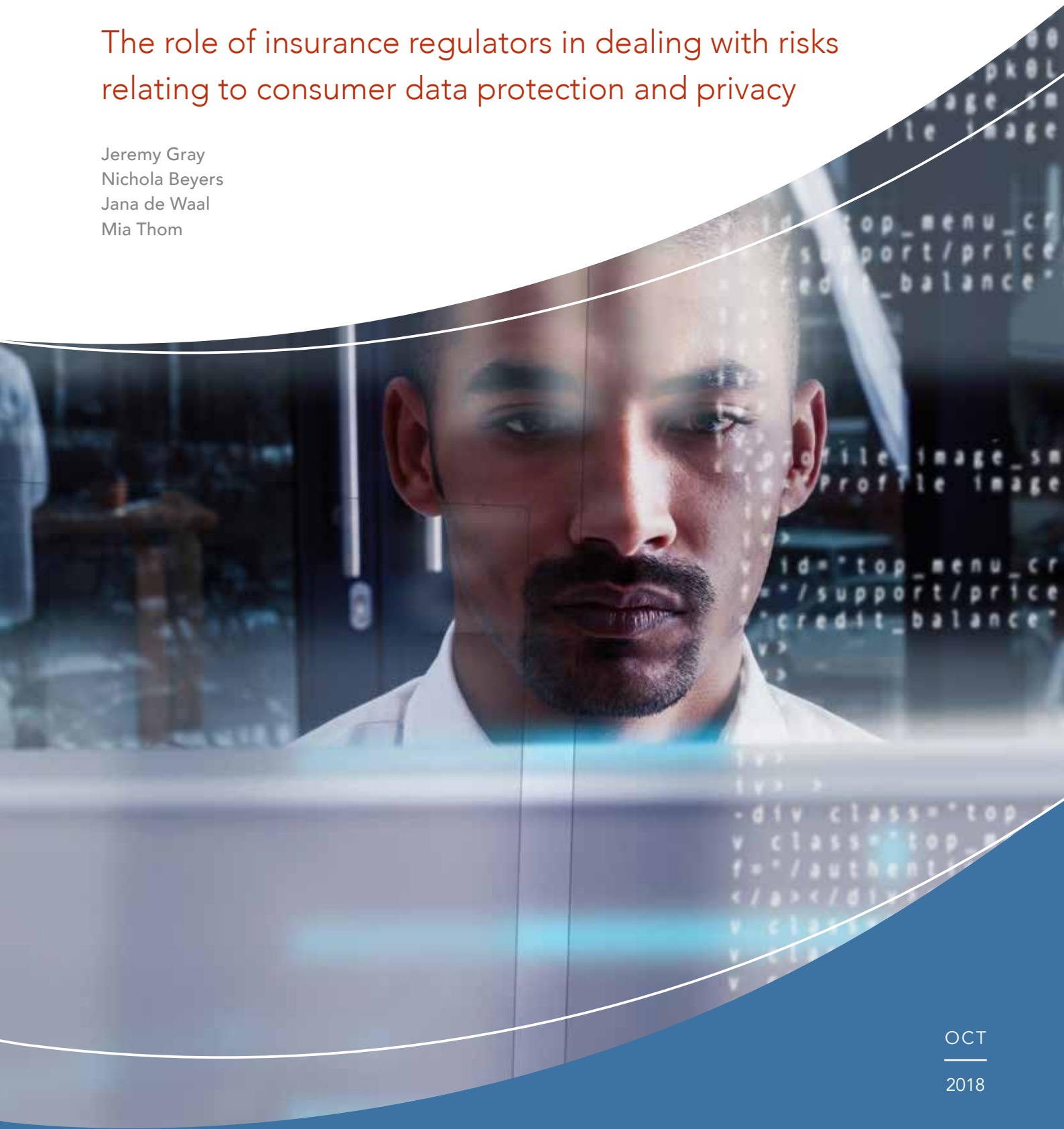


# Regulating for responsible data innovation:

The role of insurance regulators in dealing with risks relating to consumer data protection and privacy

Jeremy Gray  
Nichola Beyers  
Jana de Waal  
Mia Thom



## Imprint

**Published by:**

Access to Insurance Initiative

**Hosted by:**

Financial Systems Approaches  
to Insurance

Deutsche Gesellschaft für  
Internationale Zusammenarbeit  
(GIZ) GmbH  
Dag-Hammarskjöld-Weg 1-5  
65760 Eschborn, Germany

Telephone: +49 61 96 79-1362

Fax: +49 61 96 79-80 1362

E-mail: [secretariat@a2ii.org](mailto:secretariat@a2ii.org)

Internet: [www.a2ii.org](http://www.a2ii.org)

**Responsible:**

Access to Insurance Initiative  
Secretariat

**Text and editing:**

Access to Insurance Initiative  
Secretariat

**Pictures:**

© istock | 834500976 Tinpixels

Eschborn, October 2018

In partnership with:



## Acknowledgments

The authors would like to thank Stefanie Zinsmeyer (A2ii) for her invaluable contributions to the report and to the reviewers: David Watts, David Medine (CGAP), Denise Garcia (Financial Stability Institute), Denis Cabucos (Insurance Commission of the Philippines), Elias Omondi (Insurance Regulatory Authority, Kenya), Natalie Haanwinckel Hurtado (Superintendência de Seguros Privados (SUSEP), Brazil) and the Federal Financial Supervisory Authority of Germany (BaFin), who all took the time to provide us with helpful and constructive suggestions. We would also like to thank the individuals interviewed from regulatory bodies, expert institutions and financial services providers for your inputs into this research process.



## Contents

List of Abbreviations . . . . .	3
Executive summary . . . . .	4
<b>1. Introduction . . . . .</b>	<b>8</b>
<b>2. The opportunities and benefits of data . . . . .</b>	<b>10</b>
<b>3. What are the key data risks to consumers? . . . . .</b>	<b>12</b>
3.1 Potential negative consumer outcomes . . . . .	13
3.1.1 The data value chain . . . . .	16
3.1.2 Risk drivers . . . . .	17
<b>4. How can insurance regulators respond? . . . . .</b>	<b>20</b>
4.1 Mandate . . . . .	21
4.2 Market context: assessing how important data risks are in the market . . . . .	22
4.3 Regulatory context: omnibus, sectoral or no data protection legislation . . . . .	24
<b>5. Implementation tools . . . . .</b>	<b>29</b>
5.1 Omnibus approach . . . . .	34
5.2 Sectoral approach . . . . .	38
5.3 No legislation exists . . . . .	40
<b>6. Requirements for success: insurance regulator’s additional considerations . . . . .</b>	<b>43</b>
<b>7. Available strategies to insurance regulators . . . . .</b>	<b>44</b>
<b>8. Conclusion . . . . .</b>	<b>48</b>
<b>Bibliography . . . . .</b>	<b>49</b>
<b>Appendix A: Country case studies . . . . .</b>	<b>54</b>
Australia: Australian Information Commissioner (OAIC) . . . . .	55
Germany: The Federal Financial Supervisory Authority (BaFin) . . . . .	56
Kenya: Insurance Regulatory Authority (IRA) . . . . .	57
Mexico: Comisión Nacional de Seguros y Fianzas (CNSF) . . . . .	58
South Africa: Financial Sector Conduct Authority (FSCA) . . . . .	59
The Philippines: The Insurance Commission (IC) . . . . .	60
The USA: The National Association of Insurance Commissioners (NAIC) . . . . .	61
<b>Appendix B: List of laws cited . . . . .</b>	<b>62</b>
<b>Appendix C: List of organisations interviewed . . . . .</b>	<b>63</b>

## List of Abbreviations

APRA	Australian Prudential Regulatory Authority
ASIC	Australian Securities and Investments Commission
BaFin	Federal Financial Supervisory Authority
BDAI	Big Data and Artificial Intelligence
BfDI	Federal Commissioner for Data Protection and Freedom of Information
BMA	Bermuda Monetary Authority
CGAP	Consultative Group to Assist the Poor
CIMA	Inter-African Conference on Insurance Markets
CNSF	Comisión Nacional de Seguros y Fianzas
DIFS	Data-Intensive Financial Services
FAIS	Financial Advisory and Intermediary Services
FCA	Financial Conduct Authority
FSCA	Financial Sector Conduct Authority
FSP	Financial Service Provider
GDPR	General Data Protection Regulation
GFIN	Global Financial Innovation Network
GMEI	Global Mobile Engagement Index
IAIS	International Association of Insurance Supervisors
IC	Insurance Commission
ICP	Insurance Core Principle
IFAI	Instituto Federal de Acceso a la Información y Protección de Datos
IPRS	Integrated Population Registration System
IRA	Insurance Regulatory Authority
IRDA	Insurance Regulatory and Development Authority
MAS	Monetary Authority of Singapore
MNO	Mobile Network Operator
NAFTA	North American Free Trade Agreement
NAIC	National Association of Insurance Commissioners
OAIC	Australian Information Commissioner
OECD	Organisation for Economic Co-operation and Development
POPI	Protection of Personal Information
SARB	South African Reserve Bank
SUSEP	Superintendência de Seguros Privados
TCF	Treating Customers Fairly
UIDAI	Unique Identification Authority of India
UNCTAD	United Nations Conference on Trade and Development

## Executive summary

This report takes stock of what it takes to regulate for responsible data innovation.

**New data uses bring opportunities and risks.** New technologies mean the collection, storage and use of consumer data have grown significantly over the last decade. The use of data in the insurance industry holds enormous potential to reach new customers, to design better products that offer customers greater value and to enhance operating efficiency. Thus, the improved use of increasing consumer data can help make insurance markets more inclusive. However, as data proliferates, so do the opportunities for the exploitation of that data for illegal and/or unethical means, which manifests in risks to consumers.

Data innovation is therefore challenging the traditional role of insurance regulators. Two major dilemmas emerge that insurance regulators and indeed all financial sector regulators face when confronted with how to regulate consumer data.

1. They must tread the balance to achieve positive consumer outcomes, by both enabling data-driven innovation but still protecting consumers from the risks that arise.
2. They must protect consumers within their sector from the risks that arise even though they do not have sole regulatory oversight over the collection, storage and use of consumer data, which cuts across society. Moreover, this expansion on the traditional role of insurance regulators means that they may have insufficient expertise to understand, manage and oversee these new risks.

This study considers each of these dilemmas and explores the options available to regulators to achieve their objectives given these challenges.

Six negative consumer outcomes are identified in the insurance industry that can arise from data collection, storage and use:

- **Compromised safety and security.** The risk that a consumer is exposed or feels exposed to danger, which can result in physical or emotional hurt, injury or loss.
- **Exclusion and lack of value.** The risk that consumers do not have access to financial products and services that meet their needs and are useful and affordable.
- **Reputational risk.** The risk that an individual's character or good name is or is perceived to be impugned.
- **Financial loss.** The risk that a consumer sustains economic harm or damage.
- **Loss of privacy.** The risk that a consumer's right to determine who has access to and use of personal information, physical spaces or bodies is compromised or violated.
- **Manipulation.** The risk that a consumer's behaviour and decision-making are influenced to their detriment and hence that their autonomy is intentionally hindered.

These risks arise from five common causes or drivers:

- **Inadequate data governance and controls.** The absence – within an industry, or individual business – of a culture and a strategy that explicitly considers the data risks to consumers and actively seeks to limit the negative outcomes throughout the processes in which it engages.
- **Error.** Instances where a consumer’s data unintentionally deviates from truth or accuracy.
- **Involuntary or uninformed consent.** Instances where consumers either do not agree to have their data collected or do not fully understand the implications of having their data collected.
- **Unauthorised sharing and use.** The acquisition, transfer, possession or use of consumer data for purposes beyond that for which the information was collected, or beyond a use consistent with that purpose.
- **Data breaches.** The acquisition, transfer, possession or use of consumer data in an unauthorised manner with the intent to commit or in connection with fraud or other crimes, or where a consumer’s data ‘vanishes’ (for example, as a result of mechanical or power failure, physical damage, malware, viruses, human error or theft).

**Imperative for a context-specific response.** Given the changing landscape of data and the need to adjust to the digital age, regulators are increasingly required to tread a delicate balance to achieve positive consumer outcomes<sup>1</sup>, by both enabling data-driven innovation and protecting consumers from the risks that arise (IAIS, 2018a). Insurance regulators need to understand the context in which they operate in order to identify the most effective strategy and appropriate implementation tools to achieve positive consumer outcomes within this new and changing environment. The often global nature of data also requires a coordinated approach to global learning and supervision.

**What should the insurance regulator’s role be?** Data risks are pervasive and seldom affect only one sector. The insurance regulator – or any single other financial regulator – is therefore never the sole regulatory entity mandated to address these risks, but it requires a policy response based on social norms. In many countries, a data-specific regulatory agency is established to deal with data protection across society. Nevertheless, data-related risks may be specific to the insurance industry, or manifest uniquely in the insurance sector, meaning that insurance regulators need to consider these risks, even when a data protection regulator exists. Part of insurance regulators’ core mandate is to protect consumers from data-related risks if consumers are not effectively protected under the authority of the data protection agency. Insurance regulators should therefore be aware of what their options are to ensure that their consumers are protected from both abuse and exclusion.

---

<sup>1</sup> Insurance Core Principle (ICP) 19 on Conduct of Business discusses the objective as to protect policyholders and promote fair consumer outcomes (IAIS, 2017).

**Starting point: understand the risks to consumer outcomes.** Insurance regulators need to first understand the risks arising from the collection, storage and use of consumer data to insurance consumers within their context. The rapidly changing nature of the consumer data landscape means that ongoing monitoring and learning are required to identify new or unique risks that emerge and how they manifest differently across contexts.

**Understand what can be done within context.** Regulators are bound by the broader legislative approach to data protection adopted in their jurisdiction. Three common legislative approaches are identified:

- An **omnibus approach** whereby a cross-cutting data protection regulatory framework is established, sometimes with a dedicated regulatory authority, such as in the EU and South Africa.
- A **sectoral approach** whereby it is the responsibility of each sectoral regulator to address data protection or privacy, such as in the US.
- **No existing legislation** specific to data protection and privacy, such as in Kenya.

The overall legislative approach provides individual regulators with relatively more or less autonomy and responsibility to regulate data use within their sector. However, the individual regulators must still determine how engaged they should be within this legislative approach, based on the nature and likelihood of risks arising within their market context and what they are able to do within their capacity.

**Four regulatory strategies.** Insurance regulators may apply four broad strategies to regulate for responsible data innovation<sup>2</sup>. These approaches are driven by the country approach to data regulation and the degree of engagement needed by the insurance regulator to ensure positive consumer outcomes. In some markets a blended approach is followed where insurance regulators are, for example, waiting on data legislation to become effective.

- **Create.** Regulators that operate in a sectoral legislative approach or in an environment with no cross-cutting data privacy and protection legislation in place have the primary responsibility to develop the approach to data protection and privacy within their sector. Regulators can therefore actively create the data regulation approach for the insurance sector. This can be done by drafting and enforcing new regulation, as well as through proactive coordination strategies with other regulators.
- **Shape.** Regulators that operate within an omnibus legislative approach will not have the ability to create the overarching data legislative approach, but regulators can actively shape and tailor the application of policy to the insurance sector. This can be done by advising the policymaker on risks and outcomes that arise from insurance markets, coordinating with the data regulator on supervision to ensure that appropriate insurance sector provisions are put in place and raising awareness of data related risks with

---

<sup>2</sup> As regulators can engage in a range of potential activities, the extent to which regulators actively engage in and mould an approach will vary across regulators that may still be classified in the same category. In some cases, regulators may fall 'between' categories where they are active in some areas but passive in others. Nevertheless, these categories provide a heuristic to broadly classify regulators' observed general strategies.



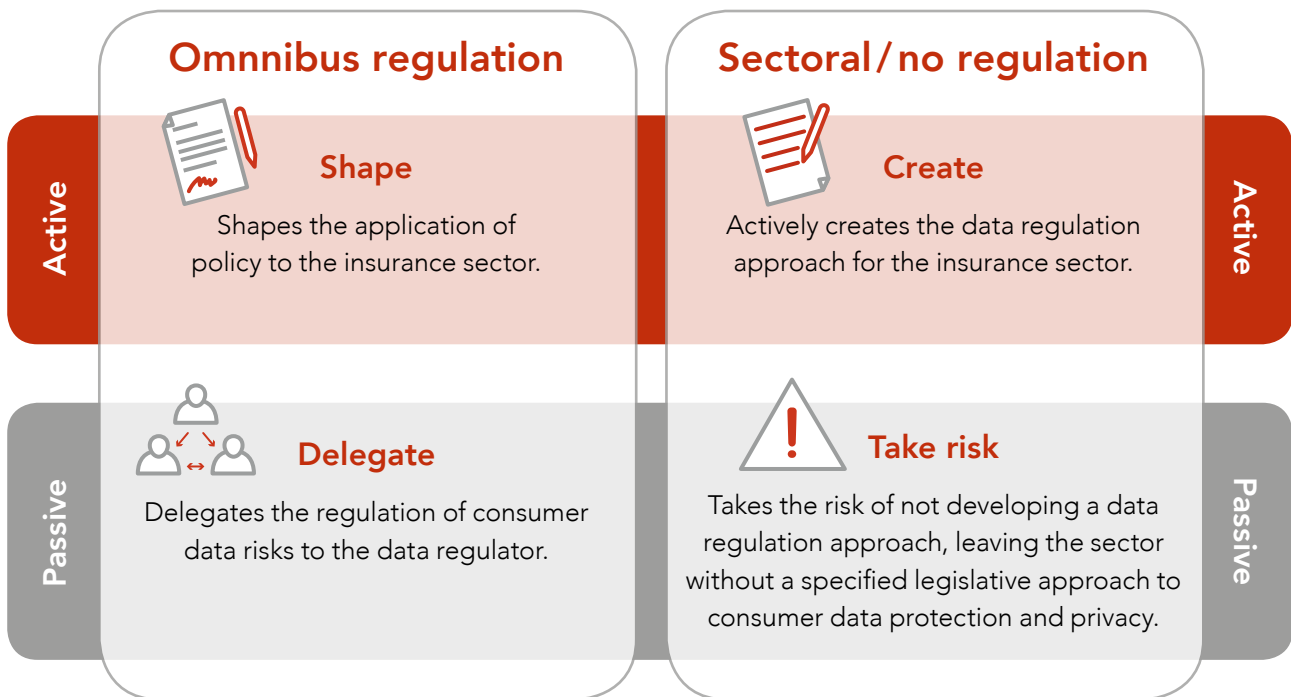


Figure 1: Available strategies to regulators | Source: Authors' own

providers and consumers. Regulators can also actively shape the approach to data protection in the insurance sector by drafting and enforcing insurance-specific regulation, supplementary to existing data protection legislation.

- **Delegate.** Alternatively, regulators that operate in an omnibus legislative approach can play a less active role, effectively delegating the regulation of consumer data risks to the data regulator. This option may be mandatory or pursued if it is considered that the omnibus regulation already effectively addresses the unique risks that manifest in the insurance market.
- **Take risk.** Regulators that operate in a sectoral legislative approach or in an environment with no legislation can alternatively remain in the default position or explicitly decide to take the risk of not developing a data regulation approach, which will mean the sector has no specified legislative approach to consumer data protection and privacy. This option is applied in markets where data-related risks are not considered an imminent threat.

## 1. INTRODUCTION

Technological change – on a global scale – is occurring at a more rapid pace than ever witnessed before and its impact on civil society and the business environment is unmistakable. It is estimated that over the course of only one internet minute in 2017, 3.5 million Google search queries were conducted, 156 million emails were sent, and USD751,522 was spent online (Desjardins, 2017). Given the vast amount of data that these activities represent, there is potential for firms to access more sources of information on consumers than ever before. As technological advances improve computing power and algorithms, firms' ability to store and use big data<sup>3</sup> has also increased exponentially (IAIS, 2017). While there is significant potential for these developments to result in innovations that improve value to consumers, they have also rendered consumers vulnerable to new threats, a trend that is growing equally exponentially. In 2013, about 575.5 million data records were breached (Gemalto, 2014). In 2017, more than 2.6 billion data records were breached, which translates into about 82 records lost, stolen or exposed every second at an increase of 350% in just five years (Gemalto, 2018). Of these incidents, 69% are classified as "identity theft", where a consumer's personal information is stolen (Gemalto, 2018).

Given the changing landscape of data and the rapid rise of data breaches, regulators are increasingly required to tread a delicate balance to empower consumers to make sovereign decisions and achieve positive consumer outcomes, by both encouraging data-driven innovation to improve value and protecting consumers from the risks that arise. Consumers cannot "make a sovereign decision" unless they: a) have sufficient information about the possible reach and potential consequences of the use of their data, b) have access to dependable means that enable them to determine how their data is used, and c) have "actual freedom of choice" (BaFin, 2018). By 2017, 107 UN member countries had implemented data protection and privacy legislation (UNCTAD, 2018). The EU's GDPR<sup>4</sup> (which was implemented in May 2018) is likely the best-known example of data protection and privacy regulation.

Insurers often collect particularly sensitive information to deliver their products. More data can create value, or it can lead to abuse. Health data is a good example – insurers can use deeper data to drive behaviour and nudge clients to live healthier lives. It can also be used to exclude people from cover, or its loss can cause significant breaches of privacy. This is not restricted to developed countries where health wearables and genome mapping are increasingly common. Such data will also be available from more digitised national health systems, greater use of telemedicine, smartphones and even location data, which can be used to identify health-seeking or risk-taking behaviour. These trends are already present in many developing countries.

This report seeks to provide a framework to support regulators on this journey to enable responsible data innovation.

**Objective.** This report identifies key considerations for insurance regulators to enable responsible data innovation in their markets. It discusses the main benefits and risks of data to con-

---

<sup>3</sup> According to Gartner (2018), big data is "high-volume, high-velocity and/or high-variety information assets that demand cost-effective, innovative forms of information processing that enable enhanced insight, decision making, and process automation".

<sup>4</sup> Available online: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679>.

sumers and provides a framework to help insurance regulators calibrate their response to the increasing collection, storage and use of data, tailored to their context.

**Methodology.** Detailed interviews with regulators, industry experts and financial services providers (FSPs) were conducted to develop and test the various frameworks included in this report. These interviews were supplemented with desktop research on consumer data protection and privacy principles and the potential risks and regulatory responses. In total, 18 stakeholder discussions were conducted. In addition, 10 regulators, spanning 15 jurisdictions, four industry experts and four FSPs were consulted. Appendix C provides a detailed list of interviewees.

## 2. THE OPPORTUNITIES AND BENEFITS OF DATA

**Data can open new consumer markets.** Across emerging markets, the use of insurance remains limited. In 2016, the average insurance penetration in emerging markets was 3.2% and emerging markets’ share (excluding China) of total insurance business was only about 10% (Swiss Re Institute, 2017). A lack of reliable data on consumers and the risks they face often requires insurers to charge higher premiums to account for the associated uncertainty, and it limits their ability to understand consumers’ needs, which contributes to exclusion. Leveraging new datasets allows insurers to price more accurately for risk, better understand their consumers’ needs and accordingly design better products, and better monitor and reduce the incidence and cost of fraud (Bhoola et al., 2014). The implication is that embracing the use of new datasets has the potential to increase insurance inclusion (Chen and Faz, 2014; Smit et al., 2017 and Cheston et al., 2018). Figure 2 illustrates, for instance, the number of insurtech innovations that have recently been observed, many of which rely on collecting new types of consumer data and using that data in innovative ways. Substantive limitations on the use of consumer data will continue to manifest in the risk that the clear majority of consumers will remain excluded from insurance.

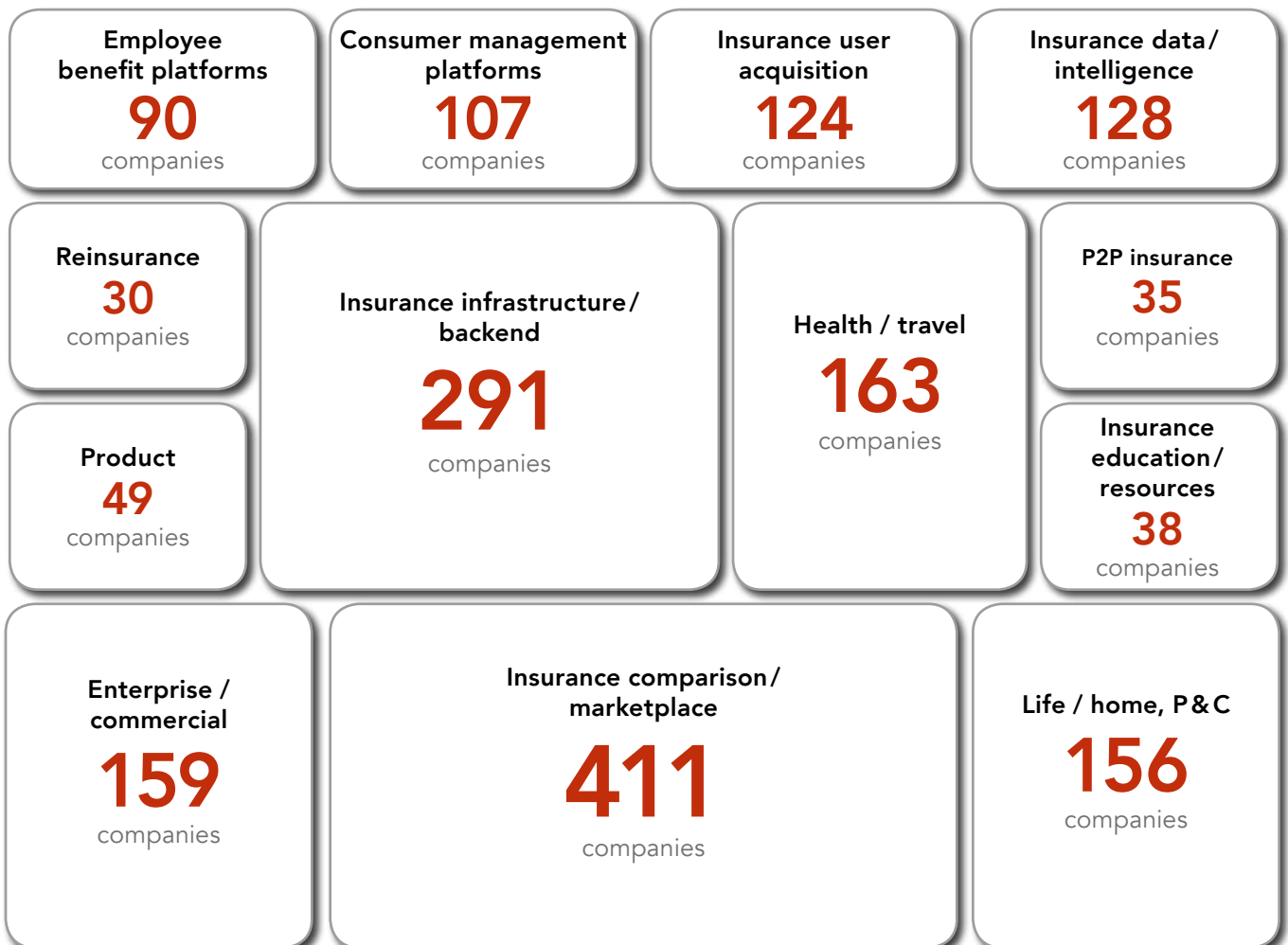


Figure 2: Insurtech start-up landscape | Source: Venture Scanner, 2018

**Data can improve value to consumers.** As the latest developments in insurtech illustrate, innovation and the use of data may also improve value to consumers, enhance efficiency and resolve issues across the value chain, thereby reducing the risk of exclusion. For example, one of the major challenges that insurers face in serving low-income markets is a “lack of information on consumers”. New data and analytics make it easier for insurance providers to improve their knowledge of their customers and even to incentivise customers to change their risk-seeking behaviour (Ransbotham and Kiron, 2018; Castro and New, 2016; Smit et al., 2017 and Chen and Faz, 2015).

**Data is critical to the business case – to manage costs and innovate.** Firms that innovate successfully differentiate themselves from their competitors in the hope of advancing their stake in the market (Riggs, 2015). Data is an increasingly fundamental factor in and driver of innovation. For example, as a direct result of their investments in big data, of the Fortune 1000 executives interviewed, 49% indicate they have decreased expenses and 44% that they have found new innovation avenues (Bean, 2017). These benefits are apparent in the insurance industry, too: According to Smit et al. (2017), digital platforms and new data and analytics initiatives introduce cost-saving and efficiency enhancements that span across the entire product lifecycle in developed and developing country insurance markets.

**Data can address exclusion.** The critical implication for developing country insurance regulators is that the use of consumer data by market players can – and is – playing a substantive role in mitigating one of the biggest existing risks to consumers in developing countries, namely exclusion. Conversely, if restrictions on data collection and use substantively limit providers’ ability to access the benefits, a ‘lack of data’ can give rise to the risk of exclusion.

### 3. WHAT ARE THE KEY DATA RISKS TO CONSUMERS?

**Treading the balance to improve consumer outcomes with data use.** Data can include more people with increasingly valuable and affordable products. However, data can also expose consumers to risk. Insurance regulators therefore need to find a balance by protecting consumers while limiting exclusion or abuse<sup>5</sup>.

**As data proliferates, so does the potential for abuse.** In 2017, more than 600 million records were affected in over 1,200 incidents of identity theft (Gemalto, 2018). This represents an increase of 73% from 2016. Given that identity theft is only one of the potential illegal uses for consumer data, the magnitude of the risks arising from data should not be underestimated.

**Data breaches occur frequently and carry a significant cost.** The high frequency of data breaches imposes significant costs on firms. The size of these costs is revealed in the IBM Security and Ponemon Institute's Cost of Data Breach Study for 2017. The study surveyed 419 companies in developed and developing markets and found the average total cost of data breaches is USD3.62 million. Given the high frequency and average cost of breaches, this is an issue that actors in the private and public spheres cannot ignore. Insurance providers are also prime targets for data breaches. In 2015, for example, Anthem, a health insurer in the US, discovered that it had suffered a significant cyber-security breach. In response to the breach – which affected 78.8 million consumer records – the company paid USD260 million “for security improvements and remedial actions in response to this breach” and “agreed to provide credit protection to all consumers whose information was compromised” (California Department of Insurance, 2017).

**Data breaches not only in developed countries.** Although the majority of data breaches have been recorded in developed countries, in 2017 alone, breaches were recorded India, South Africa, Kenya, Mexico, Nigeria and the Philippines among others developing nations (Gemalto, 2018). In 2017, for example, the South African FSP and life insurer Old Mutual “detected a case of unauthorised entry into one of [its] systems”, the result of which was that some of its clients' personal information was accessed (Old Mutual, 2018).

**Data breaches not the only negative consumer outcome: manipulation seen across the world.** In 2012, Facebook, in collaboration with Cornell University and the University of California at San Francisco, conducted a psychology experiment on 689,000 of its users by manipulating their newsfeeds without their informed consent (BBC, 2014). The “massive-scale emotional contagion” revealed by the experiment raised the issue of the social media platform's ability to manipulate its users (Kramer et al., 2014). Over time, the issue of manipulation has only become more pertinent, as social media platforms are implicated in subverting the democratic process by using users' data to influence the outcome of elections. For example, during an under-

---

<sup>5</sup> Regulators must consider a similar trade-off with many new innovations and technologies. Wiedmaier-Pfister and Ncube (2018), for instance, show that mobile insurance holds the potential to rapidly scale, enhance efficiency and reduce the cost of insurance but has also resulted in new risks with implications for insurance supervisors. These are further captured in the International Association of Insurance Supervisors' (IAIS) Application Paper on the Use of Digital Technology in Inclusive Insurance (forthcoming 2018).

cover investigation by Channel 4 News, Mark Turnbull, the managing director of Cambridge Analytica Political Global, a political consultancy firm linked to Facebook, was filmed saying that they were responsible for running “just about every element of [Kenyan President Uhuru Kenyatta’s] campaign” (Crabtree, 2018). Although his comment cannot be verified, Turnbull’s claim – of having influenced the outcome of elections in Kenya – emphasises that consumers in developing countries are also at risk of manipulation through the unauthorised sharing and use of their data.

The ultimate objective of insurance policymakers, regulators and supervisors is to ensure positive and fair consumer outcomes, as highlighted in Insurance Core Principle 19 on Conduct of Business outcomes (IAIS, 2017). This requires that regulators aim to minimise both the risk of exclusion, due to data use restrictions, as well as the risk of consumer abuse from the increased use of consumer data. The first step is, therefore, to better understand the range of risks that affect insurance consumers and how they manifest. While this section provides a general overview of data risks to consumers, Section 3.1 below outlines a specific subset of primary potential negative outcomes to insurance consumers related to the use of their data. Section 3.1.2 then discusses the primary factors that cause these risks.

### 3.1 Potential negative consumer outcomes

The term “negative consumer outcome” refers to the ultimate harmful impact or negative effect on the consumer.

While this report focuses on the direct risks to individual consumers, it is important for regulators to consider the direct risks from data to insurance providers themselves, since these risks can have a dramatic indirect effect on consumers. If, for example, a systemic issue arises that compromises several insurers, it can damage consumer trust in the insurance sector in the long-term and render consumers reluctant to take up and use insurance (Chamberlain et al., 2009 and BaFin, 2018).

Six direct negative consumer outcomes that are applicable for insurers and the insurance industry are identified below, based on IAIS (2016), IAIS (2018a), IAIS (2018b), Institute of Actuaries of Australia (2016), McKee et al. (2015), The Smart Campaign (2016), The World Bank Group (2017), BaFin (2018) and stakeholder interviews:

- **Compromised safety and security.** The risk that a consumer is exposed or feels exposed to danger, which can result in physical or emotional hurt, injury or loss. In some cases, insurers collect data on the physical location of their clients by making use of a device that is fitted to clients’ vehicles. Discovery Vitality’s DQ-Track, for example, measures clients’ driving behaviour and can be used “to verify time and location of an incident” (Discovery Limited, 2018). If this type of data is inappropriately stored and/or shared or breached, there is potential for it to be used to physically endanger consumers.
- **Exclusion and lack of value.** The risk that consumers do not have access to financial products and services that meet their needs and are useful and affordable (The World Bank Group, 2018). One of the ways in which exclusion may manifest in the insurance industry is through the process of pricing high-risk consumers out of the market. Con-

sumers can be said to be “priced out of the market” when FSPs “set a price that the consumers are not willing to pay” to those consumers that “have proven to be unprofitable” (A2ii, 2016). In other words, insurers may charge certain high-risk individuals a premium that is so high that its effect is to discourage those individuals from taking up insurance. New types of data, such as the results of predictive genetic testing<sup>6</sup> (which may identify risk factors for diseases and genetic conditions) may also be used by insurers to identify which consumers are ideal candidates for “pricing out” (The Economist, 2017). The US-based artificial intelligence firm Lapetus Solutions enables insurers to use “smartphone self-portraits” or ‘selfies’ as part of their application process and additionally “to estimate people’s life expectancy” (Noiré, 2018). Unauthorised sharing and use of this data could lead to unfair discrimination.

Even if consumers are not fully ‘priced out’, new data and automated processes facilitate differential pricing to the extent that it could mean that certain customer segments face higher premiums or higher barriers to accessing insurance (BaFin, 2018). Analysing changes in the pattern of a consumer’s financial transactions, for example, may make it possible for providers to identify major changes in their client’s life (such as a pregnancy or divorce) which could cause their premiums to increase (BaFin, 2018). Moreover, machine-learning systems that receive biased and incomplete data as their inputs produce biased outcomes. For example, a model designed to predict the likelihood of a claim may advise an insurer to charge a higher premium to healthy individuals if it draws an erroneous connection – based on human beings’ past input – about the claims likelihood of people of a certain race or from a certain neighbourhood (De Brusk, 2018). Moreover, relative to the significance of the actual consequences of sharing their data and the real value that their data has, the value that consumers derive from insurance products may fall far short – an “asymmetry of information between a data supplier and a data user” that may be to the consumer’s detriment when providers can “extract the consumer surplus<sup>7</sup>” (BaFin, 2018).

Exclusion may also manifest when data cannot be used to its full potential. This may occur due to restrictions on the viability of the business model, including “requirements for data-driven decision-making, high upfront investment costs and trained experts”, partnership issues and regulatory restrictions (Hunter et al., forthcoming). The latter describes instances where regulation prohibits insurance providers from collecting, storing and using data that could be used to reach underserved or unserved individuals, thereby adversely affecting financial inclusion.

- **Reputational risk.** The risk that an individual’s character or good name is or is perceived to be impugned. Insurers may collect sensitive personal data on clients’ health, such as whether they suffer from stigmatised diseases or conditions. If the controls determining the protection of this data are insufficient, or if this data is shared or used without informed, voluntary consent, or if this data is breached, a client’s reputation –

---

<sup>6</sup> Conversely, insurers are worried that in instances where consumers have access to the results of predictive genetic testing and insurers do not, adverse selection may arise. In 2017, for example, the New York Times featured an article on a 77-year-old woman who, after discovering that she “inherited an ApoE4 gene that increases the risk of developing Alzheimer’s disease” bought a long-term care insurance policy (Kolata, 2017).

<sup>7</sup> Consumer surplus is defined as “the difference between the maximum price that a consumer is willing to pay for a product or service and the price that he/she actually has to pay on the market.” (BaFin, 2018)



and their ability to secure and retain their personal and professional position in society – may potentially be compromised.

- **Financial loss.** The risk that a consumer sustains economic harm or damage. This description also applies to situations where the failure of an insurance product leads to an individual being unable to access another service, such as education or health-care. For example, a data error could result in a change of the terms of an individual's medical aid, thereby prohibiting the consumer from claiming in order to undergo a critical medical diagnostic procedure. Moreover, a data error could result in a change in the terms of an individual's education policy, which could lead to it not paying out when the consumer expects and requires it. In January 2018, it was reported that it is possible to buy user details of the Indian biometric system, Aadhaar, which allow the purchaser to "enter any Aadhaar number into the UIDAI [Unique Identification Authority of India] website and get access to user information including name, address, photo, phone number and email address" (BBC, 2018). By February 2018, at least six cases in which money was "fraudulently withdrawn from bank accounts using the customers' Aadhaar number" had been reported – involving a total sum of about INR15 million or USD218,865 (Bennett Coleman and Company 2018).
- **Loss of privacy.** The risk that a consumer's right to determine who has access to and use of personal information, physical spaces and bodies is compromised or violated (Moore, 2008). Insurers collect personal information from their clients (such as their name, address and contact details) and clients may share financial information with their insurers. If insurers do not have sufficient storage protocols in place or if their data is breached, the privacy of consumers could be compromised. In June 2018, confidential emails between South African FSP Liberty Holdings and its clients were hacked. Although a spokesperson for the company said that "no clients had been affected by the hack", the breach illustrates the extent to which FSPs are targeted for cyber-attacks that could lead to a loss of consumer privacy (Niselow, 2018).
- **Manipulation.** The risk that consumers' behaviour and decision-making is influenced to their detriment and hence that their autonomy is intentionally hindered (Noggle, 2018). Since manipulation does not occur through either explicit coercion or through rational persuasion, it is a discreet means of potentially eliminating options that consumers have access to, which could cause consumers to allocate their resources in a way that is to their detriment<sup>8</sup>. This negative consumer outcome is closely linked to the "nudge" described in IAIS (2018a), where insurers and intermediaries target consumers "without them being aware... through specific targeted search engines or click on sponsored links" – practices which often suffer from "a lack of transparency".

**It is important to distinguish between negative consumer outcomes and the causes of those outcomes.** While the negative consumer outcomes describe the harmful impact on consumers, the drivers cause the negative consumer outcomes to occur. The distinction between

<sup>8</sup> Manipulation, as negative consumer outcome, clearly has a harmful effect on consumers. Nevertheless, it is important to note that manipulation may also describe a positive consumer outcome, which involves the implementation of behavioural science interventions to influence individuals to make decisions that are more aligned to their needs. For example, CityMile, a Brazilian insurtech firm, offers a "usage-based insurance platform" that enables insurance providers "to collect data on driving behaviour with the end-goal of incentivising drivers to change their risky behaviour" (Smit et al., 2017).

outcomes and risk drivers can be illustrated by considering the example of data breaches, which involve the theft of consumer data. The ultimate impact of data breaches on consumers depends on what the stolen consumer data is used for, such as identity theft and/fraud. Data breaches are thus considered a driver of these negative consumer outcomes and, as such, will be discussed in more detail in the next section.

### 3.1.1 The data value chain

**Risks emerging along the data value chain.** The risks that arise to consumers and particularly the drivers of those risks, are directly linked to flaws in one or more of these stages in the data value chain. Figure 3 illustrates the different stages of the data value chain, namely collection, storage and use. Each of these stages is explained below based on research from Lyko et al., 2016 and GSM Association, 2018:

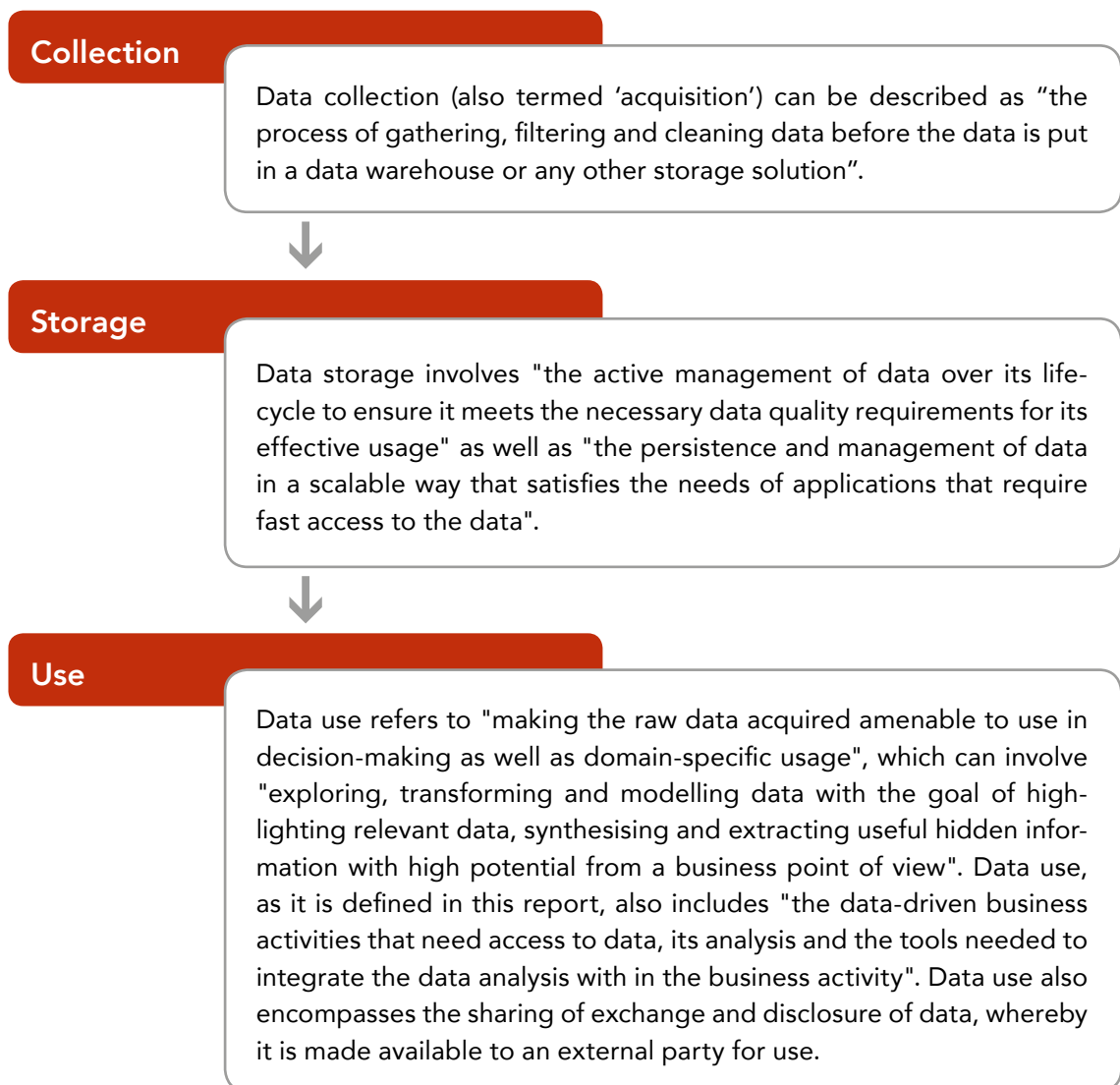


Figure 3: The data value chain | Source: Author's own based on Lyko et al. (2016) and GSM association (2018)

### 3.1.2 Risk drivers

Five primary drivers of negative consumer outcomes deriving from the collection, storage and use of data are identified. These risk drivers detailed below are not mutually exclusive and do not map onto the outcomes on a one-to-one basis. For example, a failure of controls could easily result in compromised safety and security, financial loss and loss of privacy, each of which outcome could just as easily arise as a result of a data breach. However, often in combination, these are identified as the five primary drivers of the negative consumer outcomes.

- **Inadequate data governance and controls.** This risk driver may occur due to the absence – within an industry, or individual business – of a culture and a strategy that explicitly considers the data risks to consumers and actively seeks to limit the negative outcomes throughout the processes in which it engages<sup>9</sup>. This risk driver may arise as a result of a lack of, or inadequate protocols determining, for example, how consumer data is stored and who is permitted to access it. To protect the privacy and ensure the security of consumer data, it can, for example, be encrypted and/or anonymised. In instances where insurers do not have protocols in place that allow only authorised employees to have access to unencrypted and unanonymised consumer data, negative consumer outcomes may more easily arise due to the actions of malicious or incompetent insiders than when access to consumer data within an organisation is restricted.
- **Error.** This risk driver describes instances where a consumer's data unintentionally deviates from truth or accuracy. If, for example, during collection, a consumer's health data is erroneously captured (indicating that they suffer from a specific disease when they do not, or that they possess a certain gene mutation when they do not), this information could be used to charge the consumer a prohibitively high premium, thereby excluding them from the insurance market.
- **Involuntary or uninformed consent.** An insurer, or any FSP, may be said to have obtained voluntary informed consent when "individuals agree to provide data ... and demonstrate an understanding of the implications of providing such data" (Nunan and Yenicioğlu, 2013). Involuntary or uninformed consent, as a risk driver, thus describes instances where consumers either do not agree to have their data collected, or do not fully understand the implications of having their data collected. It is noteworthy that even in instances where consumers give their informed and express consent that it is not always strictly voluntary if the consequence is not having access to the product. To this end, Recital 42 of the GDPR states that "[c]onsent should not be regarded as freely given if the [consumer] has no genuine ... choice or is unable to refuse or withdraw consent without detriment."
- **Unauthorised sharing and use.** Instances where consumer data is shared with, exposed, or revealed to third-parties without consumers' full consent or where consumer data in an external party's custody (or under its control) is used for purposes beyond that for which the information was collected, or beyond a use consistent with

---

<sup>9</sup> These controls need to be in place not just for insurers but for any entities that hold insurance consumer data. For example, in the US, some insurers pool data in the legal equivalent of credit bureaux, e.g. the Medical Information Bureau, for insurance underwriting. Similarly, in Kenya the Integrated Population Registration System (IPRS), launched in 2015, connects various government departments and pools all personal data that is centrally held about an individual.

that purpose may be described as “unauthorised sharing and use” (The World Bank Group, 2017). Unauthorised sharing and use occur when, for example, insurers share their clients’ contact details with third-parties, who then use that information for marketing purposes, without first obtaining the insurance clients’ permission. Consumer data may also be used to discriminate against individuals, which involves treating them in an unjust or prejudicial way, on the grounds of, for example, race, age, sex or medical history.

- **Data breaches.** This risk driver involves instances where a consumer’s data is acquired, transferred, possessed, or used “in an unauthorised manner, with the intent to commit, or in connection with, fraud or other crimes” or where, a consumer’s data ‘vanishes’ as a result of, for example, mechanical or power failure, physical damage, malware, viruses, human error or theft (OECD, 2008)<sup>10</sup>. Data breaches can occur even if insurers have appropriate storage protocols in place; as such, they can be distinguished from “inadequate data governance and controls” as key driver, on the basis of the fact that the latter describes instances of negligence.

Figure 4 shows the full list of negative consumer outcomes and the drivers of these outcomes identified.

**Regulators can act to either mitigate the negative consumer outcomes directly or act to prevent the risks from ever happening by understanding and preventing the drivers.** Regulatory responses to these risks tend to fall into two broad categories which, while not mutually exclusive, focus either on directly addressing the negative consumer outcomes or dealing with the drivers of those risks to reduce the likelihood and/or effect of the risks occurring.

- **Address the negative consumer outcomes directly.** Focusing directly on addressing the negative consumer outcomes requires a consumer-centric decision-making culture among the collectors, storers and users of data. Treating Customers Fairly (TCF) in South Africa, for example, details six customer outcomes that govern the way “regulated financial firms (including financial advisers)” treat their clients “at all stages of their relationship with the customer, from product design and marketing, through to the advice, point of sale and after sale stages” (FSCA, 2018). Applying these principle-based requirements to the data risk environment does not represent an attempt to deal with the causes of the risks, but rather places the onus on providers to operate in a way that best serves their consumers’ interests. Such approaches offer broad powers to regulators to hold firms accountable that fall foul of these requirements, including consumer harm due to inappropriate data collection, storage or use. The focus is less on providing explicit restrictions to what data can be collected or how it can be used, but rather on applying principles of how it is appropriate to treat consumers and their data.

---

<sup>10</sup> Data breaches is often captured within cybercrime or cyber risk. CRO Forum (2014), as cited in IAIS (2016), defines “cyber risk” as “any risks that emanate from the use of electronic data and its transmission, including technology tools such as the internet and telecommunications networks. It also encompasses physical damage that can be caused by cybersecurity incidents, fraud committed by misuse of data, any liability arising from data storage, and the availability, integrity and confidentiality of electronic information – be it related to individuals, companies, or governments.” This definition therefore includes a number of the risk drivers identified in this paper; it has been decided to split out some of the components, given the focus of this report.

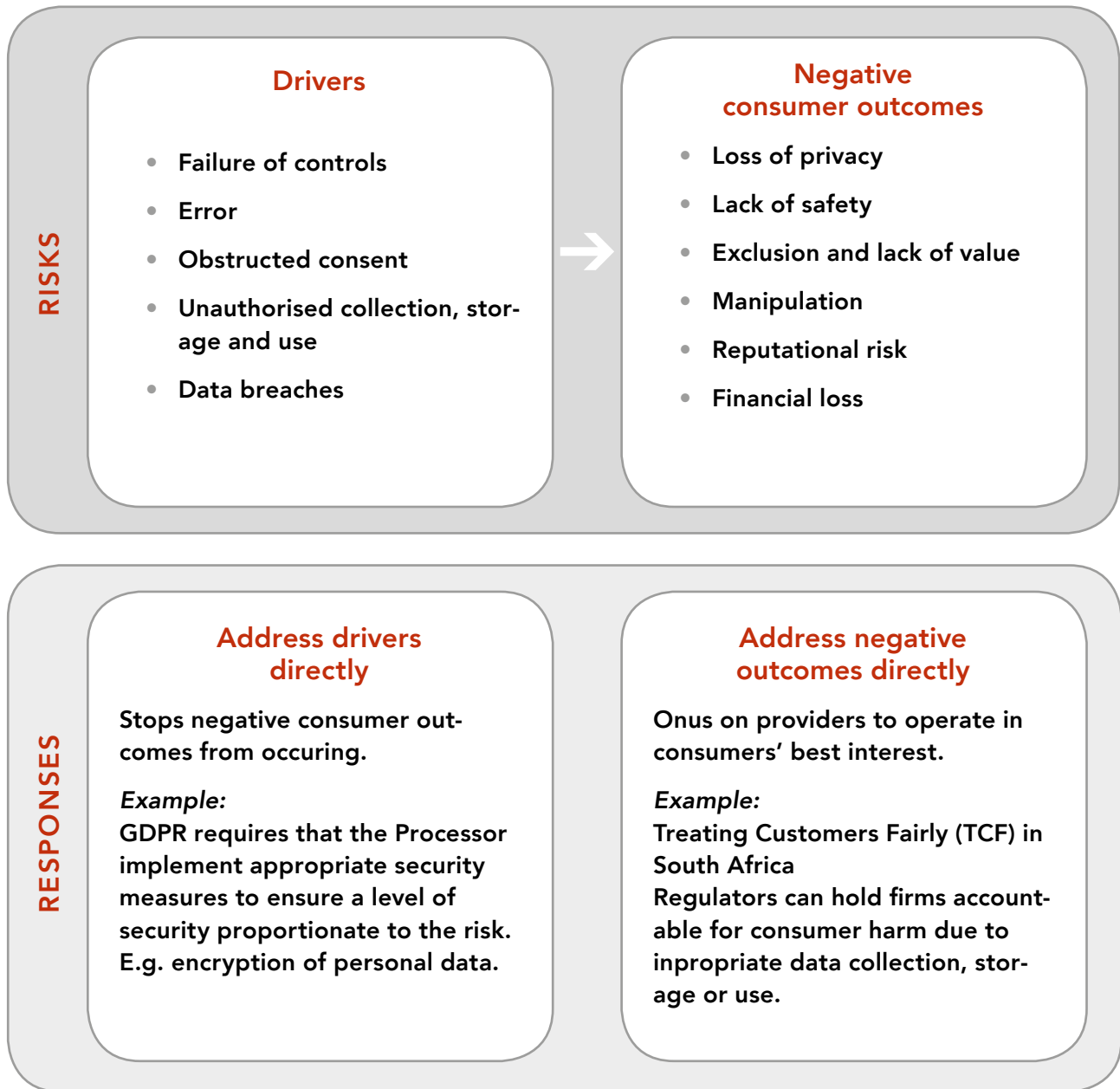


Figure 4: Negative consumer outcomes, their drivers and the potential nature of regulatory responses | Source: Authors' own

- **Prevent the risk drivers from occurring.** Alternatively, given that the occurrence of the risk drivers leads to negative consumer outcomes, regulators can act to prevent the risk drivers identified above from occurring. The requirement of encryption and holding data controllers liable for contravention of minimum security requirements are regulatory means through which inadequate controls, as risk driver, can be addressed. For example, the EU, under GDPR, requires the encryption of personal data. Article 32 of the GDPR requires that the processor implement appropriate security measures – considering the cost, nature, and scope of the implementation, as well as the likelihood that the rights of individuals may be severely affected. The measure implemented must be appropriate to ensure a level of security proportionate to the risk; one of these security measures is the encryption of personal data.

## 4. HOW CAN INSURANCE REGULATORS RESPOND?

The insurance regulator must confront the risks that arise from the use of consumer data in the insurance industry. However, the issue of data protection is also far broader than just the insurance (or financial) sector. The nature of the regulator’s response is guided by society’s overall approach to regulating the protection and privacy of consumer data, which is determined by the policymaker. The policymaker’s approach must, in itself, appropriately conform with broader societal norms.

=====

### BOX 1 | Distinguishing between data protection and the right to privacy

A person’s right to have their personal data protected stems from the broad human right to privacy. Privacy commonly includes but is not limited to the rights not to have your home searched or communications intercepted without legal basis, and it is considered by many countries to be a fundamental human right worthy of constitutional protection. Data protection legislation is used to give effect to an aspect of the right to privacy. In the absence of data protection legislation, the legislative protection of the right to privacy provides a means through which personal data may be protected.

Terminology around data protection and privacy has become opaque with different jurisdictions referring to the same terms in different ways. For example, some jurisdictions refer to data protection while others refer to privacy when they mean information privacy and not the human right to privacy. This report uses the term “data protection and privacy” in an attempt to make the term relatable to insurance regulators from all jurisdictions as the ultimate objective of the report is not to unpack the nuances of data protection in general but rather to provide guidance to the insurance regulator of its role in this space.

=====

**Insurance regulators must decide on their approach based on mandate, market and regulatory context and existing constraints.** The insurance regulator’s challenge is to determine the most appropriate response to the risks arising from the collection, storage and use of consumer data. In other words, the insurance regulator’s response must result in positive outcomes for consumers – provided that it is within its mandate to achieve, in alignment with the existing market context and feasible within the overall approach determined by the policymaker.

It is clear that each context, and therefore each solution, will differ. No one size fits all. In the remainder of this report, we therefore aim to provide some guidance for each regulator to identify its current position when dealing with these issues and what its options are – enabling it to identify its ‘size’ and find a good fit. Figure 5 illustrates these core considerations for regulators, each of which is discussed below.

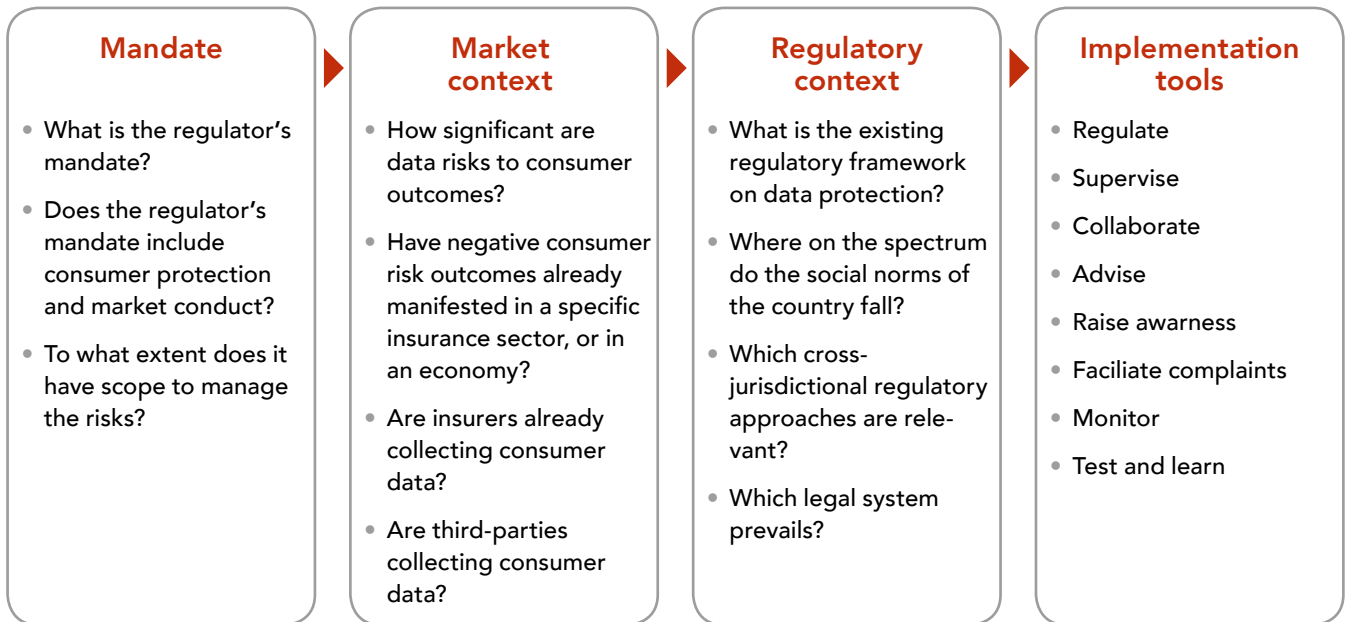


Figure 5: Regulators’ decision-making tree: considerations for insurance regulators in dealing with consumer risks related to data | Source: Authors’ own

## 4.1 Mandate

**Mandate.** What is the regulator’s mandate? Regulators are usually created by Acts of Parliament that also define their mandate and scope of activities. The legal mandate of a regulator determines the type of activities it can engage in, as well as which interventions it is able to make. Regulators with no consumer protection or market conduct mandate would therefore not have the mandate to address the risks to consumers arising from the collection, storage and use of data. This, however, applies to few insurance regulators as most insurance regulators are required to consider the consumer protection risks. Therefore, even in cases where data protection falls beyond the jurisdiction of the insurance regulator, such as where there is an established data regulator under an omnibus legislative approach, the insurance regulator will still have the mandate to protect consumers from risks that arise in their industry, including when they arise from data. Section 5.1 details the potential tools available to regulators in this context.

Regulators, like India’s Insurance Regulatory and Development Authority (IRDA), also have a third explicit mandate: to encourage market development (beyond prudential and market conduct objectives). For these regulators, the need to mitigate the risks related to consumer data collection, storage and use (as discussed in Section 3 above) is an explicit legal imperative. However, even regulators without an explicit market development mandate should give some consideration to balancing the need to protect consumers against the need to encourage innovation through increased data use by providers and thereby address the risk of exclusion.

## 4.2 Market context: assessing how important data risks are in the market

**Market context.** Provided the insurance regulator has the mandate to deal with consumer data protection and privacy risks, the next relevant consideration is current market context. Market context can be described as the circumstances or setting within which insurance sector players and consumers interact. An awareness of these parameters allows insurance regulators to determine the level of priority they should assign to responding to the risks. The factors that constitute market context, as ‘consideration’, can be streamlined into three questions:

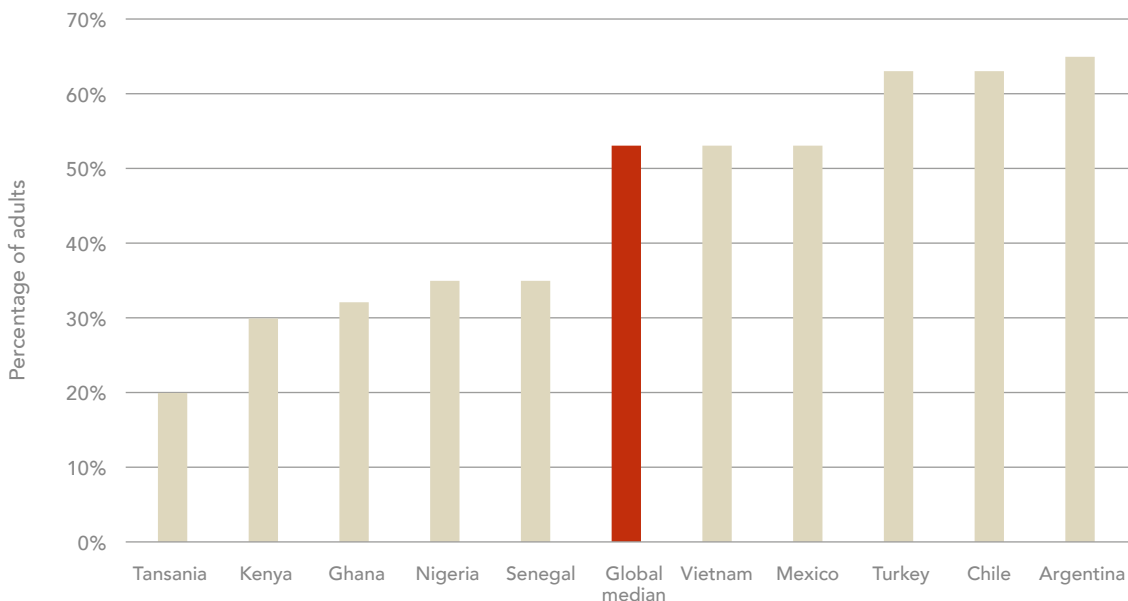
- 1. Have the negative consumer outcomes identified in Section 3.1 already manifested in a specific insurance sector, or in an economy?** Naturally, insurance regulators in whose jurisdictions these negative consumer outcomes have already occurred are under more immediate and urgent pressure to act. The leap from financial loss affecting consumers in another sector to financial loss affecting consumers of insurance is not far; as such, monitoring the incidence of data risks occurring in other sectors of an insurance regulator’s economy can serve as an early-warning system of the risks that insurers may be likely to experience in the near future. In 2017, 1,453 data breaches were recorded in the US, many of which occurred in the financial sector (Gemalto, 2018). For example, Equifax, one of the three main credit reporting agencies in the US, experienced a breach which compromised the personal information of 143 million consumers (Gressin, 2017). Although only seven breaches were recorded in South Africa in 2017, the breaches of the FSPs Old Mutual and Liberty Holdings (in 2017 and 2018 respectively) highlights the potential for South African insurance providers and their clients to be victims of data-related risks.
- 2. Are insurers already collecting consumer data?** The extent to which insurers already collect, store and use consumer data is a pertinent market context parameter for insurance regulators to consider. It can be used to gauge the likelihood of the aforementioned negative consumer outcomes occurring, even in instances where these risks have not yet been seen in the insurance industry or economy more broadly. Although the majority of negative consumer outcomes have been reported in developed countries, insurers in developing countries are already collecting and using significant amounts of data. For example, based on interviews with 15 insurance providers in developing countries, Hunter et al. (forthcoming) compiled a list of 93 client data<sup>11</sup> use cases. They found that a variety of client data is already being collected through multiple different channels and used to inform innovative insurance providers’ activities.
- 3. Even if consumer data is not being collected by players in the insurance industry, are third-parties collecting consumer data?** Even if insurers are not currently engaging in the data value chain to a significant extent, the extent to which third-parties collect, share and use consumer data also constitutes a pertinent market context parameter. Social media platforms and MNOs, for example, have significant market power and are already acquiring vast datasets on consumers in emerging markets, which insurers

---

<sup>11</sup> Client data is defined as “data that provides insight into an individual client or the characteristics of a segment of clients, who they are, what they need and how they behave” (Hunter et al., forthcoming).



could leverage in future. This market context parameter may be determined by considering the extent to which a country's population is interconnected – for which social media use and mobile phone, smartphone and internet penetration, respectively, can be considered proxies. For example, according to the Pew Research Center's (2018) Spring 2017 Global Attitudes Survey, the global median percentage of adults who use social networking sites is 53%. As illustrated in Figure 6, social media use in numerous developing countries, including Argentina, Turkey, Chile, Vietnam and Mexico, exceeds or equals this median number (Poushter et al., 2018). The use of social networking sites among adults in countries in sub-Saharan Africa – such as Nigeria, Senegal, Ghana, Kenya and Tanzania – is generally below the median at present (Poushter et al., 2018). Nevertheless, it is predicted that, by 2025, unique mobile subscriber penetration (as a percentage of the population) across sub-Saharan Africa will have increased to 52% from 44% in 2017 and that mobile internet penetration will have increased to 40% in 2025 from 21% in 2017 (GSM Association, 2018).



**Figure 6: Usage of social networking sites** | Source: Authors' own, based on Poushter et al. (2018)

Even in the most nascent insurance markets, a significant portion of people – including most existing insurance users – are connected to the internet and using social media, which means that their personal information is already being collected, stored and used. As such, even insurance regulators in whose jurisdictions negative consumer outcomes have not yet been reported may still be advised to determine how significant data risks are for consumers. Ultimately, an understanding of market context will determine the urgency and nature of action to be taken to ensure positive consumer outcomes.

### 4.3 Regulatory context: omnibus, sectoral or no data protection legislation

**Regulatory context.** The cross-sectoral nature of the negative consumer outcomes and their drivers (discussed in Sections 3.1 and 3.1.2 respectively) complicates the role of any given regulator as data protection, which stems from the right to privacy<sup>12</sup>, is a broader societal consideration. It will affect consumers within its jurisdiction; however, since the regulation of data is applicable across sectors, it may be regulated by another authority. Insurance regulators with the mandate to act in a market that requires prompt action need to also consider what the current policy-determined approach to consumer data protection and privacy is. A country's existing legislative approach to consumer data protection and privacy will determine the scope of responsibility the insurance regulator has, the constraints within which it works and ultimately the regulatory tools which it has at its disposal to achieve its objectives to effectively protect consumers from the range of data-related risks.

**Three models of data regulation.** The overall approach to dealing with the risks that are arising from data collection, storage and use across society is determined by the policymaker. Three distinct legislative approaches have been observed globally, namely omnibus, sectoral, or no legislation in place. The insurance regulator is unlikely to have a role in determining which legislative approach is selected, but it is critical to understand under which legislative approach it operates, since that directly determines what may be feasible and required by the individual regulator. These three legislative approaches are expanded on in detail below:

**Omnibus.** This approach consists of an overarching data privacy framework, covering multiple industries across sectors. The framework acts as a single source of protection for personal data that applies at most (if not all) levels. It generally takes the form of a single national data protection law with regulations that flow from it, enforced by a data protection regulator or authority. In jurisdictions that have implemented a legislative approach to data protection, the omnibus approach is by far the most commonly implemented. A well-known example of such an approach is the EU's GDPR<sup>13</sup>, but similar approaches have been implemented all over the world, including Argentina, Australia, Mexico and Morocco, among others.

**Omnibus approach: benefits and drawbacks.** The benefits of an omnibus approach include that it: a) caters for cross-sectoral institutions given that they are regulated by only one data protection law, b) creates uniformity and certainty surrounding data protection, given that there is one uniform standard, and c) minimises gaps, given its wide application. The drawbacks of an omnibus approach are: a) regulations can be somewhat vague and minimalistic, given that there is only one uniform standard that applies across sectors, b) risks that arise uniquely to a specific industry, such as the insurance industry, are not necessarily addressed and c) if an omnibus legislative approach has been adopted but the implementing data pro-

---

<sup>12</sup> The right to have personal data protected stems from the right to privacy. The right to privacy, which commonly includes the rights not to have your: a) home searched and b) communications intercepted without legal basis, is considered by many countries to be a fundamental human right enshrined in the constitution. Data protection legislation is used to give effect to an aspect of the right to privacy. In the absence of data protection legislation, the legislative protection of the right to privacy provides a means through which personal data may be protected.

<sup>13</sup> In May 2018, the EU General Data Protection Regulation (GDPR) replaced the EU Data Protection Directive that was adopted in 1995. Unlike the latter which was implemented differently by each member state, the GDPR does not require additional domestic legislation.

tection agency is still young or has not been established at all, then consumer data risks are strictly within the data protection regulator’s mandate, rather than the individual sectoral regulator’s, but may not be effectively enforced.

**Sectoral.** In the absence of an overarching data privacy framework, this legislative approach consists of numerous singular laws that apply specifically to a given industry or sector and regulate data protection in that particular industry or sector. A well-known example of such an approach is the US sectoral approach to data protection and privacy, where many of its 50 states have their own related laws (see Appendix A). Furthermore, even within states, various sectors are governed by separate data protection and privacy laws.

**Sectoral approach: benefits and drawbacks.** The main benefit of a sectoral approach derives from the fact that it is sector-specific and therefore more nuanced, since it can be tailored to each sector’s particular and unique needs and may thus be more appropriate for the risks that arise within that sector. The drawbacks of a sectoral approach are: a) the differing regulations across numerous sectors can, at times, be contradictory, which creates uncertainty, b) cross-sectoral institutions face complex problems while trying to navigate vastly different laws that are enforced by multiple regulators, and c) gaps are easily formed between where the scope of one sector’s regulation ends and the next begins.

**No regulation.** Figure 7 illustrates that of UN member countries, 21% do not have legislation in place that addresses data protection and privacy (UNCTAD, 2018). In Africa and Asia, this number rises to over 60% (UNCTAD, 2018). Of UN member countries, 10% have draft legislation pending, while no data is available on 12% of UN member countries. In the absence of any existing data protection regulation, the onus likely falls on sectoral regulators to address the risks that arise to consumers within their sector from the collection, storage and use of consumer data, at least until comprehensive regulation is promulgated.

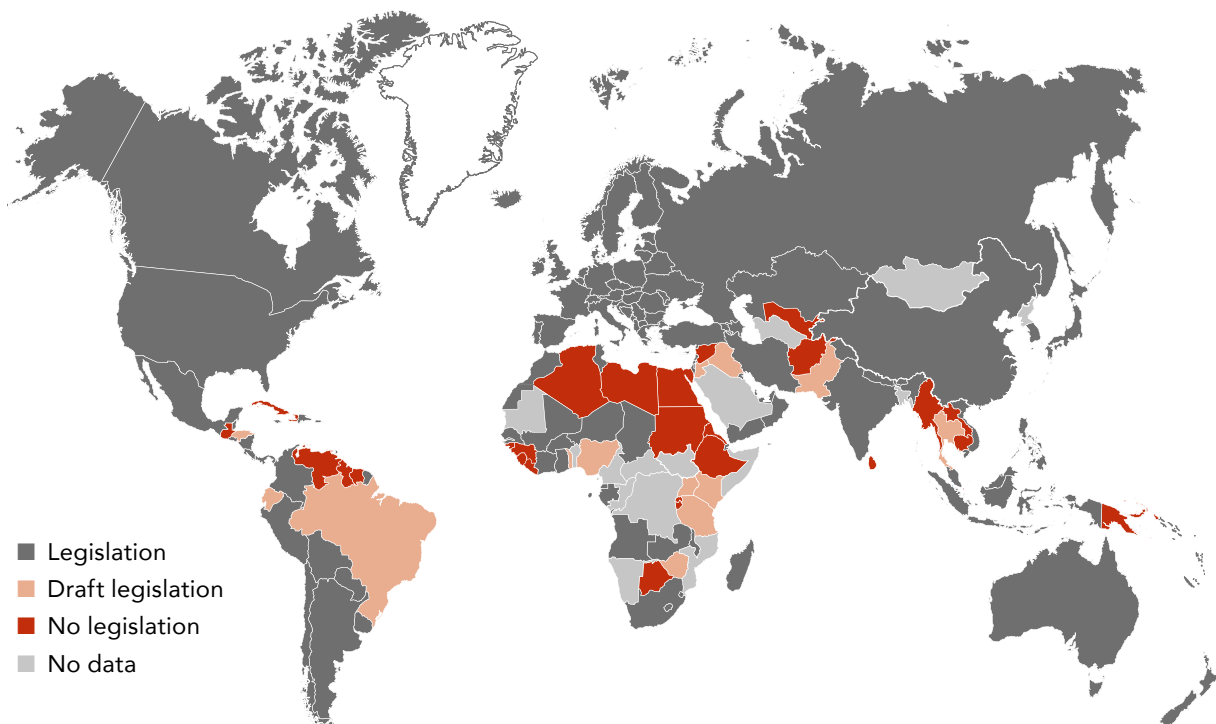


Figure 7: Data protection and privacy legislation worldwide | Source: UNCTAD (2018)

**Societal norms determine the policy direction of data regulation.** The design and content of each of these legislative approaches will differ to comply with a country's specific context. While a specific approach may best ensure the desired outcomes in one jurisdiction, that approach may not be suitable or effective in another. For an individual sector regulator, like the insurance regulator, the overall legislative approach to regulating consumer data protection and privacy can be considered as a pre-existing contextual situation within which it must operate. Nevertheless, it is critical to understand the nature of a regulator's contextual situation and why it arises. Box 2, expands on the differences in social norms across countries and the implications for the regulation of consumer data.



**BOX 2 | Societal norms**

**Societal norms differ across countries and are derived from written and unwritten sources.**

Different countries have different norms that underpin their societies. For instance, where some societies place citizens' individual rights as paramount, others place greater weight on enhancing benefits to the wider community, with less focus on the individual. A society's norms are derived over time and determined in large part by each individual society's unique history. These norms are derived from a variety of sources – some may be encapsulated either expressly (such as in written constitutions<sup>14</sup>) or implicitly (drawn from sources like historical experiences<sup>15</sup>).

Answering the question of how to regulate data privacy stems directly from these societal norms, as the nature and scope of data regulations will be determined directly by a society's norms related to fundamental concepts of individual privacy. New regulations should thus be consistent with the society's norms.

**Some of the key common distinctions observed across societies include their views on and approaches to: individual versus group rights, libertarianism versus paternalism and the horizontal versus vertical application of rights.** These ideologies are not necessarily mutually exclusive, and different societies would be positioned across a spectrum. Nevertheless, it remains important to establish where a society's norms fall on the spectrum to determine adequately the scope for and focus of data protection regulation. More detailed information on some of the key common distinctions is discussed below.

- **Individual versus group rights.** Societies tend to place varying emphasis on and favour for either individual rights or group rights. The distinction can be somewhat contentious, but both stances have trade-offs and as such are the culmination of a society having weighed up and balanced the interests of individuals vis-à-vis groups. Group rights, also known as collective rights, are held by a group and not by the individual members that make up the group, while individual rights are held by individuals themselves. The EU and USA are examples of societies that place relatively greater emphasis on the rights of the individual. By contrast, group rights are given prominence in China, where individuals are considered to benefit directly from the rights afforded to groups. The different stances of these societies may manifest in the varying ways in which data is regulated, and which components of the data value chain are more heavily regulated.

- **Libertarianism versus paternalism.** Libertarianism encourages minimal intervention from a state into the lives of its citizens, while paternalism encourages intervention by a state into the lives of its citizens in order to benefit and protect them. The US government is an example of a more libertarian state, which places emphasis on the freedom and liberty of its citizens. The EU, by contrast, follows a more paternalistic approach – actively engaging in intervention into EU citizens’ lives to protect them. A manifestation of libertarianism and paternalism can be seen in a state’s translation of the right to privacy into a negative or positive right. Negative rights can be fully enjoyed if the government abstains from interfering, while positive rights require explicit action from the government to enable their full enjoyment.
  - **Horizontal versus vertical application of the right to privacy.** Vertical application applies the right to privacy in a manner which benefits individuals over institutions, which are usually companies, but may also include government. Vertical application protects entities with less power from being exploited by entities with more power. Nevertheless, vertical application offers basic or limited protection. Horizontal application applies the right to privacy for individuals in view of one another. It is commonly used in conjunction with vertical application to offer comprehensive protection to individuals – in other words, not only protection from institutions but also from other individuals.
- =====

The critical implication is that any data regulations implemented within a society must be consistent with the existing norms within a society. Societal norms therefore determine the nature and scope of data regulations that can be implemented within that society, albeit not the specifics of the regulations. Two additional factors contribute to the overall regulatory context as it pertains to the regulation of consumer data protection and privacy.

**Cross-jurisdictional regulation.** At the cross-country level, regional regulations and trade agreements may have a direct bearing on the local approach to data protection and privacy regulation. With GDPR coming into operation, the EU has set a de facto global standard for data protection by giving its provisions extra-territorial application. In other words, the provisions of the GDPR apply to the processing of EU citizens’ data, irrespective of the location of the data processor<sup>16</sup>. The implication is that all countries must consider the level of consistency of their local approach with GDPR.

<sup>14</sup> Article 6(A)(ii) of Mexico’s Constitution, for example, goes as far as to enshrine specifically the right to private and personal data protection, confirming the importance of privacy as a societal norm in Mexico.

<sup>15</sup> For example, in Germany, the government did not conduct a census of the population for approximately 25 years because of the public reaction to the previous census, which was held in 1987 (Zensus, 2011 and Spiegel Online, 2011). The citizens took to the streets to voice their privacy fears and some even boycotted the survey. This occurred shortly after a lawsuit in the early 1980s, which related to privacy issues that eventually led to the cancellation of the planned 1983 census. Privacy concerns likely stem from Germany’s history, where census data was used to target Jews in the Nazi era (Cohn, 2013).

<sup>16</sup> According to Article 4(8) of the GDPR, processor “means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller”.

While trade bloc requirements may or may not include explicit data protection-related provisions, countries may be pressured into heightening their data protection measures in order to ensure that any privacy concerns of their trading partners are assuaged. This is especially relevant to smaller and/or developing countries that rely heavily on trade. To illustrate, Côte d'Ivoire only allows for data to move across its border to jurisdictions that have data privacy regulations in place, placing the onus on any foreign regulators that would like to export services that use consumer data to ensure that they have data privacy regulations in place. Conversely, Rwanda's implementation of the data sovereignty principle, through its National Data Revolution Policy of 2017, requires all consumer data collected in Rwanda to be retained locally.

**The domestic legal system.** The overall legal system of each country – whether a common law or civil law structure is in place – has potential implications for the regulation of consumer data protection and privacy. One of the most pertinent aspects of a common law legal system is that the law can be developed through case outcomes. This differs from a civil law legal system, where the law is developed by means of formal amendment of legislation to reflect a new position or development. Pakistan provides an example of where the content of the right to privacy has developed over the years by way of case outcomes, without explicit changes to regulation being required. Pakistan does not currently have direct data protection legislation. However, Article 14(1) of the Pakistan Constitution enshrines the right to privacy and, over the years, the courts have developed precedent in this regard<sup>17</sup>.

---

<sup>17</sup> In 1996, in *Benazir Bhutto versus Federation of Pakistan*, the Supreme Court found that the widespread practice of the surveillance of judges, politicians, military and government officials' communications was unlawful and required authorisation by Supreme Court judges. In 2004, the Lahore High Court ruled in *M.D. Tahir versus Director, State Bank of Pakistan* that it was illegal to collect ID numbers and other information of bank account holders without an allegation of wrongdoing, finding in favour of financial privacy. Courts are thus increasingly recognising the importance of privacy and developing the constitutional right by means of case precedent (Hosein, 2011).

## 5. IMPLEMENTATION TOOLS

Insurance regulators' main objective is to avoid negative consumer outcomes from the collection, storage and use of consumer data.

Within an omnibus legislative approach, the data regulator will play an important role in helping to achieve these objectives. However, the insurance regulator must still ensure that data risks are appropriately dealt with within the insurance sector and has an important and complementary role to play to address gaps in the omnibus framework for their sector. Within a sectoral legislative approach or where no explicit legislative approach has been implemented, the onus is on the insurance regulator to ensure that it implements appropriate tools to achieve these objectives. Two broad, and complementary, regulatory approaches are observed to achieving these objectives: directly addressing the negative consumer outcomes or addressing the drivers of risks.

**Addressing negative consumer outcomes.** Regulatory strategies that target market conduct outcomes, like TCF, aims to fundamentally align providers' treatment of consumers with improved outcomes to consumers. TCF in South Africa, for example, details six customer outcomes that govern the way "regulated financial firms (including financial advisers)" treat their clients "at all stages of their relationship with the customer, from product design and marketing, through to the advice, point of sale and after sale stages" (FSCA, 2018). As in South Africa, TCF in the UK is considered to be "an integral part of... business culture" (FSA, 2007). Applying these principle-based requirements to the data risk environment does not represent an attempt to deal with the causes of the risks (an example of which would be restricting the collection of data), but rather places the onus on providers to operate in a way that best serves their consumers' interests. Such approaches offer broad powers to regulators to hold firms accountable that fall foul of these requirements, including consumer harm due to inappropriate data collection, storage or use but, as these are not data protection-specific, do not provide specific guidance or rules on how to protect consumer data. As a result, it would be more challenging under such an approach to prove and sanction firms that do not protect consumers' data compared to data protection specific regulation.

**Preventing risk drivers.** Alternatively, regulators can consider measures to limit the likelihood and effect of the risk drivers, identified in Section 3.1.2, occurring. Limiting the likelihood and effect of the risk drivers will, in turn, limit the manifestation of the negative consumer outcomes. Such regulation makes it easier to hold providers accountable that introduce or do not sufficiently prevent data related risks from affecting their consumers.

Table 1 in Box 3 summarises the examples of regulatory responses to address risk drivers. Such preventative regulation is currently implemented mostly by data regulators. Insurance regulators within an omnibus legislative approach must consider whether the existing data protection legislation effectively covers these or if there are additional gaps they should consider. Insurance regulators within a sectoral legislative approach or where there is no explicit approach, can apply these same regulatory responses to their specific sector. These examples are discussed in Box 3. The remainder of this section details the range of tools, beyond regulation, available to regulators to address the risks related to consumer data protection and privacy.

=====

**BOX 3 | Preventing risk drivers**

Risk driver	Description	Regulatory response	Example(s)
<b>Inadequate data governance and controls</b>	Absence of a culture and a strategy that actively seeks to limit negative consumer outcomes throughout the data value chain. Includes lack of, or inadequate protocols determining, for example, how consumer data is stored.	Mandated encryption of personal data	EU (GDPR)
		Liability specified in the event of a breach	Argentina
<b>Error</b>	Where a consumer's data unintentionally deviates from truth or accuracy.	Organisations required to allow individuals to correct data inaccuracies	Canada
		Mechanism for correction	Australia
<b>Involuntary or uninformed consent</b>	Where consumers either do not agree to have their data collected, or do not fully understand the implications of having their data collected.	Voluntary consent	Ukraine
		Informed consent	Israel
<b>Unauthorised sharing and use</b>	Where consumer data is acquired, transferred, possessed or used for purposes beyond that for which the information was collected, or beyond a use consistent with that purpose.	Minimal data collected	EU (GDPR)
		Time stored	Angola
		Distinguish personal and sensitive	EU (GDPR)
<b>Data breaches</b>	Where a consumer's data is acquired, transferred, possessed or used in an unauthorised manner, with the intent to commit or in connection with fraud or other crimes or where, a consumer's data 'vanishes' (as a result of, for example, mechanical or power failure, physical damage, malware, viruses, human error or theft).	Breach notifications to the data subject required	Mexico

**Table 1: Observed regulatory responses to the drivers of risk** | Source: Authors' own

- **Inadequate data governance and controls.** The requirement of encryption and holding data controllers<sup>18,19</sup> liable for contravention of minimum security requirements are regulatory means through which inadequate controls, as risk driver, can be addressed.

*The EU, under GDPR, requires the encryption<sup>20</sup> of personal data. Article 32 of the GDPR requires that the processor implement appropriate security measures – considering the cost, nature, and scope of the implementation, as well as the likelihood that the rights of individuals may be severely affected. The measure implemented must be appropriate to ensure a level of security proportionate to the risk; one of these security measures is the encryption of personal data.*



*Argentina's Personal Data Protection Law specifies liability in the event of a breach.* According to the Personal Data Protection Law<sup>21</sup>, both the transferee and transferor are held jointly and severally liable for any breach of data protection obligations (DLA Piper, 2017).

- **Error.** Inaccuracies in data can be addressed by means of regulation requiring not only care in the collection of data, but also a mechanism in terms of which inaccuracies can be corrected on the demand of the consumer.

*In Canada and Australia, individuals have the right to correct inaccuracies in the personal data held by organisations.* Section 12 of Canada's Privacy Act<sup>22</sup> places obligations on organisations to ensure that the personal information kept as part of their records is accurate. Furthermore, individuals have the right to access their personal information held by organisations (subject to a few exceptions), and a right to correct the inaccuracies in their personal information records. Similarly, included in Australia's federal Privacy Act<sup>23</sup> are 13 Australian Privacy Principles, the last of which requires that an organisation provides individuals access to their personal information on request, as well as the ability to correct inaccurate, outdated or irrelevant information, unless particular circumstances apply, which may limit such access.

- **Involuntary or uninformed consent.** Negative consumer outcomes arising from uninformed and/or unlawful consent can be mitigated by prescribing the use of clear and plain language in data use consent forms, in order for consumers to provide informed and voluntary consent.

*Ukraine's Protection of Personal Data Law requires organisations to elicit explicit and voluntary consent from individuals before using their data.* The Protection of Personal Data Law<sup>24</sup> requires that consent is obtained from data subjects prior to the use of their personal data. According to Article 2, consent means a voluntary expression of will to permit the use of personal data for a determined purpose, expressed in writing or another form, which allowed the processor to conclude that consent had been granted.

*In Israel, consent must also be considered "informed" and must be re-obtained.* According to the Protection of Privacy Law<sup>25</sup>, the collection and use of personal data is permitted, subject to the informed consent of a data subject. Consent must be obtained for a specific purpose, the use of which must be proportionate to that purpose. Further, consent must be re-obtained should the purpose of use change (DLA Piper, 2017).

- **Unauthorised sharing and use.** By distinguishing between personal and sensitive data, requiring that minimal data is collected for a particular purpose and only used for that purpose, and restricting the time for which data may be stored, regulation can address some of the negative consumer outcomes that are associated with the unauthorised use and sharing of data.

*GDPR defines different categories of data, each of which is subject to proportional restrictions.* The GDPR includes a broad definition of "special categories" of personal data in Article 9, which are better known as sensitive personal data. The distinction is based on the severity of the consequences to individual privacy and thus the processing of this kind of data is subject to much stricter requirements.

*GDPR also requires that the minimum amount of data is collected to achieve the intended objective.* Article 5 of the GDPR enshrines the "data minimisation principle", requiring that the collection and processing of personal data must be adequate, relevant and limited to what is necessary in relation to the purpose.

*In Angola, data collected must only be stored for the minimum time required to achieve the intended objective. The Data Protection Law mandates that the processing of data is limited to the purpose for which it was collected and may not be stored for longer than is necessary for that purpose (DLA Piper, 2017).*

- **Data breaches.** Requiring breach notifications will not mitigate the likelihood of the negative consumer outcomes associated with data breaches occurring but will likely mitigate the effects of those breaches by giving data subjects the opportunity to take appropriate action to defend their rights.

*In Mexico, it is required that data breaches be immediately reported to the data subject. The regulations related to the Federal Law on the Protection of Personal Data held by Private Parties (*Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares*<sup>26</sup>) require that breaches be promptly reported by the data controller to the data subject so that the data subject can take the necessary steps. Breach notifications must include at least information in relation to: a) the nature of the breach, b) the personal data compromised, c) recommendations to the data subjects concerning available measures to protect their interests, d) corrective actions that were implemented immediately, and e) the means by which the data subject may obtain further information in relation to the breach (DLA Piper, 2017).*

=====

---

<sup>18</sup> Available online: [http://na.gov.pk/uploads/documents/1333523681\\_951.pdf](http://na.gov.pk/uploads/documents/1333523681_951.pdf)

<sup>19</sup> Article 4(7) of the GDPR defines a controller as “the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data”.

<sup>20</sup> Encryption is a process that involves “translating plain text data... into something that appears to be random and meaningless (ciphertext)” (Microsoft, 2018). If an insurer makes use of a weak encryption algorithm, however, consumer data may be vulnerable to being decrypted through brute force attack methods and resources (The MITRE Corporation, 2017).

<sup>21</sup> Available online: <http://unpan1.un.org/intradoc/groups/public/documents/un-dpadm/unpan044147.pdf>

<sup>22</sup> Available online: <http://laws-lois.justice.gc.ca/PDF/P-21.pdf>

<sup>23</sup> Available online: <https://www.legislation.gov.au/Details/C2018C00292>

<sup>24</sup> Available online: [http://www.legislationline.org/download/action/download/id/5569/file/Ukraine\\_law\\_protection\\_personal\\_data\\_2011\\_en.pdf](http://www.legislationline.org/download/action/download/id/5569/file/Ukraine_law_protection_personal_data_2011_en.pdf)

<sup>25</sup> Available online: <http://unpan1.un.org/intradoc/groups/public/documents/UN-DPADM/UNPAN041914.pdf>

<sup>26</sup> Available online: <http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf>

Implementation tool categories	Implementation tools	Omnibus	Sectoral	No regulation
Regulate	Draft new or amend existing regulations.	X	X	X
Supervise	(Re)interpret existing regulations.	X	X	X
	Enforce compliance with overarching law.	X		
	Enforce data protection compliance through license renewal and product approval.		X	X
Collaborate	Engage the data regulator to tailor overarching regulation.	X		
	Engage with global regulators.	X	X	X
Advise	Advise the policymaker.	X	X	X
	Issue compliance and sector-specific guidance to industry.	X	X	
Raise awareness	Raise awareness and offer training on data-related risks and responses.	X	X	X
Facilitate complaints	Offer a complaints channel for consumer data risk issues.	X	X	X
Monitor	Monitor the extent, severity and urgency of new and existing consumer data risks within the market.	X	X	X
Test-and-learn	Implement a test-and-learn approach (e.g. through a regulatory sandbox).	X	X	X

Table 2: Implementation tools available to regulators across legislative approaches | Source: Authors' own

**Selecting appropriate implementation tools.** The regulator needs to consider the consumer outcomes it wants to achieve in line with its mandate and then select an implementation strategy to best achieve these outcomes within the market and regulatory context. The regulator can, for instance, consider whether there are gaps in the legislative approach that impede the achievement of these outcomes or if there are risks to consumers that are not already effectively dealt with elsewhere. This section describes the range of implementation tools available to regulators to achieve those consumer outcomes.

The realities of each of the three overarching data protection and privacy legislative approaches mean that different insurance regulators have a different set of feasible implementation tools at their disposal. Regulation is not the only tool available to the regulator to help achieve its objective of minimising the overall risks arising to consumers. Table 2 draws on interviews with regulators to outline a range of regulation-based and non-regulation-based tools for insurance regulators to implement under each of the data protection and privacy legislative approaches identified. Even when the same tool may be applied under two different approaches, the key considerations may differ somewhat in terms of the design and application. In instances where the different legislative approaches result in differences in the design and application of the tools available to a regulator, the remainder of this section provides a discussion of the various options.

## 5.1 Omnibus approach

If a country's data protection legislation follows an omnibus approach, then the insurance regulator must first ask the question of whether there are specific consumer data protection and privacy risks that apply to the insurance industry that are not covered (or inappropriately dealt with) in the design and application of the existing data protection laws. If yes, then the regulator has a range of tools at its disposal to work within this regulatory context to still achieve its regulatory objective. Options observed include:

1. **Regulate.** The insurance regulator can draft new, separate guidelines or regulations governing entities under its supervision that directly address the identified sector-specific gaps in the overarching omnibus regulation. A critical consideration is for the insurance regulator to ensure that the new regulations do not contradict the overall omnibus data protection legislation. Engagement and coordination with the data regulator will therefore likely be important.
2. **Supervise.** The insurance regulator can use its enforcement capacity either to:
  - a) Apply industry-specific interpretation to an existing law as an alternative mechanism to address the identified sector-specific gaps in the overarching omnibus regulation. This tool may be the quickest and easiest option to address identified risk drivers through regulation. However, it will be vital to communicate and issue clear guidelines to the industry. In Germany, the regulatory framework contains requirements considering the system of governance of a supervised entity<sup>27</sup>, its risk management<sup>28</sup> and IT systems<sup>29</sup>. BaFin, Germany's financial sector regulator, for example, can employ certain measures available within the framework of the supervisory abuse control to sanction insurers when systematic irregularities concerning insurer's data protection are found ("Missstandsaufsicht")<sup>30</sup>. BaFin (2018) also emphasises that the use of automated processes does not transfer the responsibility of the results and the process itself away from providers' senior management and that these processes must be "embedded in an effective, appropriate and proper business organisation".

### BOX 4 | BaFin's strategic thoughts on supervising entities

**Defining prerequisites for BDAI use in models requiring supervisory approval.** Any use of BDAI in models that are subject to supervisory approval would also have to be approved by supervisory authorities accordingly on a case-by-case basis. Beyond the individual case, the question could be asked whether all BDAI methods are equally suited for use in models that require supervisory approval, or whether there are methods that should be ruled out. Furthermore, it is necessary to examine whether existing legal (minimum) standards for the data used and for model transparency are sufficient or whether additional requirements would be necessary.

*Source: BaFin (2018)*

<sup>27</sup> For example, Section 23 of the German Insurance Supervision Act – VAG.

<sup>28</sup> For example, Section 26 VAG, Art. 258 Delegated Act (EU) 2015/35 – DVO.

<sup>29</sup> Art. 258 lit. h and j DVO.

<sup>30</sup> See Section 298 et seqq. of the German Insurance Supervision Act.

As such, firms are not permitted to use “black box excuses” – in other words, they have a responsibility to make sure that “BDAI<sup>31</sup>-based decisions” are comprehensible to third-party experts (BaFin, 2018). Box 4 provides more detailed information on BaFin’s role in supervising firms.

- b) Additionally, the insurance regulator can assist the data regulator with the enforcement of data regulations as they pertain to the insurance industry. Working with the data regulator may make overall enforcement more efficient and effective, thereby helping to achieve the insurance regulator’s consumer protection objective. This requires close coordination with the data regulator and access to the requisite skills.
- 3. Collaborate.** The insurance regulator has a key role to play through collaboration with both local and global regulators to share their expertise.
- a) An insurance regulator can engage directly with a data regulator to share its insurance expertise and help the data regulator to effectively regulate for sector-specific risks and risk drivers. This function is dependent on whether the data regulator’s mandate allows for rule-making or whether it is purely investigative. If the data regulator’s mandate is purely investigative and compliance-oriented, then this option is likely to fall away. However, if the data regulator’s mandate includes rule-making, then the insurance regulator can collaborate with the data regulator and assist with carving out sector-specific provisions within the existing framework. Given its specific insurance-related technical knowledge and skills, the insurance regulator can potentially play a technical advisory role in the regulatory drafting process. This is the case in Australia, where the data regulator of the Victoria territory has implemented sector-specific codes that, if applicable, apply instead of the federal Privacy Act’s Privacy Principles. Similarly, the Insurance Commission of the Philippines coordinates with the National Privacy Commission in the promotion of data protection and privacy, although there is no formal rule or agreement between the two regulators.
  - b) A second critical area of collaboration for the insurance regulator is with global insurance regulators. Insurance regulators will be able to identify emerging risks within their market better, and learn from their peers’ experience of which implementation tools have been most successful through the process of shared learnings among regulators across different contexts. Additionally, input into global insurance standards or guidance on data privacy may be used to inform sector-specific standards within global data protection and privacy guidelines and practices. The International Association of Insurance Supervisors (IAIS), for instance, is putting in place a *FinTech Forum* for the exchange of ideas and lessons among supervisory experts (Dixon, 2018).

---

<sup>31</sup> Big data and artificial intelligence.

4. **Advise.** The insurance regulator has a key role to play in advising both the policymaker and the industry.
  - a) Given its specific insurance-related technical knowledge, skills and perspective on the market, the insurance regulator has a key role to play in advising the policymaker on the policymaker's approach. Under the omnibus approach, this may relate to identifying gaps in the overall legislative framework and playing the role of a technical advisor in the legislative drafting process and/or when amendments are made. Additionally, relative to the regulator, the policymaker has access to more tools – especially fiscal tools. In some cases, the use of subsidies or other fiscal incentives may be the most effective means to address the negative consumer outcomes. In the UK, for instance, advanced flood-mapping data analytics meant that some homeowners situated in flood plains were considered overly risky by insurers and excluded from accessing any form of home insurance. Once raised with the policymaker, Flood Re was established as a state-funded reinsurer to which insurers can reinsure all flood insurance policies, effectively subsidising these policies, with the aim of ensuring that all consumers are able to access insurance (Ho et al., 2018 and Flood Re, 2018).
  - b) By offering training and advice to its licensees on compliance with the overarching data law, the insurance regulator can protect consumers. By enabling licensees to comply fully with the overarching data law, the insurance regulator can ensure that the insurance-related risks that can be mitigated by the overarching law are addressed. Additionally, advising its licensees on compliance, such as developing a compliance toolkit, can ease the compliance burden for providers and increase their ability to continue to use data, thereby ameliorating the risk of exclusion. The regulator could also encourage industry members to discuss and ensure that there are enough other options offered “in the form of conventional financial services and/or services that are economical with personal data” to prevent consumers from experiencing “perceived or actual pressure” to release their personal data to providers (BaFin, 2018).
5. **Raise awareness.** Raising insurers' and consumers' awareness of the risks that arise from the increased collection, storage and use of consumer data will give them a better understanding of the imminent risks, which may a) encourage the insurer to put into place mitigation measures and b) empower the consumer to be more vigilant of who has access to their data and what they allow them to do with it. For example, Germany's financial supervisory authority, BaFin, regards consumer education as part of its consumer protection mandate.
6. **Facilitate complaints.** The new data regulators in most jurisdictions will not have well-established complaints and consumer recourse mechanisms established. Rather than simply referring data-related complaints to the data regulator, insurance regulators can encourage these complaints to be made through their existing complaints mechanisms. This not only provides consumers with an additional recourse channel, but it will also help the regulator monitor the data-related risks occurring in its sector. If, for example, risks are repeatedly occurring that are not covered by the overarching law, then the insurance regulator will know it needs to act to address them.

7. **Monitor.** Ongoing monitoring of the risks being experienced in the market and the potential of future risks likely to arise is a critical function of the insurance regulator. This is a prerequisite to inform engagement with the policymaker and data regulator, as well as its own implementation tools. The Comisión Nacional de Seguros y Fianzas (CNSF) in Mexico, for example, indicate that they are monitoring the prevalence and impact of data risks in its market, which includes conducting research on these risks and considering regulations implemented in other jurisdictions. Monitoring complaints is a traditional mechanism to monitor risks arising, but new mechanisms may also be increasingly possible. The FCA, for instance, is using sentiment analysis of social media in order to identify new consumer risks and issues even before formal complaints are made (Ho et al., 2018).
8. **Test-and-learn.** The insurance regulator can consider implementing a regulatory sandbox<sup>32</sup> that is open to licensees within its jurisdiction. This would enable new innovation in data collection and use to be tried in the market on a temporary basis with appropriate safeguards in place and would enable the regulator to closely monitor the associated risks to inform and advise the policymaker and data regulator or to identify sector-specific gaps that require the implementation of additional tools by the insurance regulator. Innovation in the consumer data space may require close coordination and cooperation with the data regulator for the sandbox to operate effectively. The Monetary Authority of Singapore (MAS), for instance, has implemented a regulatory sandbox that “will enable FIs as well as fintech players to experiment with innovative financial products or services in the production environment but within a well-defined space and duration” (MAS, 2018). A specific focus for MAS is on innovative data use – as such, it has developed a specific data sandbox to encourage this.

---

<sup>32</sup> Temporary bespoke regulatory treatment reduces or waives existing regulatory requirements for innovators, usually on an impermanent basis, in the interest of testing and learning while concomitantly implementing tailored safeguards to limit the scale of the risk (Beyers et al., 2018).

## 5.2 Sectoral approach

In the context of a sectoral approach, the insurance regulator is responsible for consumer data protection and privacy within the insurance industry. Given that the insurance regulator is essentially faced with a blank slate, not bound by existing overarching data protection principles, it can consider key data protection and privacy principles that have been implemented globally – although these will still need to be in line with the country’s societal norms as outlined in Box 2. It is likely that an insurance regulator will take a different strategy to regulating for consumer data protection and privacy than an overarching data regulator will, because they have different objectives. While an insurance regulator’s aim is to regulate for the specific risks that arise commonly in the insurance sector, the data regulator’s aim is to ensure that its regulation finds applicability in as many situations and contexts as possible. As such, the latter’s regulation is likely to remain relatively non-specific. Implementation options available to the insurance regulator operating under a sectoral data protection regulatory framework include:

1. **Regulate.** Given that no existing data regulation exists for the sector and the onus is explicitly on the insurance regulator to regulate data risks in the sector, regulation that explicitly deals with these risks is essentially a prerequisite under a sectoral approach. This may be achieved by drafting new regulation or amending existing regulations. A key consideration for this option is the coordination with other financial sector regulators to ensure that there is uniformity across the various data regulations issued within the financial sector. In the US, for example, The National Association of Insurance Commissioners (NAIC)<sup>33</sup> has implemented the option to draft new regulations – specifically, a Data Security Model Law, which it completed in October 2017 and addresses consumer data protection and privacy in the insurance sector. The state of South Carolina has already adopted the model law and a few other states, including Rhode Island and Vermont, have indicated that they are in the process of adding it to their legislative calendars.

Existing regulations, such as market conduct or TCF, can also be amended to include data protection and privacy provisions. This option, like the one above, does require considerable capacity and resources on part of the insurance regulator. The success of applying this tool – especially with regard to the enforcement of these regulations will depend on the resources available to the insurance regulator.

2. **Supervise.** The insurance regulator can use its enforcement capacity either to:
  - a) Apply industry-specific interpretation to an existing law. This tool may be the quickest and easiest option to address identified risk drivers through regulation, but in the absence of more far-reaching data protection and privacy regulation, it may be a temporary rather than a final solution. Coordination with other financial regulators will once again be critical to ensure consistency. Consumer protection rules can also be interpreted to include the protection of consumers from data-related risks.

---

<sup>33</sup> NAIC is the US standard-setting and regulatory-support organisation governed by the chief insurance commissioners from 50 states.



- b) Enforce data protection compliance through license renewal and product approval. In the absence of existing data regulations, there is an opportunity for the insurance regulator to include certain data protection requirements in license renewals and product approvals. This will necessitate clear guidance to the industry in order to ensure transparency.
3. **Collaborate.** Collaboration with other sectoral regulators, as well as global data regulators, can help the insurance regulator effectively tailor regulation and its implementation tool(s). Participating in an international forum would improve a regulator's knowledge of data-related issues, how other regulators are dealing with these issues, and take the lessons learned and apply them to the regulator's own jurisdiction. It also acts as a signalling device to insurance market participants that the regulator is actively considering these issues.
  4. **Advise.** The insurance regulator has a key role to play in advising both the policymaker and the industry. Although under a sectoral approach, the insurance regulator has the mandate to regulate consumer data risks within the insurance industry, the policymaker should still hold the broader perspective of the overall societal objectives and norms and ensure some consistency in application across sectors. As such, it is important for the regulator to engage with the policymaker to advise, inform and be informed by the policy position. Once new regulations are drafted, or existing regulations amended by the insurance regulator, it is critical that it engages with industry players to provide them clear and transparent guidance with regard to compliance.
  5. **Facilitate complaints.** Effective complaints mechanisms will inform the insurance regulator of the risks that are not being addressed adequately by the sectoral law. Alternatively, if an insurance-specific sectoral law is not yet in operation, then the regulator has an indication of which risks are more prevalent than others and what must be addressed by the sectoral law.
  6. **Test-and-learn.** Given the nature of the sectoral regulatory framework, the insurance regulator can consider implementing a regulatory sandbox that is open to licensees within its jurisdiction. This would enable new innovation in data collection and use to be tried in the market on a temporary basis with appropriate safeguards in place. It would also enable the regulator to closely monitor the associated risks and enable refinements to its strategy as a result. Innovation can often be a phenomenon that cuts across regulatory jurisdictions, which means that even within a sectoral framework, the insurance regulator would likely need to collaborate with other regulators to ensure that the sandbox is open to a wider group of participants and truly encourages responsible innovation (Beyers et al., 2017).

### 5.3 No legislation exists

If no omnibus law exists, but the regulator is also not operating within an explicitly sectoral regulatory framework, then the insurance regulator may need to consider if existing consumer protection frameworks are sufficient for its market context or if there is a need to introduce data protection and privacy requirements into regulation. The purpose of introducing data protection and privacy requirements would be to protect consumers and gain consumer trust as an interim measure while consumer data protection and privacy legislation is drafted. Furthermore, a lack of clear regulations and regulatory guidance creates regulatory uncertainty for providers, which increases the costs of doing business and has a negative impact on their ability to take risks, thereby contributing to the likelihood of consumer exclusion.

The insurance regulator would likely be conservative in its implementation of these data privacy regulations given resource constraints and it will likely be an interim measure. However, it is important for the regulator to be proactive and protect its industry's consumers from significant risks. Options available are similar to those where the insurance regulator is operating under a sectoral data protection regulatory framework, but it is vital to deliberately consider any pending or potential regulation to ensure consistency. The implementation options available include:

1. **Regulate.** The key considerations for new or amended regulation to deal with data risks under this legislative approach is to be aware of any pending legislation and craft the sectoral regulation to be as consistent with pending legislation as possible. This will facilitate a smooth transition when the legislation is ratified. For example, before the recent passing of the Brazilian Personal Data Protection Law (13.709/2018), the Brazilian insurance regulator, SUSEP, issued interim regulations – CNSP Resolution No. 297/13 – while overarching data privacy bills remained in congress, to address data risks pertinent to the insurance market (SUSEP, 2013 and Mondaq, 2013). In the absence of explicit regulatory protection, consumers are vulnerable and given that the insurance regulator's objective is to protect consumers, it cannot ignore the potential negative outcomes. In Kenya, The Insurance Regulatory Authority (IRA) is amending and reinterpreting existing market conduct guidelines to ensure appropriate consumer protection against arising data risks. The amendments are explicitly aimed at taking proposals in pending data regulation into account, to ensure consistency when the Act comes into effect.
2. **Supervise.** The insurance regulator can apply its enforcement capacity to reinterpret existing regulations. Provided that new regulation does not have to be drafted, this is possibly a faster and simpler option, but it requires very clear interpretation guidelines to the industry. The insurance regulator should aim to be consistent with any pending or future data regulation if applicable or known.
3. **Collaborate.** As with a sectoral regulatory framework, collaboration with global regulators can help the insurance regulator effectively tailor regulation and its implementation tool(s). Participating in an international forum would improve a regulator's knowledge of data-related issues, how other regulators are dealing with these issues and apply the lessons learned to the regulator's own jurisdiction. It also acts as a signalling device to insurance market participants that the regulator is actively considering these issues. The creation of the Global Financial Innovation Network (GFIN), for example,

was announced on 7 August 2018. A collaboration of initially 12 global financial regulators, the network will “seek to provide a more efficient way for innovative firms to interact with regulators, helping them navigate between countries as they look to scale new ideas. It will also create a new framework for cooperation between financial services regulators on innovation related topics, sharing different experiences and approaches” (FCA, 2018).

4. **Advise.** Similar to the sectoral approach, the insurance regulator has a key role to play in advising both the policymaker and the industry.
  - a) In an environment with no existing legislative approach to consumer data protection and privacy, the insurance regulator has a critical role to play in advising and informing the policymaker of the manner in which these risks are manifesting, in order to inform the development of a societal policy and influence pending legislation.
  - b) Once new regulations are drafted or existing regulations are amended by the insurance regulator, it is critical that it engages with industry to provide clear and transparent guidance for compliance.
5. **Raise awareness.** Raising insurers’ and consumers’ awareness of the risks that arise from the increased collection, storage and use of consumer data will give them a better understanding of the imminent risks, which may a) encourage the insurer to put in place mitigation measures and b) empower the consumer to be more vigilant of who has access to their data and what they allow them to do with it.
6. **Facilitate complaints.** Effective complaints mechanisms will inform the insurance regulator of the most immediate and pressing data related risks to be addressed by the regulator.
7. **Monitor.** Ongoing monitoring of the risks being experienced in the market and the potential of future risks likely to arise is a critical function of the insurance regulator. This is a prerequisite to inform engagement with the policymaker and its own implementation tools.
8. **Test-and-learn.** Implementing a regulatory sandbox or similar test-and-learn tool may be an opportunity for regulators to allow innovation to be tested in the market more quickly and flexibly than through alternative tools. Crucially, given the lack of existing regulation under this legislative approach, a sandbox would enable the regulator to learn about the risks that manifest from innovative collection or use of consumer data, while still maintaining appropriate safeguards (Beyers et al., 2017).

=====

**BOX 5 | Implementing a response to the use of data in data-intensive financial services (DIFS)**

In the absence of existing omnibus data protection legislation, Rothe et al. (2018) highlights a set of six recommendations for financial sector policy-makers, regulators and other authorities working on policy and regulations that affect the use of data in DIFS. They are intended to inform discussions around data protection and DIFS and to support the drafting and implementation of respective regulations.

**1. Demonstrate leadership in data protection:**

First, clarify the role of the financial sector authority in data protection within the broader regulatory framework. Due to the cross-cutting nature of data and nuances within the financial sector, policymakers should champion their sector while supporting broader regulation. Consider the trade-off between data privacy and enabling innovation when considering regulation. Develop the skills in the market to deal with data privacy in financial institutions and for customers. Public authorities should lead by example in respecting data privacy.

**2. Collaborate to uphold privacy in the digital age:**

Work with other public authorities who collect data to ensure the consistent treatment of data. Industry cooperation can facilitate economies of scale and a level playing field. This decreases costs while promoting fair competition. Consultations prior to regulation development also facilitate compliance. As the entities impacted are consulted during the development of regulation they are more likely to comply voluntarily.

**3. Enhance data awareness:**

Customers are often unaware of data risks. Policymakers should raise awareness of data risks and require FSPs to do the same. All staff that handle data should also be made aware of data risks.

**4. Empower consumers to be the sovereigns of their data:**

Consumers need to be informed of what data is being collected and for what reason. This is required to address the asymmetry in information between consumers and FSPs. Consumers should have to provide consent to use their data for uses other than those specified during collection. Consumers should also be able to change and move their data. This ensures that data is correct and that consumers receive the benefit thereof. Customer data should be deleted once its purpose has been fulfilled.

**5. Hold providers accountable:**

Automated decisions should be interpretable. This prevents prohibited discrimination. Providers should be required to have clear documentation of data sources and uses. Discrimination on inadmissible criteria should not be allowed while noting that the economic cost will be borne by the broader customer base. Providers and stakeholders utilising automated decision-making should be required to undertake a risk assessment.

**6. Enforce secure data storage:**

Secure data storage is fundamental to data privacy. This includes data access procedures, hardware and software requirements and physical security of servers. Similar care should be ensured when third-parties are provided access to data.

*Source: Rothe et al., 2018*

=====

## 6. REQUIREMENTS FOR SUCCESS: INSURANCE REGULATOR'S ADDITIONAL CONSIDERATIONS

The section above outlines the implementation options available to regulators given their contextual realities. However, the effectiveness of these implementation tools will still hinge on the regulator's capacity, ability to coordinate effectively and ability to build awareness among both providers and consumers.

**Capacity and learning.** The capacity that is available to the insurance regulator will determine the extent to which data protection and privacy regulations can realistically be enforced. There is a trade-off between drafting strict and complex regulation that places high demands on capacity and simple but adequate regulation, the enforcement of which is manageable despite capacity constraints. The regulation of data protection and privacy requires new skills and knowledge to understand the risks and how they manifest. This will likely require additional recruitment or the development of new skills and emphasises the importance of interdisciplinary supervisory teams (IAIS, 2018a). The MAS, for instance, has a particular focus on recruiting for data scientists, and it second staff to industry players, foreign regulatory bodies and supranational organisations to help them keep up-to-date with the latest innovations (Beyers et al., 2018). In order to map the risks and facilitate an exchange of information with relevant parties, regulators could also seek partnerships with, for example, insurtech firms and research organisations and through peer-learning platforms. Global platforms that facilitate the exchange of information with peer regulators like the IAIS Fintech Forum and the Global Financial Innovation Network (GFIN) offer such examples.

The extent of change in the data landscape also requires regulators to develop deliberate approaches to learn and build capacity on how best to regulate and supervise insurance markets for positive consumer outcomes.

**Coordination.** Data effectively extends the insurance value chain and pulls in new players, requiring effective coordination with new regulators and proactive engagement with policy-makers. A sectoral approach requires at least some level of coordination among regulators across sectors to ensure that data protection and privacy laws are applied somewhat consistently and that, for institutions operating in numerous sectors, the laws are fairly uniform. Under an omnibus approach, coordination between the insurance regulator and the data regulator will be required. The insurance regulator will have insurance-specific technical expertise, while the data regulator will have data-specific technical expertise, both of which are required in regulatory design and enforcement.

**Awareness.** Engagement with providers and consumers will be significant to drive awareness of potential risks and how best to respond as a responsible market player and as an insurance consumer. Empowering consumers to protect themselves will need to be a key pillar to achieve positive consumer outcomes.

## 7. AVAILABLE STRATEGIES TO INSURANCE REGULATORS

**Overall implementation strategies: regulators’ decision, based on desired outcomes and constraints.** As outlined throughout this paper, insurance regulators must work within their existing constraints. The existing legislative approach is determined by the policymaker, but it is the framework within which the insurance regulator must operate and so determines which strategies can and cannot be implemented by the regulator to pursue its aims. The insurance regulator has a choice to make in terms of how engaged it will be in addressing the risks to consumers from the collection, storage and use of consumer data. This choice will be made based on the regulator’s mandate, the market context and its capacity to deal with these risks.

Insurance regulators may apply four broad strategies to regulate for responsible data innovation<sup>34</sup>. These approaches, summarised in Figure 8 are driven by the country approach to data regulation and the degree of engagement needed by the insurance regulator.

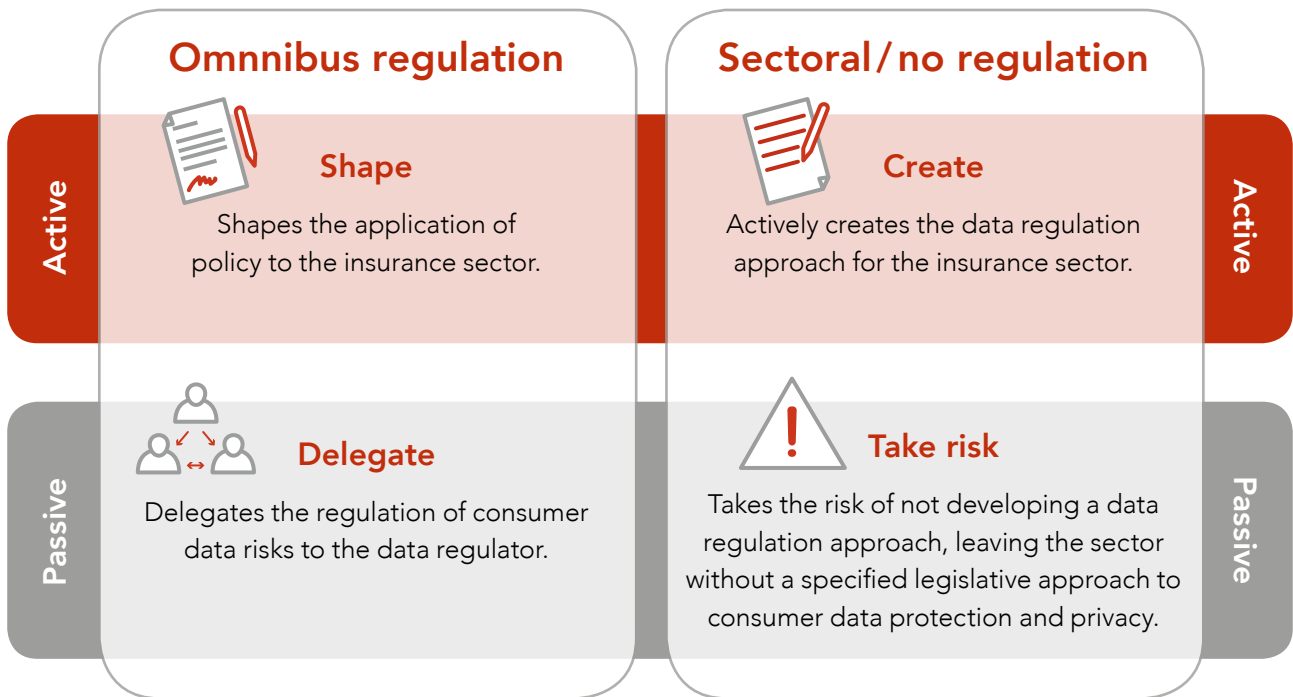


Figure 8: Available strategies to regulators | Source: Authors’ own

**Create.** Regulators that operate in a sectoral legislative approach or in an environment with no cross-cutting data privacy and protection legislation in place have the primary responsibility to develop the approach to data protection and privacy within their sector. Regulators can there-

<sup>34</sup> As regulators can engage in a range of potential activities, the extent to which regulators actively engage in and mould an approach will vary across regulators that may still be classified in the same category. In some cases, regulators may fall ‘between’ categories where they are active in some areas but passive in others. Nevertheless, these categories provide a heuristic to broadly classify regulators’ observed general strategies.

fore actively create the data regulation approach for the insurance sector. This can be done by drafting and enforcing new regulation, as well as through proactive coordination strategies with other regulators.

=====

**BOX 6 | Examples of the 'create' approach**

**Kenya**

In the absence of a data protection and privacy legislative framework, the Insurance Regulatory Authority (IRA) has amended regulation to deal with data related risks to consumers. Examples of tools implemented include:

*Regulate:* The IRA is amending and reinterpreting existing market conduct guidelines to ensure appropriate consumer protection against arising data risks. The amendments are explicitly aimed at taking proposals in pending data regulation into account, to ensure consistency when the Act comes into effect. Moreover, as per stakeholder interviews, the IRA is considering the need for harmonisation with global regulations and guidelines.

**USA**

Operating under a sectoral approach, the NAIC has drafted new regulation to address data protection and privacy for the insurance sector. Examples of tools implemented include:

*Regulate:* The NAIC completed its drafting of a Data Security Model Law in October 2017, which addresses consumer data protection and privacy in the insurance sector. The state of South Carolina has already adopted the model law and a few other states, including Rhode Island and Vermont, have indicated that they are in the process of adding it to their legislative calendars. The Model Law makes provision for enforcement by the regulator and for penalties to be issued.

*Please refer to Appendix A for more details on these country case studies.*

=====

**Shape.** Regulators operating within an omnibus legislative approach will not have the ability to create the overarching data legislative approach, but they do have the opportunity to tailor and shape the approach within their sector. This can be done by advising the policymaker on risks and outcomes that arise from insurance markets and by coordinating with the data regulator on supervision to ensure that insurance-sector appropriate provisions are put in place. Regulators can also actively shape the approach to data protection in the insurance sector by drafting and enforcing insurance-specific regulation, supplementary to existing data protection legislation.

=====

**BOX 7 | Examples of the 'shape' approach**

**South Africa**

The Financial Sector Conduct Authority (FSCA) has taken a very active role in the regulation of data risks, following a 'shape' strategy, especially in implementing requirements in the interim period before all of the provisions of Protection of Personal Information Act of 2013 (POPI) become operational. The FSCA has employed regulatory

tools to supplement the existing omnibus framework and intends to engage actively with the data regulator once it is formally established. Examples of tools implemented include:

*Regulate:* The FSCA has issued various rules and regulations relating to data privacy and protection including: a) Financial Advisory and Intermediary Services (FAIS) conduct requirements – requiring consent before information may be disclosed, b) Policy Holder Protection Rules – relating to the sharing of data in groups or partnerships, to be implemented early 2020, c) TCF principles – requiring that insurance providers target positive consumer outcomes as a priority, and d) under the Financial Sector Regulation Act of 2017, which established the twin peaks system, requirements prescribe how conglomerates share information in groups, however this is monitored by SARB – the prudential authority.

*Coordinate:* The FSCA has a unit that comments on legislation such as POPI while awaiting the formal establishment of the data regulator. Once established, the unit expects to engage actively with the data regulator.

**Philippines**

The Insurance Commission of the Philippines has followed a ‘shape’ strategy by employing regulatory tools to augment the existing omnibus legislative framework and by actively coordinating with the National Privacy Commission to promote data protection and privacy. Examples of tools implemented include:

*Regulate:* The Insurance Commission issued guidelines extending the scope of the national data protection and privacy regulations to insurers specifically.

*Coordinate:* While there is no formal rule or agreement between the two regulators, the Insurance Commission coordinates with the National Privacy Commission in the promotion of data protection and privacy.

*Please refer to Appendix A for more details on these country case studies.*

=====

**Delegate.** Alternatively, regulators that operate in an omnibus legislative approach can play a less active role, effectively delegating the regulation of consumer data risks to the data regulator. This option may be pursued if it is considered that the omnibus regulation already effectively addresses the unique risks that manifest in the insurance market.

=====

**BOX 8 | Examples of the ‘delegate’ approach**

**Mexico**

The CNSF has followed a ‘delegate’ strategy, so far considering the Federal Law on the Protection of Personal Data Held by Private Parties to sufficiently deal with the risks in the insurance sector. Examples of tools implemented include:

*Monitor:* The CNSF are monitoring the prevalence and impact of data risks in its market, which includes conducting research on these risks and considering regulations implemented in other jurisdictions.

*Please refer to Appendix A for more details on these country case studies.*

=====



**Take risk.** Regulators that operate in a sectoral legislative approach or in an environment with no legislation can alternatively remain in the default position or explicitly decide to take the risk of not developing a data regulation approach, which will mean the sector has no specified legislative approach to consumer data protection and privacy. This option is applied in markets where data-related risks are not considered an imminent threat.

**Ongoing monitoring of risks arising remains critical, regardless of strategy.** All insurance regulators should ensure that strategies be employed to effectively monitor existing and imminent risks within their market. An understanding of the risks to consumers and what is driving those risks is crucial to either tailor the existing strategy or to adjust the strategy, if required. Regulators employing the 'create' strategy, for instance, must maintain ongoing monitoring to adjust and tailor their tools to most effectively address the risks arising. Regulators employing the 'take risk' strategy, on the other hand, must maintain ongoing monitoring to determine whether this strategy remains appropriate. Once data-related risks become more imminent and begin to manifest in the market, such a regulator will need to reconsider its strategy.

IAIS (2018a) emphasises that regulators will need to become "data driven" and "digital intelligence led". Regulators need to understand how incumbent insurers and intermediaries, as well as newer market participants, including insurtech start-ups and Big Techs, are behaving and the impact on outcomes for consumers. This requires regulators to monitor the behaviour and outcomes, by examining information flowing from multiple sources and may require investment in technology by regulators to do this effectively.

**Rapid change requires peer learning, global coordination and ongoing research.** In developing countries, the rapidly growing levels of connectedness means that the amount of consumer data available is growing exponentially. At the same time, new technologies and techniques mean that this data can be used in innovative ways. For regulators, the speed of change and novelty of some of the implications makes this a challenging area to effectively address. Coordination and peer learning at a global level is therefore crucial to accelerate this learning process. Developing countries in particular have the ability to learn from the experiences of developed markets. However, what works in one market may not be appropriate in another. Ongoing research to understand the nuances of the issues and risks arising is therefore critical to ensure that regulatory responses be informed by global learning, yet also tailored to specific context.

## 8. CONCLUSION

The use of consumer data is the area of most rapid innovation and change in the insurance sector globally. The potential of data to ameliorate the risk of exclusion has already been illustrated and is expected to offer substantive further inroads into dealing with insurance exclusion in developing countries. However, the collection, storage and use of this consumer data by providers also brings with them new risks of consumer abuse.

Data affects society as a whole and the approach to achieving positive outcomes with its use requires a policy response across sectors. The insurance regulator, however, is responsible to ensure positive outcomes for current and potential consumers of insurance. The strategies and tools employed to achieve this objective must therefore be tailored according to the overall legislative approach as well as be aligned with the insurance regulator's mandate and the insurance market context.

This report outlines the key decision considerations for regulators to determine which strategy is feasible within each context and describes the range of implementation tools that regulators have at their disposal to deal with these data-related consumer risks.

---

## BIBLIOGRAPHY

A2ii (2016). *Data protection challenges in mobile insurance: Report of the 19th A2ii-IAIS consultation call*. Available online: [https://a2ii.org/sites/default/files/reports/19.20consultation\\_call\\_engl\\_web.pdf](https://a2ii.org/sites/default/files/reports/19.20consultation_call_engl_web.pdf).

---

ARD/ZDF (2017). *Kern-Ergebnisse der ARD/ZDF-Onlinestudie 2017*. Available online: [www.ard-zdf-onlinestudie.de/files/2017/Artikel/Kern-Ergebnisse\\_ARDZDF-Onlinestudie\\_2017.pdf](http://www.ard-zdf-onlinestudie.de/files/2017/Artikel/Kern-Ergebnisse_ARDZDF-Onlinestudie_2017.pdf).

---

Australian Prudential Regulatory Authority (2018). *Industry supervision: APRA*. Available online: [www.apra.gov.au/supervision](http://www.apra.gov.au/supervision).

---

Australian Securities and Investments Commission (2018). *Our role: ASIC – Australian Securities and Investments Commission*. Available online: <https://asic.gov.au/about-asic/what-we-do/our-role/>.

---

BaFin (2018). *Big Data meets artificial intelligence*. Available online: [www.bafin.de/SharedDocs/Downloads/EN/dl\\_bdai\\_studie\\_en.html;jsessionid=17D8386C1A00AD740CF23AB405425824.1\\_cid298](http://www.bafin.de/SharedDocs/Downloads/EN/dl_bdai_studie_en.html;jsessionid=17D8386C1A00AD740CF23AB405425824.1_cid298).

---

BBC (2014). *Facebook emotion experiment sparks criticism*. Available online: [www.bbc.com/news/technology-28051930](http://www.bbc.com/news/technology-28051930).

---

BBC (2017). *Kenya election 2017: Commission denies system was hacked*. Available online: [www.bbc.com/news/world-africa-40882268](http://www.bbc.com/news/world-africa-40882268).

---

BBC (2018). *Aadhaar: 'Leak' in world's biggest database worries Indians*. Available online: [www.bbc.com/news/world-asia-india-42575443](http://www.bbc.com/news/world-asia-india-42575443).

---

Bennett Coleman and Company (2018). *Government admits to cases of fraudulent withdrawal of money through Aadhaar*. Available online: <https://economictimes.indiatimes.com/news/politics-and-nation/government-admits-to-cases-of-fraudulent-withdrawal-of-money-through-aadhaar/articleshow/62807903.cms+&cd=4&hl=en&ct=clnk&gl=z>.

---

Bhoola, K., Kruger, K., Peick, J. Pio, P. and Tshabalala, N.A. (2014). *Big Data analytics*. Actuarial Society 2014 Convention, Cape Town, 22–23 October 2014. Available online: <https://actuariesociety.org.za/convention/convention2014/assets/pdf/papers/2014 ASSA Bhoola Kruger.pdf>.

---

California Department of Insurance (2017). *Investigation of major Anthem cyber breach reveals foreign nation behind breach*. Available online: <http://www.insurance.ca.gov/0400-news/0100-press-releases/2017/release001-17.cfm>.

---

Castro, D. and New, J. (2016). *The promise of Artificial Intelligence*. Available online: <http://www2.datainnovation.org/2016-promise-of-ai.pdf>.

---

Chamberlain, D., Bester, H. and Hougaard, C. (2009). *Risk it or insure it?* Available online: [https://cenfri.org/wp-content/uploads/2017/12/FN8\\_Insurance-decision\\_English.pdf](https://cenfri.org/wp-content/uploads/2017/12/FN8_Insurance-decision_English.pdf).

---

Chen, G. and Faz, X. (2014). *Hype or hope? Implications of Big Data for financial inclusion*. CGAP. Available online: <http://www.cgap.org/blog/hype-or-hope-implications-big-data-financial-inclusion>.

---

Chen, G. and Faz, X. (2015). *The potential of digital data: How far can it advance financial inclusion?* Available online:

[http://www.cgap.org/sites/default/files/Focus-Note-The-Potential-of-Digital-Data-Jan-2015\\_1.pdf](http://www.cgap.org/sites/default/files/Focus-Note-The-Potential-of-Digital-Data-Jan-2015_1.pdf).

---

Cheston, S., Rhyne, E., Silverberg, K., Kelly, S., McGrath, A., French, C. and Ferenzy, D. (2018).

*Inclusive insurance: Closing the protection gap for emerging customers.* Available online:

[www.centerforfinancialinclusion.org/storage/Inclusive\\_Insurance\\_Final\\_2018.01.06.pdf](http://www.centerforfinancialinclusion.org/storage/Inclusive_Insurance_Final_2018.01.06.pdf).

---

Cohn, D. (2013). *Lessons from the German census.* Available online:

<http://www.pewresearch.org/fact-tank/2013/06/20/lessons-from-the-german-census/>.

---

Collett, M. (2018). *Commonwealth Bank: Here's what you should know about the data breach if you're a customer.* Available online: <http://www.abc.net.au/news/2018-05-03/what-cba-customers-need-to-know-about-the-data-breach/9722614>.

---

Comisión Nacional de Seguros y Fianzas (2018). *Gob.mx.* Available online: <https://www.gob.mx/cnsf>.

---

Crabtree, J. (2018). *Here's how Cambridge Analytica played a dominant role in Kenya's chaotic 2017 elections.* Available online:

<https://www.cnn.com/2018/03/23/cambridge-analytica-and-its-role-in-kenya-2017-elections.html>.

---

De Brusk, C. (2018). *The risk of machine-learning bias (and how to prevent it).* Available online:

<https://sloanreview.mit.edu/article/the-risk-of-machine-learning-bias-and-how-to-prevent-it/>.

---

Desjardins, J. (2017). *Here's everything that happens in one minute on the internet.* Available online:

<https://www.businessinsider.com/everything-that-happens-in-one-minute-on-the-internet-2017-9?IR=T>.

---

Dixon, J. (2018). *Newsletter Issue 77.* Available online:

<https://www.iaisweb.org/page/news/newsletter/file/76396/iais-newsletter-august-2018>.

---

DLA Piper (2017). *DLA Piper global data protection laws of the world: World map.* Available online:

<https://www.dlapiperdataprotection.com/index.html?t=world-map&c=AO>.

---

FCA (2018). *Global Financial Innovation Network.* Available online: <https://www.fca.org.uk/publications/consultation-papers/global-financial-innovation-network>.

---

Flood Re (2018). *How Flood Re works.* Available online: <https://www.floodre.co.uk/how-flood-re-works/>.

---

FSCA (2018). *Treating Customers Fairly.* Available online:

<https://www.fscaconsumered.co.za/Consumer/Pages/Treating-Customers-Fairly.aspx>.

---

Gartner (2018). *Gartner IT glossary: Big data.* Available online:

<https://www.gartner.com/it-glossary/big-data>.

---

Gemalto (2018). *Breach level index infographic 2017.* Available online:

<https://breachlevelindex.com/assets/Breach-Level-Index-Infographic-2017-Gemalto-1500.jpg>.

---

Gramlich, J. (2018). *5 facts about Americans and Facebook.* Available online:

<http://www.pewresearch.org/fact-tank/2018/04/10/5-facts-about-americans-and-facebook/>.

---

---

Gressin, S. (2017). *The Equifax data breach: What to do*. [Online]. Available from: <https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do>.

---

GSM Association (2018). *The data value chain*. Available online: [https://www.gsma.com/publicpolicy/wp-content/uploads/2018/06/GSMA\\_Data\\_Value\\_Chain\\_June\\_2018.pdf](https://www.gsma.com/publicpolicy/wp-content/uploads/2018/06/GSMA_Data_Value_Chain_June_2018.pdf).

---

GSMA Intelligence (2017). *GMEI 2017: Global Mobile Engagement Index*. Available online: <https://www.gsmainelligence.com/research/?file=e4549aeda553ac832ff9126c7d6c0861&download>.

---

Ho, H S., Francis, H., Sicsic, M. and Thom, M. (2018). *Panel discussion on the use of innovation facilities as a regulatory tool*. 11th Annual IAIS Global Seminar.

---

Hosein, G. (2011). *Privacy and developing countries*. Available online: [https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2011/hosein\\_201109/](https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2011/hosein_201109/).

---

Hunter, R., Nordin, K. and Thom, M. (forthcoming). *Client data in inclusive insurance*.

---

IAIS (2016). *Issues paper on cyber risk to the insurance sector*. Available online: <https://www.iaisweb.org/page/supervisory-material/issues-papers>.

---

IAIS (2017). *Insurance core principles*. Available online: <https://www.iaisweb.org/page/supervisory-material/insurance-core-principles/file/70028/all-adopted-icps-updated-november-2017>.

---

IAIS (2018a). *Issues paper on the increasing use of digital technology in insurance and its potential impact on consumer outcomes*. Consultation draft: 25 July 2018.

---

IAIS (2018b). *Application paper on the use of digital technology in inclusive insurance*. Consultation draft: 29 January 2018.

---

Institute of Actuaries of Australia (2016). *The impact of big data on the future of insurance*. Green Paper. Available online: <https://actuaries.asn.au/Library/Opinion/2016/BIGDATAGPWEB.pdf>.

---

Insurance Regulatory Authority (2018). *The role of the IRA*. Available online: <https://www.ira.go.ke/>.

---

ITU (2017). *ICT Development Index 2017*. Available online: <http://www.itu.int/net4/ITU-D/idi/2017/index.html#idi2017rank-tab>.

---

Kolata, G. (2017). *New gene tests pose a threat to insurers*. Available online: <https://www.nytimes.com/2017/05/12/health/new-gene-tests-pose-a-threat-to-insurers.html>.

---

Lyko K., Nitzschke M. and Ngonga Ngomo, A.C. (2016). *Big Data Acquisition*. In Cavanillas J., Curry E., Wahlster W. (eds.) *New Horizons for a Data-Driven Economy*. Springer.

---

McKee, K., Kaffenberger, M. and Zimmerman, J. M. (2015). *Doing digital finance right: the case for stronger mitigation of customer risks*. Available online: <http://www.cgap.org/sites/default/files/Focus-Note-Doing-Digital-Finance-Right-Jun-2015.pdf>.

---

Mondaq (2013). *Data protection and the insurance market Brazilian legal aspects: Data protection Brazil*. Available online: <http://www.mondaq.com/brazil/x/280724/Data+Protection+Privacy/Data+Protection+and+The+Insurance+Market+Brazilian+Legal+Aspects>.

---

Monetary Authority of Singapore (MAS) (2018). *Understanding and applying to the sandbox*. Available online: <http://www.mas.gov.sg/Singapore-Financial-Centre/Smart-Financial-Centre/FinTech-Regulatory-Sandbox/Understanding-and-applying-to-the-sandbox.aspx>.

---

Niselow, T. (2018). *Regulator seeks finer details of Liberty data breach*. Available online: <https://www.fin24.com/Companies/ICT/regulator-seeks-finer-details-of-liberty-data-breach-20180618>.

---

Noggle, R. (2018). *The Ethics of Manipulation*. In Edward N. Zalta (ed.). *The Stanford Encyclopedia of Philosophy (Summer 2018 Edition)*. Available online: <https://plato.stanford.edu/archives/sum2018/entries/ethics-manipulation/>.

---

Noiré, M-E. (2018). *Selfies becoming a useful tool for payments and insurance?* Available online: <https://atelier.bnpparibas/en/fintech/article/selfies-tool-payments-insurance>.

---

Old Mutual (2018). *Important customer notice*. Available online: <https://www.oldmutual.co.za/about-us/governance/customer-confirmation>.

---

Pew Research Center (2014). *Global opinions of U.S. Surveillance*. Available online: <http://www.pewglobal.org/2014/07/14/nsa-opinion/table/country-citizens/>.

---

Ransbotham, S. and Kiron, D. (2018). *Improve customer engagement*. Available online: <https://sloanreview.mit.edu/projects/using-analytics-to-improve-customer-engagement/>.

---

Rothe, M., Dix, A. and Ohlenburg on behalf of GIZ/BMZ. (2018). *Responsible use of personal data and automated decision-making in financial services*. Published by Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH.

---

Saarinen, M., Ladousse, J. and Auvray, E. (2017). *Data protection in France: overview*. Available online: <https://uk.practicallaw.thomsonreuters.com/6-502-1481>.

---

Sensis (2018). *Yellow social media report 2018*. Available online: <https://www.yellow.com.au/wp-content/uploads/2018/06/Yellow-Social-Media-Consumer-Stats.pdf>.

---

Shapshak, T. (2016). *Facebook grows 16% in South Africa, 6% in Nigeria, 18% in Kenya*. Available online: <https://www.forbes.com/sites/tobyshapshak/2016/06/30/facebook-grows-16-in-south-africa-6-in-nigeria-18-in-kenya/#7cafad7162e7>.

---

Smit, H., Denoon-Stevens, C. and Esser, A. (2017). *Insurtech for development*. Available online: [https://cenfri.org/wp-content/uploads/2017/11/InsurTech-Research-Study\\_March-2017.pdf](https://cenfri.org/wp-content/uploads/2017/11/InsurTech-Research-Study_March-2017.pdf).

---

Smout, A. (2018). *Facebook faces small but symbolic UK fine over data protection breaches*. Available online: <https://www.reuters.com/article/us-facebook-privacy-britain/facebook-faces-small-but-symbolic-uk-fine-over-data-protection-breaches-idUSKBN1K033N>.

---

Solove, D. (2015). *The growing problems with the sectoral approach to privacy law*. Available online: <https://teachprivacy.com/problems-sectoral-approach-privacy-law/>.

---

Spiegel Online (2011). *The count: Germany launches first census since Reunification*. Available online: <http://www.spiegel.de/international/germany/the-count-germany-launches-first-census-since-reunification-a-761497.html>.

---

SUSEP (2013). *RESOLUÇÃO CNSP No 297, DE 2013*. Available online: <http://www2.susep.gov.br/bibliotecaweb/docOriginal.aspx?tipo=1&codigo=31579>.

---

Swiss Re Institute (2017). *World insurance in 2016: The China growth engine steams ahead*. No 3/2017. Available online: [https://www.tsb.org.tr/images/Documents/Teknik/sigma3\\_2017\\_en.pdf](https://www.tsb.org.tr/images/Documents/Teknik/sigma3_2017_en.pdf).

---

The Economist (2017). *Genetic testing threatens the insurance industry*. Available online: <https://www.economist.com/finance-and-economics/2017/08/03/genetic-testing-threatens-the-insurance-industry>.

---

The Financial Services Authority (2007). *Financial Services Authority: Treating customers fairly – culture*. Available online: <https://www.fca.org.uk/publication/archive/fsa-tcf-culture.pdf>.

---

The Smart Campaign (2016). *Client protection certification standards: Version 2.0*. Available online: [https://www.smartcampaign.org/storage/documents/Tools\\_and\\_Resources/Standards\\_2.0\\_English\\_Word\\_for\\_Website.pdf](https://www.smartcampaign.org/storage/documents/Tools_and_Resources/Standards_2.0_English_Word_for_Website.pdf).

---

The World Bank Group (2017). *Good Practices for Financial Consumer Protection, 2017 Edition*. Available online: <https://openknowledge.worldbank.org/handle/10986/28996>.

---

The World Bank Group (2018). *Databank: World Development Indicators*. Available online: <http://databank.worldbank.org/data/source/world-development-indicators/preview/on>.

---

Thom, M. (2018). *Role of insurtech in overcoming challenges in microinsurance*. Available online: [https://cenfri.org/wp-content/uploads/2018/05/Role-of-Insurtech-in-overcoming-challenges-in-microinsurance\\_May-2018\\_English.pdf](https://cenfri.org/wp-content/uploads/2018/05/Role-of-Insurtech-in-overcoming-challenges-in-microinsurance_May-2018_English.pdf).

---

Thomson Reuters Practical Law (2018). *Data protection in France: Overview*. Available online: <https://uk.practicallaw.thomsonreuters.com/6-502-1481>.

---

UNCTAD (2018). *Data protection and privacy legislation worldwide*. Available online: [http://unctad.org/en/Pages/DTL/STI\\_and\\_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx](http://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx).

---

Venture Scanner (2018). *Venture Scanner: Insurtech posts*. Available online: [www.venturescanner.com/blog/tags/insurtech](http://www.venturescanner.com/blog/tags/insurtech).

---

Wiedmaier-Pfister, M. and Ncube, S. (2018). *Regulating mobile insurance*. Available online: [https://a2ii.org/sites/default/files/reports/2018\\_05\\_02\\_mobile\\_insurance\\_regulation\\_web.pdf](https://a2ii.org/sites/default/files/reports/2018_05_02_mobile_insurance_regulation_web.pdf).

---

Zensus (2011). *ZENSUS2011: History*. Available online: [https://www.zensus2011.de/EN/2011Census/History/History\\_node.html%20\(Germany%20census\)](https://www.zensus2011.de/EN/2011Census/History/History_node.html%20(Germany%20census)).

---

## APPENDIX A: COUNTRY CASE STUDIES

This section describes the strategies to consumer data protection and privacy followed by insurance regulators across six countries. The section is structured according to the considerations of the decision-making tree introduced in Section 4. Each case study discusses each regulator's mandate, its market context, regulatory context and the tools implemented in its strategy. The country case studies are selected to illustrate a mix of different market contexts (across both developed and developing countries), different regulatory frameworks (across all three legislative approaches) and different regulator strategies employing a range of different implementation tools. The information captured within these case studies is drawn from a combination of discussions with the individual regulators, legislative review and secondary research.



## Australia: Australian Information Commissioner (OAIC)

**Mandate.** There is no separate insurance regulator in Australia, since the twin peaks regulatory structure is in place. As such, the Australian Prudential Regulation Authority (APRA) has a mandate for prudential oversight, while the Australian Securities and Investments Commission (ASIC) has a mandate for market conduct and consumer protection, which also covers the insurance sector (Australian Securities and Investments Commission, 2018 and Australian Prudential Regulatory Authority, 2018).

In terms of data protection and privacy, Australian states legislate for their own data privacy. Nevertheless, the OAIC has a broad mandate, which includes: a) conducting investigations, b) reviewing decisions, c) handling complaints, d) monitoring, e) providing advice to the public, government agencies and businesses, f) issuing and revoking guidelines, and g) making proposals to ministers for legislative change.

**Market context.** In 2017, 40 data breaches were recorded (Gemalto, 2018). Moreover, in 2018, it was revealed that Australia's biggest bank – The Commonwealth Bank – lost the financial records of 19.8 million customers (Collett, 2018). The level of digital connectedness is high, which renders future data breaches likely. To illustrate: In 2017, Australia's Global Mobile Engagement Index (GMEI)<sup>35</sup> score was 4.5 (GSMA Intelligence, 2017). In 2016, there were 110.1 mobile cellular subscriptions per 100 people (The World Bank Group, 2018). In 2017, 88.5% of households had internet access and 86% of households had a computer (ITU, 2017). Almost nine in 10 people (88%) have a social media profile; with 91% of social media users having Facebook profiles, rendering it the most popular platform (Sensis, 2018).

**Regulatory context.** The legislative approach in place in Australia is the omnibus approach, under the Federal Privacy Act of 1988 and its Australian Privacy Principles. There is a strong focus on individual rights, although human rights are not explicitly protected within the Australian Constitution. The domestic legal system that prevails is the common law system.

**Implementation strategy.** ASIC has followed a 'delegate' strategy, largely delegating the regulation of data risks to OAIC. However, OAIC is aiming to create a space to enable ASIC to move towards a 'shape' strategy. Examples of tools implemented include:

*Collaborate:* The OAIC is aiming to create space within the legal environment for unique and tailored data-related regulation for different sectors. As such, the tailoring is driven by the data regulator, rather than the financial regulator and the suggested approach is for sector-specific regulations to fall under the auspices of the information commissioner rather than under the financial regulator.

<sup>35</sup> The GMEI "measures the level of engagement of smartphone and non-smartphone users across a wide array of use cases and services" (GSMA Intelligence, 2017). The score combines usage and frequency; a higher score indicates that consumers are more likely to engage in mobile services frequently (GSMA Intelligence, 2017).

## Germany: The Federal Financial Supervisory Authority (BaFin)

**Mandate.** Germany's BaFin is the financial sector regulator that oversees banks, financial institutions and insurers (but not insurance intermediaries). Collective consumer protection within the financial services sector is one of BaFin's core tasks, but it has an extensive mandate that includes principle-based supervision, monitoring and conducting investigations.

**Market context.** Risk drivers have already occurred in Germany – one data breach was recorded in 2017 (Gemalto, 2018). The high level of digital connectedness also means that it is highly likely that further incidents will occur in future. For example, in 2017, Germany's GMEI score was 3.9 (GSMA Intelligence, 2017). In 2016, there were 126.3 mobile cellular subscriptions per 100 people (The World Bank Group, 2018). In 2017, 90.8% of households had access to the internet and 91.4% of households had a computer (ITU, 2017). In 2017, 33% of the German population logged onto Facebook at least once a week and 21% logged on daily (ARD/ZDF, 2017).

**Regulatory context.** The omnibus approach prevails in Germany, since it is subject to the EU-wide GDPR. In terms of societal norms, there is a strong focus on individual rights and privacy is enshrined as a basic right in Article 10 of the Constitution, 1949. The domestic legal system in place is the civil law system.

**Implementation strategy.** Given that BaFin falls under an omnibus approach and both regulates and supervises in a way that enables them to deal with specific data protection issues in insurance, within the context of this framework, they fall under the 'shape' approach. With its BDAI report, BaFin actively engaged with the financial industry in discussions about possible benefits and risks arising from the use of Big Data considering the financial regulatory framework.

*Regulate:* There is relevant data protection requirements, beyond the overarching data laws. The regulatory framework contains requirements considering the system of governance of a supervised entity<sup>36</sup>, its risk management<sup>37</sup> and IT systems<sup>38</sup>. BaFin can employ certain measures available within the framework of the supervisory abuse control to sanction insurers when systematic irregularities concerning insurer's data protection are found ("Missstandsaufsicht")<sup>39</sup>.

In the private insurance sector, the principle of equal treatment is a legal requirement for life, substitutive health, nursing care and casualty insurance with premium refund<sup>40</sup> as well as mutual insurance companies<sup>41</sup>. Furthermore, Section 19 in conjunction with 20 of the General Equal Treatment Act limits different treatments based on religion, disability, age or sexual identity in private insurances to differences based on approved principles of risk-adequate calculation, i.e. an actuarial risk assessment using statistical surveys (protection from arbitrary discrimination in the private insurance sector).

<sup>36</sup> For example, Section 23 of the German Insurance Supervision Act – VAG.

<sup>37</sup> For example, Section 26 VAG, Art. 258 Delegated Act (EU) 2015/35 – DVO.

<sup>38</sup> Art. 258 lit. h and j DVO.

<sup>39</sup> See Section 298 et seqq. of the German Insurance Supervision Act.

<sup>40</sup> See Sections 138 (2), 146 (2), 147, 148, 161 (1) Insurance Supervision Act (VAG).

<sup>41</sup> Section 177 (1) VAG.

*Supervise:* BaFin plays a supporting role to the Federal Commissioner for Data Protection and Freedom of Information (BfDI) in implementing and enforcing data protection laws. BaFin (2018) also emphasises that the use of automated processes does not transfer the responsibility of the results and the process itself away from providers' senior management and that these processes must be "embedded in an effective, appropriate and proper business organisation". As such, firms are not permitted to use "black box excuses" – in other words, they have a responsibility to make sure that "BDAI<sup>42</sup>-based decisions" are comprehensible to third-party experts (BaFin, 2018).

*Advise:* Through its innovation hub, BaFin assists firms with compliance with GDPR as well as other regulation.

## Kenya: Insurance Regulatory Authority (IRA)

**Mandate.** The IRA has a mandate for consumer protection and to encourage market development (Insurance Regulatory Authority, 2018).

**Market context.** Two data breaches were recorded in Kenya in 2017 (Gemalto, 2018). Moreover, during the same year, the opposition presidential candidate, Raila Odinga, claimed that "the electoral commission's IT system has been hacked to manipulate the election results" (BBC, 2017). Kenya's GMEI score was 1.5 in 2017 (GSMA Intelligence, 2017). In 2016, there were 80.4 mobile cellular subscriptions per 100 people (The World Bank Group, 2018). According to ITU, in 2017, 22.3% of Kenyan households had internet access and 14.8% of households had a computer (ITU, 2017). In 2016, Kenya had 5.3 million monthly active Facebook users, which translates to approximately 11% of the population (Shapshak, 2016 and The World Bank Group, 2018).

**Regulatory context.** At present, there is no data protection regulation in place. Nevertheless, the Data Protection Bill was tabled in Parliament in 2015 and was published for public consultation in June 2018. In terms of societal norms and domestic legal system, respectively, Article 31 of the Kenyan Constitution specifically protects the right to privacy and the common law system operates in Kenya.

**Implementation strategy.** The IRA has followed a 'create' strategy. In the absence of a data protection and privacy legislative framework, the IRA has amended regulation to deal with data related risks to consumers. Examples of tools implemented include:

*Regulate:* The IRA is amending and reinterpreting existing market conduct guidelines to ensure appropriate consumer protection against arising data risks. The amendments are explicitly aimed at taking proposals in pending data regulation into account, to ensure consistency when the Act comes into effect. Moreover, as per stakeholder interviews, the IRA is considering the need for harmonisation with global regulations and guidelines.

<sup>42</sup> Big data and artificial intelligence.

## Mexico: Comisión Nacional de Seguros y Fianzas (CNSF)

**Mandate.** The CNSF is responsible for regulating the insurance and surety bond markets, as well as for promoting the development of both sectors. CNSF is also responsible for overseeing the operation of both industries to ensure that all companies comply with the country's regulatory framework (Comisión Nacional de Seguros y Fianzas, 2018).

In terms of data protection and privacy, the data regulator is the Federal Institute for Access to Information and Data Protection or IFAI (Instituto Federal de Acceso a la Información y Protección de Datos). Its mandate includes: a) ensuring compliance with data protection laws, b) enforcing data protection, c) implementing verification and sanctions procedures, and d) developing and promoting analysis of and research into personal data protection.

**Market context.** Risk drivers have already been reported in the Mexican market – two data breaches were recorded in 2017 (Gemalto, 2018). The GMEI score for Mexico was 2.1 in 2017 (GSMA Intelligence, 2017). In 2016, there were 87.6 mobile cellular subscriptions per 100 people (The World Bank Group, 2018). Of households in Mexico, 47% had internet access and 45.6% had a computer in 2017 (ITU, 2017).

**Regulatory context.** The omnibus approach, under the Federal Law on the Protection of Personal Data Held by Private Parties (Ley Federal de Protección de Datos Personales en Posesión de los Particulares) is present in Mexico. Article 6 of the Mexican Constitution (2010) states that individuals have the right not only to privacy but also to the protection of their personal data and the right to access, rectify, oppose and cancel personal data under the terms specified by the federal laws. The civil law system prevails. In addition, due to the fact that the US and Canada are key trading partners within the North American Free Trade Agreement (NAFTA), policymakers and regulators in Mexico may be under pressure to harmonise their approach with US and Canadian laws.

**Implementation strategy.** On the basis of its legal mandate, the CNSF must follow a 'delegate' strategy, with consideration for Mexico's Federal law on the Protection of Personal Data Held by Private Parties to sufficiently deal with the risks in the insurance sector. Examples of tools implemented include:

*Monitor:* The CNSF is monitoring the prevalence and impact of data risks in its market, which includes conducting research on these risks and considering regulations implemented in other jurisdictions.

## South Africa: Financial Sector Conduct Authority (FSCA)

**Mandate.** There is no separate insurance regulator in South Africa as the twin peaks regulatory structure is in place. The South African Reserve Bank (SARB) has a mandate for prudential oversight, while the FSCA has a mandate for market conduct and consumer protection, which also covers the insurance sector.

In terms of data protection and privacy, the Information Regulator is the South African data regulator, but the body has yet to come into operation. Once formally established its mandate will include: a) providing education relating to the protection and processing of personal information, b) monitoring and enforcing compliance with the provisions of POPI, c) consulting with interested parties and acting as mediator, d) receiving, investigating and attempting to resolve complaints, e) issuing enforcement notices and codes of conduct, and f) facilitating cross-border cooperation.

**Market context.** Seven data breaches were recorded in South Africa in 2017 (Gemalto, 2018). The GMEI score was 2.3 in 2017 (GSMA Intelligence, 2017). In 2016, there were 147 mobile cellular subscriptions per 100 people (The World Bank Group, 2018). Of South African households, 53% had internet access and 24% had a computer in 2017 (ITU, 2017).

**Regulatory context.** The legislative approach in place in South Africa is the omnibus approach, under POPI. To date, many sections of the personal protection legislation have not yet come into effect but it is expected to come into operation by the end of 2018. The right to privacy is considered a fundamental human right and enshrined, along with many other individual rights, in the Bill of Rights of the South African Constitution. The domestic legal system that prevails is the common law system.

**Implementation strategy.** The FSCA has taken a very active role in the regulation of data risks, following a 'shape' strategy, especially in implementing requirements in the interim period before all of the provisions of POPI become operational. The FSCA has employed regulatory tools to supplement the existing omnibus framework and intends to engage actively with the data regulator once it is formally established. Examples of tools implemented include:

*Regulate:* The FSCA has issued various rules and regulations relating to data privacy and protection including: a) FAIS conduct requirements – requiring consent before information may be disclosed, b) Policy Holder Protection Rules – relating to the sharing of data in groups or partnerships, to be implemented in early 2020, c) TCF principles – requiring that insurance providers target positive consumer outcomes as a priority, and d) under the Financial Sector Regulation Act of 2017, which established the twin peaks system, requirements prescribe how conglomerates share information in groups, however this is monitored by SARB – the prudential authority.

*Coordinate:* The FSCA has a unit that comments on legislation such as POPI while awaiting the formal establishment of the data regulator. Once established, the unit expects to engage actively with the data regulator.

## The Philippines: The Insurance Commission (IC)

**Mandate.** The IC regulates and supervises the insurance, pre-need and HMO industries. Its objective includes establishing a sound national insurance market while safeguarding the rights and interests of the insuring public. The IC's extensive mandate includes the promulgation and implementation of insurance policies, rules and regulations; examination of the business methods of its licensees; and adjudication of claims and complaints related to insurance contracts.

With regard to data protection and privacy, the National Privacy Commission (NPC), established in 2016, is mandated to administer and implement the provisions of the Data Privacy Act of 2012, and to monitor and ensure compliance of the Philippines with international data protection standards. In 2016, in accordance with its mandate, the NPC issued implementation rules and regulations of the Data Privacy Act.

**Market context.** According to Gemalto (2018), there was one breach recorded in the Philippines during 2017. The GMEI score for the Philippines was 2.2 in 2017 (GSMA Intelligence, 2017). In 2016, there were 109.4 mobile cellular subscriptions per 100 people (The World Bank Group, 2018). In the Philippines, 39.1% of households had internet access and 34% of households had a computer in 2017 (ITU, 2017).

**Regulatory context.** The Philippines follows an omnibus approach by means of its Data Privacy Act, which was implemented in 2012. In terms of societal norms, there is a strong focus on privacy as a fundamental right, enshrined both expressly in the Privacy Act and implicitly in the Constitution (Article III, Section 3), which protects the privacy of personal communication and correspondence. The domestic legal system in place is a hybrid, but it is predominantly a civil law system.

**Implementation strategy.** The IC has followed a 'shape' strategy by employing regulatory tools to augment the existing omnibus legislative framework and by actively coordinating with the NPC to promote data protection and privacy. Examples of tools implemented include:

*Regulate:* The IC issued guidelines extending the scope of the national data protection and privacy regulations to insurers specifically.

*Coordinate:* While there is no formal rule or agreement between the two regulators, the IC coordinates with the NPC in the promotion of data protection and privacy.

## The USA: The National Association of Insurance Commissioners (NAIC)

**Mandate.** The NAIC is the US standard-setting and regulatory-support organisation. It is governed by the chief insurance commissioners from the 50 states, the District of Columbia and the five US territories and ensures relatively uniform standards across states. The overarching mandate of the individual insurance commissioners is to protect consumers. This includes overseeing insurer solvency, licensing agents and brokers, performing market conduct reviews, resolving consumer complaints, and investigating and prosecuting insurance fraud.

**Market context.** In 2017, 1,453 data breaches were recorded in the US, many of which occurred in the financial sector (Gemalto, 2018). For example, Equifax, one of the three main credit reporting agencies in the US, experienced a breach which compromised the personal information of 143 million consumers (Gressin, 2017). Insurance providers are also explicitly targeted in US breaches – in 2015, for example, Anthem, a health insurer in the US, discovered that it had suffered a significant cyber security breach, which affected 78.8 million consumer records (California Department of Insurance, 2017). What is more, the level of digital connectedness in the US is high, which renders further incidents almost a certainty. In 2017, the US had the third highest GMEI score – 4.7 (GSMA Intelligence, 2017). In 2016, there were 122.9 mobile cellular subscriptions per 100 people (The World Bank Group, 2018). In 2017, 84% of households had access to the internet and 87% of households had a computer (ITU, 2017). Of adults in the US, 68% reported that they used Facebook in January 2018, which corresponds to the percentage reported in April 2016 (Gramlich, 2018).

**Regulatory context.** The prevalent legislative approach in the US is sectoral and there is no data regulator. The US tends towards favouring: a) individual rights and b) a libertarian approach, as is evident in the Declaration of Independence (1776), which states that: a) “all men are created equal... with certain unalienable Rights, that among these are Life, Liberty and the pursuit of Happiness” and b) “...whenever any Form of Government becomes destructive of these ends, it is the Right of the People to alter or to abolish it”. Given that the common law system is in place in the US, ongoing tort cases (including the Equifax breach) will set the precedent for the quantification of liability from data breaches.

The state legislature is responsible for drafting insurance regulation. Each state’s insurance commissioner operates under that particular state’s insurance legislation, but individual insurance commissioners can contribute to insurance-specific data protection legislation by means of its membership to NAIC. Furthermore, the Gramm-Leach-Bliley Act of 1999, also known as the Financial Modernization Act, also applies to insurance companies, requiring them to communicate to customers how they share and protect personal information among other things.

**Implementation strategy.** The NAIC has followed a ‘create’ strategy. Operating under a sectoral approach, NAIC has drafted new regulation to address data protection and privacy for the insurance sector. Examples of tools implemented include:

*Regulate:* NAIC completed its drafting of a Data Security Model Law in October 2017, which addresses consumer data protection and privacy in the insurance sector. The state of South Carolina has already adopted the model law and a few other states, including Rhode Island and Vermont, have indicated that they are in the process of adding it to their legislative calendars. The Model Law makes provision for enforcement by the regulator and for penalties to be issued.

## APPENDIX B: LIST OF LAWS CITED

<b>Angola</b>	Data Protection Law, 2011
<b>Argentina</b>	Personal Data Protection Law, 2000
<b>Australia</b>	Constitution, 1900
	Federal Privacy Act, 1988
	Australian Privacy Principles, 2014
<b>Canada</b>	Privacy Act, 1985
<b>European Union</b>	General Data Protection Regulation, 2016
<b>France</b>	Public Health Code, 2018
<b>Germany</b>	Constitution, 1949
	General Equal Treatment Act, 2006
	Insurance Supervision Act, 2000
<b>Israel</b>	Protection of Privacy Law, 1981
<b>Mexico</b>	Constitution, 1917
	Federal Law on the Protection of Personal Data Held by Private Parties ( <i>Federal de Protección de Datos Personales en Posesión de los Particulares</i> ), 2010
	Regulations to the Federal Law on the Protection of Personal Data Held by Private Parties ( <i>Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares</i> ), 2011
<b>Morocco</b>	Data Protection Act, 2009
<b>Philippines</b>	Constitution, 1986
	Data Privacy Act, 2012
<b>Rwanda</b>	Data Revolution Policy, 2017
<b>South Africa</b>	Constitution, 1996
	Protection of Personal Information Act, 2013
	Financial Sector Regulation Act, 2017
<b>Ukraine</b>	Protection of Personal Data Law, 2010
<b>United Kingdom</b>	Magna Carta, 1215
<b>United States:</b>	Declaration of Independence, 1776
	Gramm-Leach-Bliley Act, 1999
	NAIC Data Security Model Law, 2017



## APPENDIX C: LIST OF ORGANISATIONS INTERVIEWED

Name of organisation	Individual	Country	Type of organisation
Bermuda Monetary Authority (BMA)	Marcelo Ramella	Bermuda	Supervisor
Comisión Nacional de Seguros y Fianzas (CNSF)	Denise Garcia	Mexico	Supervisor
Consultative Group to Assist the Poor (CGAP)	David Medine	Global	Consultant
Consultcolors	Michael Rothe	UK	Consultant
Discovery Limited	Leanne Jones	South Africa, UK, USA, China, Singapore and Australia	FSP
Financial Conduct Authority (FCA)	Paul Worthington	UK	Supervisor
Financial Sector Conduct Authority (FSCA)	Caroline da Silva Farzana Badat Jacky Huma	South Africa	Supervisor
Inclusivity Solutions	Jeremy Leach Tyler Tappendorf	Kenya and Rwanda	FSP
Insurance Commission of the Philippines (IC)	Denis Cabucos	Philippines	Supervisor
Insurance Regulatory Authority (IRA)	Elias Omondi	Kenya	Supervisor
Inter-African Conference on Insurance Markets (CIMA)	Luc Noubissi	Benin, Burkina Faso, Cameroon, Central African Republic, Comoros, Chad, Côte d'Ivoire, Gabon, Guinea, Equatorial Guinea, Mali, Niger, Senegal and Togo	Supervisor
Marsh Africa	Christelle Marais	Botswana, Egypt, Malawi, Namibia, Nigeria, South Africa, Uganda, Zambia, Zimbabwe	FSP
NuvaLaw	Hendrik Kotze	South Africa, Netherlands and UK	FSP
Private	David Watts		Consultant
Private	Louis de Koker		Consultant
Superintendência de Seguros Privados (SUSEP)	Gustavo Caldas Gabriel Costa Natalie Hurtado	Brazil	Supervisor
The Federal Financial Supervisory Authority (BaFin)		Germany	Supervisor
The National Association of Insurance Commissioners (NAIC)	Gita Timmerman Timothy Mullen	USA	Supervisor

The Initiative is a partnership between:



Hosted by:




Access to Insurance Initiative  
Hosted by GIZ Sector Project  
Financial Systems Approaches to Insurance  
Deutsche Gesellschaft für Internationale  
Zusammenarbeit (GIZ) GmbH  
Dag-Hammarskjöld-Weg 1-5  
65760 Eschborn, Germany

Telephone: +49 61 96 79-1362

Fax: +49 61 96 79-80 1362

E-mail: [secretariat@a2ii.org](mailto:secretariat@a2ii.org)

Internet: [www.a2ii.org](http://www.a2ii.org)

 [a2ii\\_org](https://twitter.com/a2ii_org)

Promoting access to responsible, inclusive insurance for all.