieve a high uniform level of protection and to facilitate the transborder flow of personal data. This Directive will be replaced in May 2018 with the GDPR ((EU) 2016/679) which will be directly applicable throughout the Union. The following analysis is based on the GDPR as the future framework for Europe. The Regulation covers the entire private sector as well as large parts of the public sector (except law enforcement). The GDPR has its primary basis in Art. 7 and 8 of the European Charter of Fundamental Rights which guarantee the right to privacy and the protection of personal data.

The GDPR principles for processing personal data in Europe are:

» lawfulness, fairness and transparency,
» purpose limitation,
» data minimisation,
» accuracy,
» storage limitation,
» integrity and confidentiality,
» accountability[46],
» more rights for the data subject,
» regulation of transborder data flow, and
» enhanced enforcement.

45 Not to be confused with the European Court of Human Rights discussed at 3.2.1, above.

46 Art. 5 GDPR

The following paragraphs will elaborate on these principles.

Lawfulness, fairness and transparency: With regard to financial services, the legal basis for the collection and processing of personal data by the bank (or financial service provider) is **the customer's informed consent** which is normally given when entering into a contractual relationship.[47] Processing of personal data can also be legitimised if it is necessary for the purposes of the **legitimate interests** pursued by the controller or a third party, except where such interests are overridden by the interests and fundamental rights and freedoms of the data subject which require protection of personal data.[48]

When collecting information, e.g. about the financial situation and creditworthiness, from the data subject (customer) directly, the provider must proceed in a completely transparent fashion. Inter alia, the provider has to provide information about his or her identity, the purposes and legal basis of the processing for which the personal data are intended, and at least the categories of possible recipients to the data subject.[49] If the collection of data is based on legitimate interests, the customer must be told what these interests are. A general reference to 'legitimate interests' will not suffice. Therefore the Lenddo Privacy Policy[50] is most likely not in line with EU law when it merely states that the information collected from a customer will be used inter alia 'for other legitimate business purposes.' If the customer gives his consent on such vague information, his consent will not be deemed valid under EU law.[51]

If the bank or insurance collects additional information about the customer from third parties, e.g. credit reference agencies, similar duties to inform apply.[52] The credit reference agencies themselves can rely on the legal basis of a 'legitimate interest' to the extent to which specific personal data are necessary and relevant to ascertain the creditworthiness or insurability of the customer.[53]

Consent can only justify the processing of personal data if it is freely given.[54] This is not the case when the provision of a service (e.g. access to financial resources) is conditional

47 Art. 6 (1) (a), (b) GDPR

48 Art. 6 (1) (f) GDPR

49 Art. 13 GDPR

50 See Annex 1 of the Draft Report 'Decision-making in the financial services sector – Understanding Classification Algorithms'. Lenddo offers scoring and identity verification technology and since 2015 has opened its technologies for third parties, such as banks, lending institutions, utilities companies and credit cards worldwide 'to reduce risk, increase portfolio size, improve customer service and verify applicants.' (www.lenddo.com/about.html, as seen on 25 August 2017)

51 Cf. Art. 7 (2) GDPR

52 Art. 14 GDPR

53 Art. 6 (1) (f) GDPR

54 Art. 7 (1) GDPR

on consent to the processing of personal data that is not necessary for the provision of these services.[55] This limits considerably the collection and processing of personal data by financial service providers and takes into account the specific **economic imbalance** which often exists between partners negotiating a credit agreement. For example, it would be illegal in Europe to offer a mobile banking account or microcredit only to customers who agree to have all the data, photos, messages, etc. stored on their mobile phones analysed to check their creditworthiness.[56]

The GDPR also **specifically restricts the processing of special categories of (sensitive) personal data** such as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric data, data concerning health or a person's sex life or sexual identity.[57] Although there are exceptions to this rule such as explicit consent by the data subject it is more than doubtful whether the collection of such data would pass the test of Art. 7 (4) since it is hardly conceivable that such data could be considered to be necessary for a loan agreement or insurance cover. Unlike the legal situation in the USA (see below, Section 3.3.1), data offered by data brokers, e.g. on AIDS and HIV infection or dementia sufferers,[58] could not legally be used in the EU for providing financial services. The situation may be different in the case of health or life insurance.[59] Sex is not a special category of personal data under EU data protection law. But anti-discrimination laws forbid the turning down of applications for credit or insurance on the grounds of sex.[60]

Additional restrictions and obligations apply when **automated decision-making including profiling** takes place. This is particularly relevant for credit scoring decisions. "Profiling" means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements."[61] Using algorithms to determine the creditworthiness or insurability of a person in most cases will be seen as automated decision-making or more specifically profiling under the GDPR. Therefore the bank or insurance company using such algorithms would be obliged to inform the data subject (customer) about the fact that such algorithms are used and provide 'meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.'[62] Although **trade secrets** linked to the algorithms must be protected[63] the EU Regulation still takes the view that this does not prevent meaningful information about the logic involved to be given to the data subject. This includes the factors/information which are fed into the algorithm as well as their relative weight in the scoring process.

Accuracy: With regard to the question of which factors may be used as input for the algorithm to calculate the creditworthiness or insurability of a person, e.g. German law at present contains very specific provisions which are not common in other EU Member States. Personal information may only be used to assess the probability that the (potential) debtor will be able to honour his obligations (creditworthiness) if it can be proven 'on the basis of scientifically recognised mathematical–statistical procedures that this information is relevant for determining the creditworthiness' of the debtor.[64] Although this provision has not been integrated in this detailed fashion in the GDPR it could be argued that the more general provisions of the Regulation justify the same requirement. The same applies to the practice of redlining (exclusion of consumers exclusively on the grounds of their addresses). This is considered to be illegal by supervisory authorities in Germany[65], but in order to maintain this state of the law or extend it to the entire EU one would have to argue (and the supervisory authorities and courts would have to support the view) that addresses alone are not adequate and relevant to what is necessary for the purpose of a credit or insurance agreement.

Another example of personal data which have been used as input for the scoring algorithm is the fact that the consumer has gathered information on interest rates from several banks and providers of financial services in order to get the best deal. This has been used in the past by the biggest German credit reference agency SCHUFA (Schutzgemeinschaft für allgemeine Kreditsicherung) as a factor which led to

55 Art. 7 (4) GDPR

56 This practice was referred to by Xavier Faz (CGAP) as being used in African markets by mobile operators using the M-Shwari Banking Service.

57 Art. 9 Abs. 1 GDPR

58 Cf. Annex 3 of the Draft Report 'Decision-making in the financial services sector – Understanding Classification Algorithms'

59 However, in the EU no such lists from data brokers are at present available.

60 Cf. Directive 2004/113/EC implementing the principle of equal treatment between men and women in the access to and supply of goods and services, OJ L 373/37

61 Art. 4 (4) GDPR

62 Art. 13 (2) (f) GDPR

63 This would apply to the precise algorithm formula used.

64 § 28b Nr. 1 Federal Data Protection Act (BDSG), as from May 2018 § 31 para. 1 No. 1 BDSG (new)

65 Cf. Berliner Beauftragter für Datenschutz und Informationsfreiheit, Jahresbericht 2009, 34. Even if addresses are used legally as one criterion among others, consumers have to be informed beforehand, cf. § 28b Nr. 4 BDSG, as from May 2018 § 31 para. 1 No. 4 BDSG (new). Whether rating on the basis of postal codes (called 'territorial rating system' (TRS) by insurers) would be legal under German or European law remains doubtful. This has been a contentious issue in the USA for a long time and was outlawed for car insurance after a referendum in California in 1988 (cf. https://www.theguardian.com/commentisfree/2014/jul/21/auto-insurance-red-lining-poor-urban-drivers, seen on 9 April 2017).

deteriorating credit scores (on the assumption that the consumer concerned lacked financial resources). This was stopped after the supervisory authorities stated that this practice was illegal.

If automated decision-making is used by the credit industry the (potential) customer has the right to obtain **human intervention**[66] on the part of the controller and to contest the decision. The replacement of human interaction and decision-making with 'several mathematical models running in parallel … making credit decisions in less than 10 seconds' (quoted from the website of ZestFinance)[67] would subject the person looking for credit to automated decision-making without any possibility of human intervention or objection. Automated decision-making may not be based on special categories of data such as data concerning health or racial origin unless either the data subject has explicitly consented or there is a reason of substantial public interest under Union or Member State law.[68] An example would be the processing of sensitive personal data for humanitarian purposes, including for monitoring epidemics and their spread or in situations of humanitarian emergencies, in particular in situations of natural and man-made disasters.[69]

Credit reference agencies in Europe can use personal data from public records if there is a legal basis for this (e.g. the debtors register (*Schuldnerverzeichnis*) in Germany). However, the scraping of public records by credit reference agencies is not as common as in the USA where the collection of personal data for business purposes is largely unregulated (see below).

Purpose limitation, data minimisation and storage limitation: The concept of **big data** is based on the assumption that 'raising the sample size of the training-dataset, extending the number of features tested and increasing the quality of the data will all lead to a model that is better at weeding out "bad" customers and able to enhance the profitability of any product sold.'[70] This assumption is being challenged by authors who take the view that the quality of judgments does not necessarily improve with the quantity and quality of data collected to inform these judgments.[71] **Statistical correlations do not necessarily show causal links**. Behind this debate lies the more fundamental question of whether algorithms do in fact lead to correct results when assessing the creditworthiness or insurability of a person.

66 Art. 22 (3) GDPR

67 Cf. Draft Report on Decision-making in the financial services sector – Understanding Classification Algorithms, p. 12

68 Art. 22 (4), Art. 9 (2)(a, g) GDPR

69 Recital 46 of the GDPR

70 Cf. Draft Report on Decision-making in the financial services sector – Understanding Classification Algorithms, p. 12

71 Art. 22 (4), Art. 9 (2)(a, g) GDPR

Linked to this is the vital question of whose burden of proof it is to show that either the algorithm delivers correct results or that it does not.

However, the principles of purpose limitation, data minimisation and storage limitation[72] are limiting the use of **big data** only as long as **big *personal* data** is concerned. As soon as the data are anonymised they may be used in big data applications without violating EU law. **Anonymisation**, pseudonymisation[73] and encryption are all considered by the GDPR as good practice when processing personal data. Whereas pseudonymous and encrypted data are still personal data covered by the GDPR, anonymous data are not. In any event financial service providers should be completely transparent vis-à-vis the customer when engaging in big data analysis even if they only use anonymous data. A positive example from another industry is the practice by Deutsche Telekom which not only informs its mobile network customers about big data analytics but also – beyond the legal obligations – allows for an opt-out.[74] Since doubts have been raised as to whether anonymisation is at all feasible in a big data environment it is probably more apt to use the term 'robust de-identification' describing a process of constant monitoring and reducing the risk of identification.[75] The European Parliament has recently pointed out that even the processing of non-personal data might impact on individuals' private lives and other rights and freedoms leading to a stigmatisation of whole groups of the population.[76]

De-identification is even more important if FinTechs or InsurTechs plan to process **social media** data. They must take into account what their customers may think if they learn that their social media data are being used to assess their creditworthiness.[77] Not all users of social media have the same level of awareness about their privacy settings.[78] The use of social media data – which often includes sensitive data referring to health and political opinions – may have discriminatory and exclusive effects on data subjects. An example for these effects is the Chinese planning outline for a social

72 Art. 5 (1) (b, c and e) GDPR

73 Defined in Art. 4 Nr. 5 GDPR as 'the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person'.

74 See below p. 38

75 Cf. Lagos/Polonetsky, Public vs Nonpublic Data: The Benefits of Administrative Controls, 66 Stan. L. Rev. Online 103 (2013); see also Art. 29-Working Party, Opinion 5/2014 on Anonymisation Techniques of April 2014 (WP 216)

76 European Parliament, Resolution of 14 March 2017 on fundamental rights implications of big data: privacy, data protection, non-discrimination, security and law enforcement (2016/2225(INI)), para. 5

77 Joint Committee of the European Supervisory Authorities, Discussion Paper on the Use of Big Data by Financial Institutions, JC 2016 86, para. 25

78 In Germany the credit reference agency SCHUFA shelved plans to cooperate with Facebook when they became public.

credit system which provides for a comprehensive system of 'credit scores' allocated to each citizen ('citizen score') which takes into account online behaviour including political comments posted by the data subject or any of his or her friends and thereby determining opportunities for life beyond the financial sector.[79]

Anonymisation is not only of key importance with regard to big data but also to data exports to non-European countries without adequate levels of data protection.[80]

Integrity and confidentiality: Since providers of digital financial services rely on **telecommunications** alongside the GDPR with its general obligation to provide for technical and organisational measures for data security they also have to take into account the specific Directive 2002/58/EC on privacy and electronic communications (ePrivacy Directive). This Directive obliges Member States to 'ensure the **confidentiality of communications** and the related traffic data by means of a public communications network and publicly available communications services'.[81] 'Traffic data relating to subscribers and users[82] processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication …'[83] The latter provision limits the use of personal traffic data for big data applications beyond the requirements of general EU data protection law. It is particularly important for the provision of financial access by mobile network operators. The recording of content data may, however, be required by national law for evidential purposes if financial transactions are made via telecommunications.

Accountability: Financial institutions – as all controllers of personal data – will be obliged under the GDPR prior to the processing to carry out a **data protection impact assessment** *'where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons…'*[84] In view of the use of new technologies providers of digital financial services (FinTechs, InsurTechs) will regularly obliged accordingly. In order to fulfil this obligation they could rely on ISO standard 22307:2008.

79 https://chinacopyrightandmedia.wordpress.com/2014/06/14/planning-outline-for-the-construction-of-a-social-credit-system-2014-2020/

80 Cf. Privacy Bridges: EU and US Privacy Experts in Search for Transatlantic Privacy Solutions (2015), esp. Privacy Bridge 6 (Best practices for de-identification of personal data)

81 Art. 5 (1) Directive 2002/58

82 This Directive – unlike the GDPR – covers data of natural as well as legal persons.

83 Art. 6 (1) Directive 2002/58

84 Art. 35 (1) GDPR

Furthermore financial institutions are obliged to implement 'privacy by design and by default'[85] which could 'incentivise businesses to innovate and develop' not only 'new ideas, methods, and technologies for security and protection of personal data'[86] but also new business models.

More rights for the data subject: The GDPR considerably strengthens the rights of data subjects beyond the already existing rights of access, correction and deletion. A new right to data portability is created which gives the customer a right to receive his or her data in a machine-readable format in order to transfer them to another bank or provider. This may facilitate the market access of FinTechs in addition to new harmonised rules to be adopted by EU Member States under the second Payment Services Directive (see II 2 b).[87]

Regulation of transborder data flows: *EU data protection law since 1995 allows for the* **export of personal data** to jurisdictions outside the EU only on condition that either the jurisdiction where the data are to be exported to have an adequate level of data protection[88] in place (to be determined by the European Commission[89]) or other instruments such as standard contractual clauses or binding corporate rules make up for the lacking legal framework in the importing country. This factor may lead to a **certain tendency to globalise European standards** for data protection. At the time of writing about half of the UN Member States have privacy or data protection laws on the statute book. Many of them are following the EU model.[90]

Enhanced enforcement: Under EU data protection law Member States are obliged to establish independent **supervisory authorities** (Data Protection/Information Commissioners or Commissions). Their position and independence has been considerably strengthened by Art. 8 of the Charter of Fundamental Rights and the jurisprudence of the European Court of Justice. The GDPR allows for administrative fines of up to EUR 20,000,000, or in the case of an undertaking, up to 4% of the total worldwide annual turnover, for violations of the Regulation.

85 Art. 25 (2) GDPR

86 Joint Committee of the European Supervisory Authorities, Discussion Paper on the Use of Big Data by Financial Institutions, JC 2016 86, para. 21

87 Ibid.

88 'Adequate' is not 'identical', but has been interpreted by the European Court of Justice as meaning 'essentially equivalent'.

89 Adequacy has been certified for the following third countries: Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland and Uruguay. These adequacy decisions were taken under Directive 95/46 and will remain in force under Art. 45 (9) GDPR.

90 Buttarelli, The EU GDPR as a clarion call for a new global digital gold standard, IDPL 2016, Vol. 6 No. 2, 77

Specific legislation on credit information and other areas

Among the relevant EU consumer protection rules the Consumer Credit Directive of 2008[91] supports the **principle of responsible lending** by requiring Member States shall 'ensure that, before the conclusion of the credit agreement, the creditor assesses the consumer's creditworthiness on the basis of sufficient information, where appropriate obtained from the consumer and, where necessary, on the basis of a consultation of the relevant database.'[92] However, this does not entitle the creditor to an unlimited collection of personal consumer data. The term 'sufficient information' is to be read together with the Data Protection Directive (as from 2018 the GDPR) which only allows for the collection of personal data insofar as they are necessary for the purposes of a future credit agreement. The Consumer Credit Directive also obliges Member States to provide effective alternative dispute resolution mechanisms for the settlement of consumer disputes with regard to credit agreements. These mechanisms should work in parallel with the independent data protection authorities under the GDPR.

As from January 2018 the new EU Payment Services Directive[93] (PSD 2) will give payment institutions (e.g. FinTechs) the right of access to credit institutions' (banks) account services on a non-discriminatory basis to allow them to provide customers with payment services if they have explicitly consented to their account information being accessed.[94] This is likely to facilitate new business models and increase competition in the financial sector. The processing of personal data by payment systems and payment service providers shall be permitted when necessary to safeguard the prevention, investigation and detection of payment fraud. The technical details of how FinTechs will be able to access consumer data (e.g. by 'screen scraping' or otherwise) are still under discussion.[95] Finally, the PSD 2, like the Consumer Credit Directive, requires Member States to provide alternative dispute resolution procedures for the speedy settlement of disputes between users and providers of payment services.[96]

The European Commission is also closely observing the potential negative effect that the use of big data may have on competition and thus also on consumers. For this reason, it has just imposed a EUR 2.4 billion sanction on Google Search for illegally using its dominant market position to promote its own shopping service in internet searches.[97] So far, however, there is no sign of imminent specific anti-trust regulation in this field.[98]

3.2.3 Further Regional Frameworks

Organisation of American States

The Organisation of American States (OAS) in 1969 adopted the American Convention on Human Rights which contains in Art. 11 a right to privacy which states that 'no one may be the object of arbitrary or abusive interference with his private life, his correspondence, or of unlawful attacks on his honor or reputation.'

African Union

More recently in 2014 the African Union adopted a Convention on Cybersecurity and Personal Data Protection which in Chapter II contains a number of detailed provisions closely modelled on the European legal framework including a number of specificities (not exclusively related to the financial sector). However, this Convention has not yet entered into force.[99] There are two regional African organisations, the Economic Community of West African States and the East African Community which more recently have approved certain general rules on data protection and cyber law.[100]

Asia-Pacific Economic Cooperation

APEC has formulated a privacy framework based on the OECD Guidelines which – to a less strict degree – echo the EU system of controlling data exports.

3.2.4 Conclusion

Regional legal frameworks are becoming more important in the process of an emerging international framework. The EU has adopted the most encompassing and strictest regulatory framework with some global influence due to its rules requiring adequate protection standards for data exports outside the EU.

91 Directive 2008/48/EC of the European Parliament and of the Council of 23 April 2008 on credit agreements for consumers and repealing Council Directive 87/102/EEC, OJ L 133/66 of 22.5.2008

92 Art. 8 (1) Consumer Credit Directive

93 Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, OJ L 337/35

94 Art. 36, 94 PSD 2

95 Cf. the Final Report with Draft Regulatory Technical Standards on Strong Customer Authentication and common and secure communication under Article 98 of Directive 2015/2366 (PSD 2) by the European Banking Authority (February 2017)

96 Art. 102 PSD 2

97 http://uk.reuters.com/article/uk-eu-google-antitrust-idUKKBN19I102

98 Cf. Van Wissen M and Prompers L, 2016. Big Data, Big Concerns? EU competition law implications of the changing role of big data in the financial services industry. Competition Policy International. 14 December 2016

99 Senegal is the only African state having ratified it. It will enter into force after 15 African states have ratified it.

100 See World Wide Web Foundation, A Smart Web for a More Equal Future, Personal Data – An overview of low and middle-income countries, July 2017, 8

3.3 National Legal Frameworks

There are numerous national legal systems outside Europe which provide for information privacy and the handling of credit information. The USA and Philippines have been chosen as examples of countries from the northern and southern hemispheres.

3.3.1 United States

Data privacy framework

Unlike in Europe there is no omnibus[101] federal privacy legislation regulating the private sector in the USA. The Privacy Act 1974 only covers the public sector (i.e. federal government agencies).[102] Congress has traditionally reacted to threats to privacy in the private sector in an ad hoc, 'patchwork' fashion. There is, for example, federal legislation regulating specific privacy aspects in the financial sector. However, data brokers are free to process and trade sensitive information (e.g. on HIV infection or dementia) despite increased legal protection for electronic patient files.[103]

Specific legislation on credit information

The Fair Credit Reporting Act (FCRA) 1970[104] was passed to protect individuals from the misuse of personal information by credit reporting agencies.[105] It regulates the disclosure of personal credit information by credit reporting agencies. They may disclose such information only to persons whom they have reason to believe intend to use the information to evaluate an application for credit, employment, insurance, licence, governmental benefit or any other legitimate business need. The FCRA – unlike the law in the EU, including the UK[106] – does not restrict in any way the collection of personal information by banks or intermediaries such as credit reporting agencies. They may legally collect excessive personal data which are not relevant for the purpose of evaluating a credit application.[107] This is a major difference to the European legal framework. In the USA there are three major national credit reporting agencies: Experian, Equifax and Trans Union. Each of these companies has information on virtually every adult American citizen, and they routinely-prepare credit reports about individuals.[108] These agencies are required to provide a central website to consumers to request their credit reports. This is not the case for other smaller consumer reporting agencies, which have to provide a toll-free phone number for such requests.

It was only by passing the Equal Credit Opportunity Act (ECOA)[109] 1974 that Congress limited the type of data which could be collected by creditors themselves. Special categories of data such as data relating to race, colour, religion, national origin, sex, marital status or age (provided the applicant has the capacity to contract) may not be used to deny access to financial resources. However, ECOA does not apply to discriminatory behaviour by credit reporting agencies and the degree of compliance with ECOA in reality is doubtful.[110]

A similar prohibition for the housing sector is stated in the Fair Housing Act 1968.[111] Health information may only be disclosed by credit reporting agencies vis-à-vis insurance if the data subject gives his or her explicit consent. But as the report on decision-making in the financial sector[112] notes, the collection of sensitive health data (e.g. on HIV infection) by credit reference agencies is legal in the US.

Under the FCRA, consumers have a number of rights:

» They have the right to know what's in their file with a credit reporting agency and can ask for one free credit report every year. To this end the Federal Trade Commission (FTC) offers an online tool for requesting credit reports[113] and actively encourages the use of it.

» They have the right to have inaccurate, incomplete or unverifiable information corrected or deleted;[114] exercising this right may lead to lower interest rates for loans. [115]

» Consumer reporting agencies may not give out outdated negative information in most cases (no negative information older than seven years and no information on bankruptcies older than 10 years).

101 Omnibus (lat.), all-encompassing

102 There are also numerous State Laws which are not covered here.

103 Cf. Health Information Technology for Economic and Clinical Health Act (HITECH Act) 2009

104 15 U.S.C. § 1681 et seq., amended by the Fair and Accurate Credit Transactions Act (FACTA) 2003

105 Rotenberg, The Privacy Law Sourcebook 2016, p. 41

106 Cf. the somewhat generalised account given in the Report on on Decision-Making in the Financial Services Sector – Understanding Classification Algorithms, p. 19

107 Reidenberg, Privacy in the Information Economy, A Fortress or Frontier for Individual Rights?, 44 Fed. Comm. L.J. 195 (1992)

108 Solove, Rotenberg and Schwartz, Information Privacy Law (2006), p. 702

109 15 U.S.C: 1691 et seq.

110 See Pam Dixon, Executive Director of the World Privacy Forum during a hearing in front of the US Senate's committee on Commerce, Science and Transportation, as quoted in the Draft Report 'Decision-making in the financial services sector – Understanding Classification Algorithms', p. 11

111 Sec. 804 [42 U.S.C. 3604]; cf. Draft Report on Decision-making in the financial services sector – Understanding Classification Algorithms, p. 22 f.

112 Draft Report on Decision-making in the financial services sector – Understanding Classification Algorithms, p. 11 and Appendix 3

113 https://www.consumer.ftc.gov/articles/0155-free-credit-reports?utm_source=take-action (seen on 10 April 2017)

114 This is of particular importance in view of the high error rate in credit reports in the USA (ca. 20%), cf. Mahoney, Errors and Gotchas: How Credit Report Errors and Unreliable Credit Scores Hurt Consumers, Report on behalf of the Consumers Union to the Federal Trade Commission (2014). This problem is not limited to the US.

115 https://www.consumer.ftc.gov/blog/it-pays-check-your-credit-report (seen on 10 April 2017)

» They have the right to know their score (but not the algorithm with which the score is calculated).

» A credit reporting agency may not give information about the consumer to employers without the consumer's consent.

» They must be given an advance warning (pre-adverse action notification) before a creditor, an insurer or an employer turns down an application for a loan, insurance cover or a job based on a credit or consumer report.

» They may sue credit reporting agencies for damages if they violate the FCRA.[116]

The FCRA is being enforced by the FTC which has the task to protect consumers against deceptive practices. This may include those cases of differential pricing which cross the line into fraudulent behaviour because sellers attract customers with false promises or bury important details in the small print of complex contracts.[117] The FTC also investigates complaints from individual consumers.

3.3.2 Philippines

Data privacy framework

The Philippines have omnibus privacy legislation on the statute book since 2012 which was brought into effect in 2016. The Data Privacy Act (DPA)[118] largely follows the European model. It includes the principles of purpose specification and limitation and personal data may not be retained once the original purpose of processing has been achieved. However, there are some interesting differences: information about someone's education as well as social security number, licences and tax returns are added to the special categories of sensitive data known under the EU GDPR. However, unlike in Europe, the DPA in principle does not apply to information covered by the Credit Information System Act[119]. But it will still apply to banks and other lenders when collecting and processing data about their customers themselves.[120]

These institutions and persons are obliged to inform the customer before entering personal information into a processing system inter alia about the type of information, the purpose of processing, the recipients and the length of storage.[121] In addition, customers have the right of 'reasonable access' to their data.[122]

Specific legislation on credit information

With the enactment of the Credit Information System Act 2008[123] (CISA) a centralised public Credit Information Commission (CIC) was created. This Commission runs a central registry aggregating credit information. Lending institutions are obliged to forward all positive and negative information about borrowers to the registry run by CIC. They can then either access the database themselves or use credit bureaux to establish the creditworthiness of potential borrowers. The CIC does not evaluate this information; the lenders will have to draw their own conclusions. In March 2016, six companies were accredited as credit bureaux (called Special Accessing Entities) for doing business in the Philippines; five of them foreign companies, one local. The core policy foundation of the CISA – according to the President of the CIC – is to increase access to credit for micro, small and medium-sized enterprises (MSMEs) which make up 99.58% of all businesses in the Philippines[124]. The CIC President continued: 'In lending, just like other businesses, time is cost. If the time required for lenders to get to know their clients is reduced, then that should translate into better service to the borrowers while opening up a bigger market and a higher quality loan portfolio for lenders. Being complete and up-to-date, we believe that credit scoring using CIC-collected credit reports will be the standard in the Philippine financial market in the next few years.'[125] The Financial Infrastructure Development Network launched during the APEC meeting in November 2015 in Manila wants to strengthen credit access for MSMEs in order to boost economic growth.[126]

3.3.3 Conclusion

Although there are stark contrasts between the economic, social and political situation in the USA and the Philippines it is interesting to see that both countries have regulation on privacy and credit information on the statute book. Albeit

116 State laws may provide for additional rights of consumers.

117 Cf. Executive Office of the President of the USA, Big Data and Differential Pricing (2015), p. 17

118 Republic Act No. 10173 ('An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes')

119 Sec. 5 lit. d DPA

120 Cf. Sec. 5, second sentence: 'Provided, that the non-applicability of the Act or these Rules do not extend to personal information controllers or personal information processors, who remain subject to the requirements of implementing security measures for personal data protection: Provided further, that the processing of the information provided in the preceding paragraphs shall be exempted from the requirements of the Act only to the minimum extent necessary to achieve the specific purpose, function, or activity.' The exact legal relationship between DPA and CISA is still to be determined.

121 Sec. 16 lit. b DPA

122 Sec. 17 lit. c DPA

123 Republic Act No. 9510

124 Figures for 2012 from the Department for Trade and Industry, http://www.philstar.com/banking/2015/07/21/1479053/cic-issues-guidelines-credit-bureaus (seen on March 12, 2017)

125 http://www.philstar.com/banking/2015/07/21/1479053/cic-issues-guidelines-credit-bureaus (seen on March 12, 2017)

126 http://www.philstar.com:8080/business/2016/03/14/1562871/philippines-oks-first-6-credit-bureaus (seen on 12 March 2017)

the dynamics in the development vary, as the regulations in the Philippines are far younger than those in the USA. Although the legal reality is certainly still another matter, certain legal rules in these fields seem to be a condition for good governance.

3.4. Summary

To summarise the analysis of three examples for legal frameworks regulating data privacy in the financial sector and credit scoring in particular, it can be concluded that **considerable differences exist between the global level, Europe, the USA and the Philippines**.[127] This is true not only for the legal, but also for the economic and social context. However, there are (at least) three main principles that can be found in all three regions and countries:

a) Transparency
Each data subject has a right to be informed about the processing of personal financial information referring to him or her and be given access to this information.

b) Accuracy
Each data subject has the right to have incorrect personal financial information corrected or deleted.

c) Enforcement
Oversight bodies exist in all three regions or countries, some of them specialist data privacy supervisory bodies (EU, Philippines), or general consumer protection bodies (USA). The US FTC has already applied harsh sanctions in certain cases of illegal data processing and the European supervisory authorities will have the power to do so when the GDPR comes into force in May 2018.

Other principles can be found in one or more, but not all, of the three legal frameworks analysed:

a) Personal information on the financial situation of data subjects/consumers may only be processed either with the informed consent of the data subject or if it is necessary for the purpose of concluding and implementing a credit or insurance agreement (prescribed in the EU and the Philippines).

b) A free credit report for the data subject/consumer per year (prescribed in the USA and Germany, possible in the EU and the Philippines).

c) The duty to embark on a data privacy impact assessment before processing financial customer data (prescribed in the EU).

d) The duty to develop services and business models which follow the concept of 'privacy by design and by default' (prescribed in the EU). This includes state-of-the-art methods for anonymisation or de-identification in the context of **big data**.

e) In the case of automated decision-making (profiling), increased transparency obligations, i.e. the duty to give a meaningful explanation to the data subject about the logic involved in the processing of his or her data while protecting business secrets (prescribed in the EU), as well as the right of the data subject to have the decision taken by the algorithm or a machine double-checked by a human being (right to human intervention) (prescribed in the EU).

f) Special categories of (sensitive) data concerning health, race, sex or religious belief may not be processed in the context of financial services even with the consent of the data subject; exceptions to this rule apply only if it is necessary to provide the specific service, e.g. life or health insurance (under EU law only).

g) 'Credit security freezing' which allows any consumer to place a security freeze on their credit report in case they are the victim of identity fraud in order to prevent further damage by criminals who apply for credit in their name. This is provided for in most US states[128] by state legislation as well as in Australia and New Zealand.

Whereas the US legal system lacks the requirement of informed consent or the need of a legitimate ground for processing customer data, the duty to design services and products according to the principles of privacy by design and by default and restrictions on automated decision-making (profiling), the EU has only limited restrictions for profiling and no duty to provide customers with a free annual credit report. In all legal systems visited there seem to be too high hurdles for consumers to find out about the working of algorithms used for scoring purposes.

127 For another comparison of regional regulatory frameworks on privacy in different countries see UNCTAD (2016) as referred to in World Wide Web Foundation (above note 25), 11 et seq.

128 http://consumersunion.org/research/security-freeze/ (seen on 6 April 2017)

4 | RECOMMENDATIONS FOR COUNTRIES WITH AND WITHOUT FRAMEWORKS ON HOW TO STRENGTHEN PRIVACY IN THE CONTEXT OF DIGITAL FINANCIAL SERVICES AND BIG DATA

In view of this comparative analysis it is difficult to suggest precise ways to achieve global standards for digital financial services to protect data privacy. However, it is now widely accepted that despite all cultural and legal differences, data privacy is not merely 'a first-world problem'.[129] Reports from developing countries[130] show that users of financial services often have similar problems as in developed countries and that in some developing countries innovative solutions for these problems are being called for.[131]

The question remains what steps could and should be taken to build the necessary trust-enhancing architecture[132] for digital financial services worldwide. Since **access to financial resources** is a **basic need** and can be seen as part of the right of everyone to an adequate standard of living for themselves and their family, including adequate food, clothing and housing, and to the continuous improvement of living conditions, it should not be made dependent on the excessive disclosure and processing of customers' personal information. In other words, access to financial resources does not justify the neglect of the data subject's informational autonomy, turning them into a mere object of data processing. The data subject will have to disclose certain data necessary to evaluate his or her creditworthiness or insurability. But he or she should still have freedom of choice and stay in control of the data disclosed and processed to the largest possible extent. Furthermore, the possible discriminatory or exclusive effects of big data analysis, like social sorting or segmentation, have to be avoided. This may well go beyond the scope of individual data privacy and include the effects on specific disadvantaged and underserved groups.[133]

Establishing uniform and legally binding global standards for data privacy to be observed by digital financial service providers will not happen by the turn of a key. It is bound to be a lengthy process just as the establishment of global data privacy standards in general. More than half of the countries in the world have data privacy laws but the rest is still lacking this legal framework. Therefore a number of different steps should be considered by industry, governments and the international community.

4.1 Good and Best Practice

To begin with, it is of vital importance to identify good and best practice for digital financial service providers against the backdrop of the principles mentioned above, in particular the principles of privacy by design and privacy by default. This should be further encouraged by governments, financial regulators and international stakeholders such as the G20 and the World Bank.

The G20 High-Level Principles for Digital Financial Inclusion already contain some practical examples of how customers of financial services could be given meaningful

129 Cf. the blogpost by Kate McKee, http://www.cgap.org/blog/5032-million-reasons-tackle-data-protection-now (seen on March 13, 2017)

130 See the example of blacklisting in Kenya mentioned above in Section 2.

131 Cf. Zeituna and others, Where Credit Is Due – Customer Experience of Digital Credit in Kenya (2017)

132 Cf. Costa/Deb/Kuzansky, Big Data, Small Credit: The Digital Revolution and its Impact on Emerging Markets Consumers, Omidyar Network, 2015, p. 30

133 Cf. European Parliament, Resolution of 14 March 2017 on fundamental rights implications of big data (2016/2225 (INI)), para. 5

choice and control online or offline.[134] Identifying customers when entering into a credit agreement is vital to create trust for providers of digital financial services. If – as suggested by the G20 Principles[135] – new and innovative forms of identification, such as biometric identification, are considered particularly for those currently lacking any form of identification, the recently published recommendations by the 'Berlin Group' on the necessary use of privacy-enhancing technologies[136] should be followed. The 'blockchain' technology is another novel development which may offer privacy-enhancing methods of verification. At the same time it raises different privacy issues because it relies on the permanent de-centralised storage of personal information and would therefore not allow for deletion at the request of a data subject. Anonymisation or encryption may help to find solutions here.[137]

Another practical example from Germany may illustrate good practice: The telecoms provider Deutsche Telekom is analysing metadata from its mobile network in an anonymised fashion to gain additional information to improve their customer services. Although this is not required legally they are offering their customers the possibility to opt-out of this process before the data are anonymised, as a confidence-building measure.[138]

Privacy-enhancing business models could be **certified with seals** as envisaged by the EU GDPR.[139] Governments may also encourage such business models in the public procurement sector by preferring digital financial service providers with privacy-compliant or privacy-enhancing services and products. Thus the **competitive advantage** which respect for the customer's data privacy gives will be strengthened. Competition in turn will offer greater freedom of choice for the consumer and data subject.

4.2 Self-Regulation

The credit industry on the national level, as well as internationally, should be encouraged to formulate codes of practice which stress and increase transparency and freedom of choice for the consumer and data subject. However, self-regulation by the industry does have its limits as long as there is no legal framework to which codes of practice can refer. In unregulated markets such 'soft law' rules without oversight or sanctions make little difference and often tend to be mere marketing exercises. Therefore 'regulated self-regulation' or 'co-regulation' is the preferred option. Self-regulation should not be an alternative to, but a valuable add-on for, legislation. As Principle 5 of the G20 High-Level Principles points out, enforceable, industry-based codes of conduct should be encouraged in order to self-regulate for higher standards than legally required.[140]

4.3 Digital and Financial Literacy and Awareness

As the analysis above has shown, data privacy requires transparency and freedom of choice. Above all, it requires that the consumer is well-informed about the consequences of sharing personal data in a digital environment as well as his or her rights as a data subject (digital literacy) and about the conditions and consequences of applying for credit in this environment (financial literacy). This is generally accepted in the current international discussion.[141] Certainly, people in different countries have different preferences and views about what kind of data they consider to be 'private'.[142] But few people would want to be confronted with a 'choice' of 'take it or leave it' when offered financial services in return for excessive personal information that is irrelevant for assessing the creditworthiness but of economic (e.g. marketing) interest for the credit institution or agency. Obviously, the revelations about mass surveillance by governments as well as massive data breaches (e.g. Yahoo) have already increased awareness among data subjects.[143]

The Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH on behalf of the German Federal Ministry for Economic Cooperation and Development (BMZ) is addressing the issue of digital financial literacy in a

134 See Principle 5, G20 High-Level Principles for Digital Financial Inclusion, p. 15 et seq.

135 G20 High-Level Principles for Digital Financial Inclusion, p. 20

136 International Working Group on Data Protection in Telecommunications ('Berlin Group'), Working Paper on Biometrics in Online Authentication, November 2016, https://www.datenschutz-berlin.de/working-paper.html (seen on March 15, 2017)

137 Cf. Berberich and Steiner, Blockchain Technology and the GDPR – How to Reconcile Privacy and Distributed Ledgers?, EDPL 2016, 422 et seq.

138 https://www.telekom.com/de/medien/medieninformationen/detail/telekom-will-wirtschaftswunder-4-0-349084 (seen on 10 April 2017)

139 Art. 42 GDPR

140 G20 High-Level Principles for Digital Financial Inclusion, p. 16

141 See Principle 6, G20 High-Level Principles for Digital Financial Inclusion, p. 17 et seq.

142 Cf. the survey of consumers in Colombia and Kenya by Costa, Deb and Kuzansky, Big Data, Small Credit: The Digital Revolution and its Impact on Emerging Markets Consumers, Omidyar Network, 2015, p. 19 et seq. ('In Kenya, about 41 per cent of those we interviewed were concerned about their information being given to the government revenue authorities. In Colombia, 87 per cent worry their information would be accessed by criminals (and were far less concerned about tax authorities). But these considerations did not overshadow their willingness to share sensitive personal data with lenders in order to access credit … Again, we expect these attitudes to change and evolve as consumers become more entrenched and experienced in the formal financial system, and as more financial services become available to them.', p. 24)

143 Cf. the blogpost by Kate McKee, http://www.cgap.org/blog/5032-million-reasons-tackle-data-protection-now (seen on March 13, 2017)

current project in Jordan.[144] In collaboration with the Central Bank of Jordan, information campaigns and training courses for Syrian refugees, low-income Jordanians and women in particular, promote the responsible use of digital financial services. Another example for increasing digital and data privacy literacy is the training of Ugandan smallholders to access their own data and to build up their own track record. The project implemented by GIZ on behalf of BMZ in co-operation with Bernhard Rothfos will raise awareness among farmers about digital solutions used for data collection and mobile payments. Farmers will be trained and sensitised on the consequences of collecting their production data, e.g. as a basis for loan assessments. Farmers shall benefit from increased transparency by accessing their personal transaction data. This will help them to plan their farms as businesses.

4.4 National Legislation

It remains to be seen if and at what pace countries around the world will adopt general legal frameworks for data privacy or specific rules for digital financial services including privacy issues in this sector. A right to privacy may also be derived from existing constitutional guarantees as has recently happened in India where the Supreme Court unanimously interpreted an existing article of the constitution as providing for such a right, thus throwing into doubt the legality of a national biometric identification scheme (Aadhar).[145] The EU GDPR with its adequacy requirement (see above, p. 6) has created a certain momentum here and could well continue to support the spreading of general data privacy laws. APEC has formulated a privacy framework based on the OECD Guidelines which – to a less strict degree – echo the EU system of controlling data exports. The OECD Guidelines themselves with the principles of limiting the collection of personal data, of purpose specification and use limitation and the principle of accountability of data controllers seem to be the highest common denominator for national data privacy laws.

The increasing number of national data privacy laws and laws on consumer protection may either foster the process of developing international legal standards or it may be the other way round. Be that as it may, in view of the great importance for economic development, national regulators should not wait for the international community to pass binding rules at least in the area of data privacy and to provide for a use of big data without discriminatory or exclusive effects.

144 https://www.giz.de/en/worldwide/38566.html

145 Puttaswamy v. Union of India, see https://www.worldprivacyforum.org/2017/08/a-big-win-for-privacy-in-india/ (seen on 25 August 2017)

4.5 Cooperation in Oversight and Complaint Handling Procedures

In Europe, there are numerous oversight bodies in the financial sector[146] as well as data protection authorities under the existing and future legal framework. Cooperation between these bodies is vital to create synergies in the necessary oversight of data privacy rules. Financial oversight bodies should share information with data protection supervisors and vice versa as far as legally possible. Mechanisms for knowledge-sharing to facilitate this should not only be established between regulators and service providers[147] but also between regulators for different sectors (e.g. anti-trust authorities). This is equally true for consumer protection authorities who – like the FTC – play an exclusive role in this field in the USA where there is no specific data privacy oversight mechanism in the private sector. The European Data Protection Supervisor has suggested the creation of a Digital Clearing House between different regulators in Europe.[148] This may be extended at some stage to become a global platform. Regulatory bodies and non-governmental organisations should also consider closer cooperation. Despite their different roles and bearing in mind the legal restrictions for regulators, their actions can have positive synergetic effects. Regulators with their formal sanctioning powers can effectively enforce the law but may have limited powers to do so publicly, whereas NGOs can more easily drum up public support and raise public awareness of the issues.

In countries without a legal framework and oversight for privacy and data protection, complaint handling procedures (including alternative dispute resolution outside the courts [149]) should be established which could address not only grievances concerning the denial or conditions of credit but also data privacy issues in this context.

146 Cf. Joint Committee of the European Supervisory Authorities, Discussion Paper on the Use of Big Data by Financial Institutions, JC 2016 86

147 See G 20 High-Level Principles for Digital Financial Inclusion, p. 10

148 European Data Protection Supervisor, Opinion 8/2016 of 23 September 2016, p. 15

149 Cf. the EU Payment Services Directive, above Chapter III 2 b).

4.6 International Standards

Eventually global legal and technical standards will be necessary to provide for a minimum level of protection as well as a level playing field for providers and data subjects. Numerous standard-setting bodies are working in this field already.[150] The International Conference of Data Protection and Privacy Commissioners has on various occasions called for the adoption of international standards for data protection or the integration of such standards in existing international conventions.[151] Following the revelations on mass surveillance by intelligence agencies there have been calls to update the International Covenant on Civil and Political Rights in order to better protect privacy in the digital age.[152] The resolutions passed by the UN General Assembly and the activities of the UN Special Rapporteur on the Right to Privacy[153] may support this development.

4.7 Next Steps for the G20

The G20 governments should consider the following steps:

a) Support and finance research and innovation in privacy-enhancing big data technologies such as anonymisation (de-identification);

b) Support and intensify efforts on the national and international level (e.g. in the UN General Assembly, the International Law Commission and other standard-setting bodies) to draft rules on how to use big data technologies either in general or specifically to foster financial inclusion in order to safeguard the fundamental right of data subjects to data privacy and create a global level playing field to boost the digital economy worldwide.[154]

150 See GPFI, Global Standard-Setting Bodies and Financial Inclusion – The Evolving Landscape, White Paper, March 2016, p. 53

151 See e.g. the Madrid Resolution on International Standards on the Protection of Personal Data and Privacy (2009), https://icdppc.org/wp-content/uploads/2015/02/The-Madrid-Resolution.pdf (seen on March 15, 2017)

152 ACLU, Informational Privacy in the Digital Age, https://www.aclu.org/other/human-right-privacy-digital-age (seen on March 15, 2017)

153 http://www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx (seen on March 15, 2017)

154 Cf. the proposal made by the European Parliament in its Resolution of 14 March 2017 on fundamental rights implications of big data, p. 6, for the European Single Digital Market

5 I CONCLUSION

Despite differences in existing legal frameworks and markets, data privacy is increasingly acknowledged as a prerequisite rather than an obstacle for financial inclusion. Data subjects in their role as consumers should have a real choice and transparency as to which purposes their personal data are collected for. FinTechs and InsurTechs need to verify to whom they give credit or insurance cover. Trust – or to use Albert Schweitzer's term 'confidence' – is key in order to achieve financial inclusion. A trust-enhancing architecture requires openness, choice and control for the data subject. A creditor or insurer has a legitimate interest to assess the financial situation of potential customers. But excessive and non-transparent processing of personal data can have an additional exclusionary effect on customers who would rather stay offline than lose control over their data. If scoring processes rely on false personal information, the data subject must have a right and a practical possibility to discover and correct the mistake. Financial inclusion will only happen if transparency and limited collection and retention of personal data are the guiding principles for any financial institution. Big data can be used in a privacy-enhancing fashion by implementing de-identification techniques.

A final remark: it is not sufficient to follow legal and technical rules for the use of big data methods, ethical standards have to be observed as well. Big data could lead to conformist behaviour by penalising any deviation from the statistical or expected norm. Potential customers may be induced to avoid certain behaviour, contact with certain people or visiting certain areas.[155] The data subject is more than a consumer. He or she is also a citizen. If citizens are subjected to a 'social credit system'[156] or 'Citizen Score'[157] in which governments analyse their buying habits, social media behaviour and political opinion with big data algorithms to determine one's opportunities for life then this is neither acceptable for free and democratic societies nor is it ethically defensible.

155 See the Preliminary Opinion by the European Data Protection Supervisor, Privacy and competitiveness in the age of big data (March 2014)

156 https://chinacopyrightandmedia.wordpress.com/2014/06/14/planning-outline-for-the-construction-of-a-social-credit-system-2014-2020/ (seen on March 15, 2017)

157 http://www.computerworld.com/article/2990203/security/aclu-orwellian-citizen-score-chinas-credit-score-system-is-a-warning-for-americans.html (seen on March 15, 2017)

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