access to insurance initiative

What is the role of insurance regulators in dealing with consumer data protection risks arising from increased data availability and usage?

Early findings, May 2018

Introduction

Growth in consumer data collection and use: A changing global paradigm. Across industries, businesses are collecting, storing and using increasing amounts of consumer data. This has been made possible by the growth in the reach of the internet, particularly through smartphone penetration, and the increased capacity to collect and share data on individuals. The technological developments in data analytics have increasingly allowed businesses to use this data to better understand consumers to design products suited to their individual needs and to micro-target advertising. The increasing amount of data available on individual consumers, combined with these improved data-processing tools, has enabled the monetisation of consumer data, as businesses recognise its value.

This data space bringing with it major new risks to consumers. The relative recency of many of these developments means that, in many countries, regulation to deal with these new risks is still "catching up" or does not exist yet. The nature of the largest data collectors, who rely on a global network, renders them unrestricted by national and/or regional borders, which creates further complexities for regulators.

How this is relevant for insurance regulators

New data able to open new consumer markets. Across emerging insurance markets, the use of insurance remains limited. A lack of reliable data on consumers and the risks they face often requires insurers to charge higher premiums to account for the uncertainty of the risks, and it limits their ability to understand consumers' needs. Leveraging these vast new datasets means that insurers can price more accurately for risk, can better understand their consumers' needs and accordingly design better products, and can better monitor and reduce the incidence and cost of fraud. The implication is that embracing the use of new datasets has the potential to substantively increase insurance inclusion.

Increased use of data enabling more accurate pricing of risk, which can improve product value to consumers, but can also increase the risk of discrimination and exclusion of customers. While there are many potential benefits to consumers from insurers making increased use of data, it also raises the risk of consumers being excluded from insurance cover because of tailored or differentiated risk selection based on "big data" that deems certain customers too risky. As risk is more accurately modelled, high-risk customers are more likely to be priced out of the risk pool or even entirely excluded if no regulation exists to mitigate against such practices. Consumers' decision-making heuristics may also be exploited, as data enables providers to better understand these on an individual level.

The considerations regarding the use of data are not a consideration for the distant future. It is important that insurance regulators already consider their response in the short term.

The insurance industry already collecting sensitive personal data on its customers. The use of data to understand and model risk is the very basis on which the insurance industry has been built. Datasets, like mortality tables, enable insurers to model and price for risk on life policies. Market research data, like demand-side surveys and qualitative interviews, enables insurers to better understand their consumers

Supported by

cenfri · fsdafrica · UKaid from the British people · BMZ Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung · Ministry of Foreign Affairs of the Netherlands · IAIS International Association of Insurance Supervisors

and so design better products. The collection of Know Your Customer (KYC) data is a regulatory requirement under AML/CFT legislation in most jurisdictions. Therefore, insurers are already collecting and storing personal information on their customers, even if they are not all using it to a great extent.

Large amounts of personal consumer data, relevant to insurers, already being collected by third parties in developing countries. Even in relatively less developed insurance markets, global technology and data platforms (like the FANGs[1]) and local technology-related firms (like MNOs) are already collecting personal information on both existing and potential insurance clients that is highly relevant to insurers. While insurers in many developing markets may not yet be using this data to any significant extent, it is highly likely that they will increasingly do so in the near future. In many insurance markets, insurers are already partnered with some of these third parties, and data sharing is increasingly common and set to increase. A number of insurers are already leveraging satellite/aerial imagery collected by external providers to facilitate claims processing (Smit et al., 2017). Other examples include health wearables[2], telematics[3], artificial intelligence[4], social scoring, social media, location data and genome mapping. As such, it is important for regulators to be prepared and to ensure that appropriate regulatory frameworks be in place.

The objective of this research study

Defining data-related risks within inclusive insurance, exploring arising consumer protection issues and generating practical insights on how regulators can deal with emerging risks. Insurance regulators are often ill-equipped to understand and deal with the range of emerging risks. Furthermore, in most jurisdictions, data protection regulation falls under the mandate of the communications or data regulator. As most of these data issues are cross-cutting (not just across the financial sector but often across the entire services sector), the insurance regulator is frequently in a challenging position to deal with these data-related risks. This study will therefore aim to unpack and define the different data-related risks within inclusive insurance, explore the consumer protection issues that arise, consult supervisors from different regions on their experiences and approaches in this regard, and generate practical insights to inform guidance to regulators on how to deal with these emerging risks. This note should be considered as the research team's initial findings. They will be augmented and adjusted through additional research and interviews.

[1] Facebook, Amazon, Netflix and Google

[2] Discovery Vitality, for example, is an add on service (or loyalty program) for Discovery insurance in South Africa. Vitality collects data on your health indicators, how often you go to the gym, what types of groceries you buy, what time of medicine you buy at the pharmacy etc, and uses that information to start nudging you to adopt healthier habits by setting goals for improved health (completing assignments, exercising, quitting smoking, eating healthy food etc). They then reward you for hitting your goals by offering money back on healthy groceries, money back on preventative care items at pharmacies, reduced gym membership fees if you regularly attend and discounts at retailers if you achieve your previous week's health target. The program encourages healthy behaviour among customers, improving health outcomes and in turn reducing medical costs to the insurer over the long term (Nordin, 2017).

[3] CarIQ, for example, is an Indian-based telematics platform that enables car owners to track and assess their driving behaviour behaviour. They are partnering with insurance companies to use their system to offer usage based insurance. Motor insurance companies can then price premiums based on the driving behaviour (Nordin, 2017).

[4] ToGarantido, Brazil's largest online microinsurance broker, have partnered with Fred Chatbots, for example, to offer a 100% digital sales process through using chatbots and artificial intelligence. The chat bot can learn with time what specific categories of customers are more likely to purchase and to tailor messaging and product promotions. The chat bot increases the efficiency and reduces the cost of the sales process whilst providing a personalised sales experience to consumers (Nordin, 2017).

The key consumer risks affecting the insurance industry

Six core risks to consumers. Figure 1, below, provides a simplified snapshot of the major risks that may arise from insurers' use of consumer data and of the primary drivers of these risks.

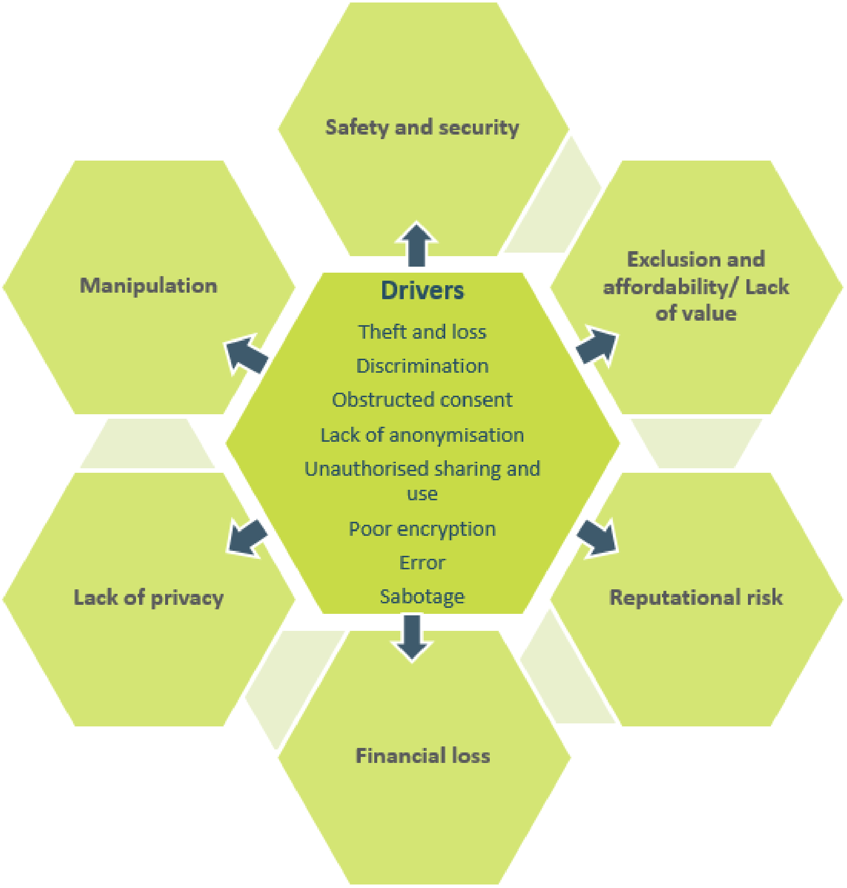


Figure 1: Key risks and primary drivers

Source: Authors' own based on AIG, 2013; Armerding, 2017; Isaca, 2012; Newman, 2002; Ovelami, 2014; Uydess et al., 2018

Six core risks to consumers arise, which are applicable for insurers and the insurance industry (AIG, 2013; Armerding, 2017; Isaca, 2012; Newman, 2002; Ovelami, 2014; Uydess et al., 2018):

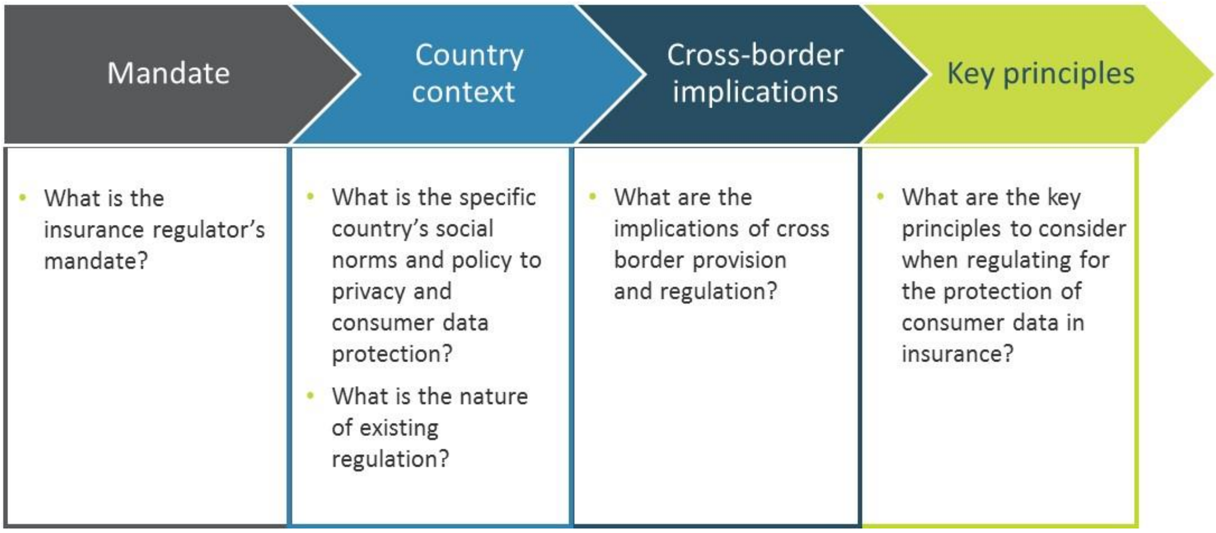
- *Safety and security.* Poorly encrypted data has the potential to reveal sensitive information about a client (including physical location), which could be used for malicious harm against the individual.
- *Exclusion and affordability; Lack of value.* Consumers are at risk of being excluded from insurance cover because of tailored or differentiated risk selection based on "big data". This differentiated and automated analysis of risk could exclude clients who are deemed too risky. Applying a similar principle, providers that can perfectly price for individuals' risks and willingness

to pay can charge individualised premiums equivalent to consumers' maximum willingness to pay for the risk cover.

- *Reputational risk.* Personal information can be used, either intentionally or unintentionally, to harm a consumer's reputation. This could be through the theft of data but may also apply when providers share or use sensitive personal data like health information.
- *Financial loss.* Data used to exploit consumers (particularly when stolen) inflicts financial loss on individuals.
- *Loss of privacy.* Individual privacy is encapsulated as a fundamental human right in the constitution of many jurisdictions. The collection and analysis of individual data can undermine this privacy.
- *Manipulation* refers to the increasingly discreet way of not only influencing but also eliminating options that a consumer has access to by using collected consumer data to influence consumers' behaviour and decision-making.

The role that insurance regulators can play in addressing these consumer risks

Key considerations for insurance regulators. An insurance regulator's role in, and approach to, dealing with these data risks hinges on its mandate and the regulatory context in which it operates. Figure 2, below, highlights four key considerations for insurance regulators as they deliberate on an appropriate approach to deal with these consumer risks.



Mandate	Country context	Cross-border implications	Key principles
• What is the insurance regulator's mandate?	• What is the specific country's social norms and policy to privacy and consumer data protection? • What is the nature of existing regulation?	• What are the implications of cross border provision and regulation?	• What are the key principles to consider when regulating for the protection of consumer data in insurance?

Figure 2: Considerations for insurance regulators

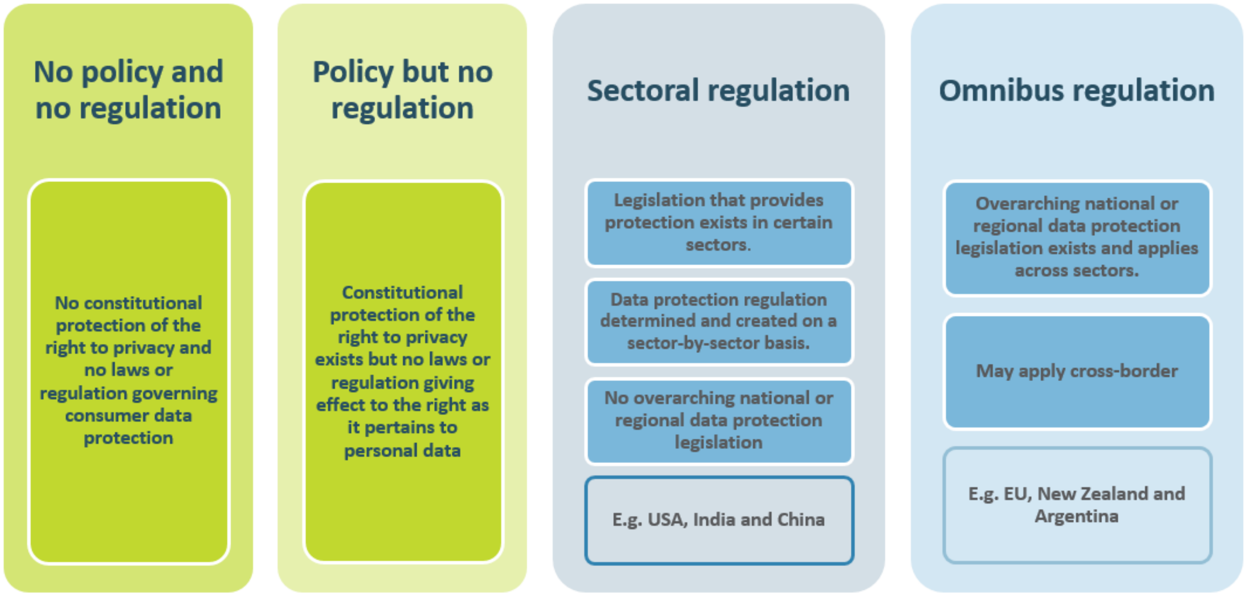
Source: Authors' own

The extent to which the regulator's mandate permits and requires it to engage with the benefits and risks that arise from increased use of consumer data. Regulators are usually created by acts of Parliament that also define their mandate and scope of activities. Regulators with a purely prudential oversight mandate may have limited authority to consider consumer protection risks, rendering this matter largely peripheral to their core focus. Most insurance regulators' mandates are not limited to purely prudential oversight; however, many are required to also consider market conduct, thereby ensuring that consumers are sufficiently protected from arising risks. Increasingly, the mandates of financial regulators (including insurance regulators) extend even further, beyond a focus on prudential and market conduct regulation and supervision. Market development is a "broader" mandate that is increasingly observed – the insurance regulator in India, for example, is even officially called the Insurance Regulatory and Development Authority (IRDA). Although regulators never lose sight of their responsibility to regulate the market and ensure its stability, the activities of regulatory authorities that have an explicit market development mandate would include supporting innovation and the development of innovative providers. The implication is that, when regulating data use within their industry, regulators with a broader mandate would be required to explicitly consider the trade-off between i) the potential of increased use of data to develop the industry and ii) the increased risks to consumers. Insurance regulators with a narrower mandate may not consider this trade-off as explicitly.

Country context determining the type and nature of the role that the insurance regulator can play to regulate data use in the industry. The existing regulatory landscape is fundamental for insurance regulators when they consider their role and approach to regulating for consumer data risks. Consideration must be given both to their country's social norms or policy position relating to data privacy and to the nature of existing (or lack of) data protection regulation:

- ***Social norms*** relate to the relative importance of individual privacy within a country. This is often enshrined in the constitution. Social norms can vary between i) considering individual privacy as a paramount human right (such as in the EU) and ii) placing relatively greater emphasis on business development and group rights. The latter emphasis implicitly asserts that allowing greater use of individual data will lead to greater benefits for society as a whole (through, for example, better product design) than protecting individual privacy will. Social norms will fall across a spectrum, and it is important for any given insurance regulator to understand its country's position to appreciate what is appropriate within that environment regarding the regulation of data.

- The existing ***data protection regulatory system*** differs across countries. Many, especially developing countries, do not have explicit data protection and data privacy regulations in place. Among those countries that do have such regulation in place, the approach to data regulation falls into two categories: sectoral and omnibus. Under the sectoral approach, data protection regulation is determined and created on a sector-by-sector basis. In contrast, under an omnibus approach, overarching national or regional data protection legislation exists and applies across sectors. The scope of responsibility for the insurance regulator will directly depend on the existing data protection regulatory system. Figure 3, below, illustrates these different categories, with examples.



No policy and no regulation

No constitutional protection of the right to privacy and no laws or regulation governing consumer data protection

Policy but no regulation

Constitutional protection of the right to privacy exists but no laws or regulation giving effect to the right as it pertains to personal data

Sectoral regulation

Legislation that provides protection exists in certain sectors.

Data protection regulation determined and created on a sector-by-sector basis.

No overarching national or regional data protection legislation

E.g. USA, India and China

Omnibus regulation

Overarching national or regional data protection legislation exists and applies across sectors.

May apply cross-border

E.g. EU, New Zealand and Argentina

Countries falling into a particular category may have draft or pending legislation, which – once in operation – may change the applicable framework category

Figure 3: Categorising regulatory systems to data protection

Source: Authors' own based on DLA Piper (2018) and Deloitte (2017)

Under an omnibus regime, an insurance regulator may act as an advisor to the data regulator or even lobby for specific or unique data protection regulation for the insurance industry, whereas under a sectoral approach or in a jurisdiction without existing data protection regulation, the insurance regulator will have a responsibility to consider and implement appropriate regulation for the insurance sector.

The ease with which data flows across borders: requiring regulators to deliberate on the cross-border implications of regulation. Most of the largest collectors of personal data are supranational and serve customers across multiple jurisdictions. In contrast, most insurance regulators are limited to a single regulatory jurisdiction. Increasingly, consideration will need to be given to how to facilitate effective coordination between individual regulators that must regulate large, borderless data collectors. The EU's recently enforced General Data Protection Regulation (GDPR) is an important example of the need for individual regulators to consider existing global regulations and the implications thereof. Article 3 of the GDPR expands its territorial reach to apply not only to data processors and controllers established in the EU but also to those that are either offering goods or services to EU residents; or monitoring EU residents' behaviour occurring within the EU (GDPR, Regulation EU 2016/679). This may have far-reaching implications for individual insurance regulators.

Key principles for regulating data protection tending to be common across countries with relevant regulation; though implementation differs based on country context. An understanding of where the country is situated (both in terms of social norms and in terms of the regulatory approach) relative to other countries will enable developing-country insurance regulators that are implementing data protection regulations to draw on appropriate regulatory principles from other jurisdictions. The key principles for consideration in the regulation of data protection include (DLA Piper, 2017; 2018; GDPR, Regulation EU 2016/679; Deloitte, 2017; UNCTAD, 2016):

- ***Data-handling requirements*** relate to requirements in respect of *inter alia* the collection, processing and storage of consumer data. Such requirements may include restricting the collection of only certain specific data, only using it for a specific purpose and only storing it for a certain (specified) period.
- ***Informed consent requirements*** consider the freedom of the consumer (data subject) to give consent and to understand the consequences thereof, and for such consent to be requested in clear and plain language.
- ***Defining personal and sensitive data.*** Many jurisdictions distinguish between personal and sensitive data, often having more onerous requirements or putting in place greater restrictions on the use of sensitive data in order to protect consumers. A common distinction made between the two includes the consideration of personal data as data with which a person can be identified, whereas data is considered sensitive where the distribution thereof may lead to harm or, more specifically, discrimination.
- ***Reasonable use*** refers to the use of consumer data only in the context of the use of the data for which consent was specifically provided, for the purpose of which the consent specified, and to the extent to which consent was given.
- ***Security mechanisms*** include the protection of consumer data by means of, for example, deanonymisation and encryption. In this way, consumers should not be able to be identified by their data in the event of a breach.

Conclusion

The increasing collection, storage and use of consumer data offers insurance and the insurance industry new opportunities to reach new customers, design new products, improve efficiencies and offer greater value. However, this brings with it a range of consumer risks for which regulators must consider what response is appropriate. The role of the insurance regulator in dealing with these emerging risks may differ substantially based on its own mandate and its country’s existing regulatory system. It is important that individual regulators give due deliberation to each of the considerations outlined to develop an approach appropriate for their specific regulatory contexts.

The concepts outlined in this note should merely be considered as the research team’s initial findings. They will be augmented and adjusted through additional research and interviews. Anyone who wishes to contribute to this research project, should please contact Stefanie Zinsmeyer at stefanie.zinsmeyer@giz.de or Jeremy Gray at jeremy@cenfri.org.

References

AIG. 2013. Cyber and Data Security Risks and the Real Estate Industry. [online] Available at: https://www.aig.com/content/dam/aig/america-canada/us/documents/business/industry/aig-cyber-edge-whitepaper-final-brochure.pdf

Armerding, T. 2018. The 5 worst big data privacy risks (and how to guard against them). [online] CSO Online. Available at: https://www.csoonline.com/article/2855641/privacy/the-5-worst-big-data-privacy-risks-and-how-to-guard-against-them.html

Deloitte., 2017. Privacy is paramount: personal data protection in Africa. Johannesburg: Creative Services at Deloitte.

DLA Piper., 2017. Data protection laws of the world. Available from: https://www.dlapiperdataprotection.com/system/modules/za.co.heliosdesign.dla.lotw.data_protection/functions/handbook.pdf?country=all

ISACA, 2012. Top Ten Big Data Security and Privacy Challenges. [online] Available at: https://www.isaca.org/Groups/Professional-English/big-data/GroupDocuments/Big_Data_Top_Ten_v1.pdf

Newman, N. 2013. The Costs of Lost Privacy: Consumer Harm and Rising Economic Inequality in the Age of Google. WILLIAM MITCHELL LAW REVIEW, Volume 40, Issue 2, 2014. Available at SSRN: https://ssrn.com/abstract=2310146 or http://dx.doi.org/10.2139/ssrn.2310146

Nordin, K. 2017. Data: Consumer insights to client value and business viability. [online] available at: https://cenfri.org/wp-content/uploads/2017/11/Insurance-for-development-Kigali-learning-session_i2i_August-2017.pdf

Oyelami, J. 2018. Managing the Theft and Sabotage of Information: An Organizational Case Study on Information Security Breaches and Rick Analysis. [online] Available at: https://ijcsits.org/papers/vol4no62014/5vol4no6.pdf

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) Official Journal of the European Union, Vol. L119 (4 May 2016), pp. 1-88.

Smit, H., Denoon-Stevens, C. and Esser, A. 2017. InsurTech for Development: A review of insurance technologies and applications in Africa, Asia and Latin America. [online] Available at: https://cenfri.org/wp-content/uploads/2017/11/InsurTech-Research-Study_March-2017.pdf

UNCTAD., 2016. Data protection regulations and international data flows: Implications for trade and development. Switzerland: United Nations Publication.

Uydess, A., Blackburn, W., Grojean, A. and Johnson, S. (2018). Cambridge Analytica Scandal: Don’t Blame Facebook. Blame Bad Ethics.. [online] Intouch Solutions. Available at: https://www.intouchsol.com/wp-content/uploads/Blog/PDFs/CambridgeAnalyticaPOV_IntouchSolutions.pdf