IAIS
INTERNATIONAL ASSOCIATION OF INSURANCE SUPERVISORS

aii 10 years
access to insurance initiative

Regulating InsurTech: Role of the regulator in managing data risks and protecting consumers

Report of the A2ii – IAIS Consultation Call

JAN
2019

The Consultation Calls are organised as a partnership between the Access to Insurance Initiative (A2ii) and the International Association of Insurance Supervisors (IAIS) to provide supervisors with a platform to exchange experiences and lessons learnt in expanding access to insurance.

Introduction

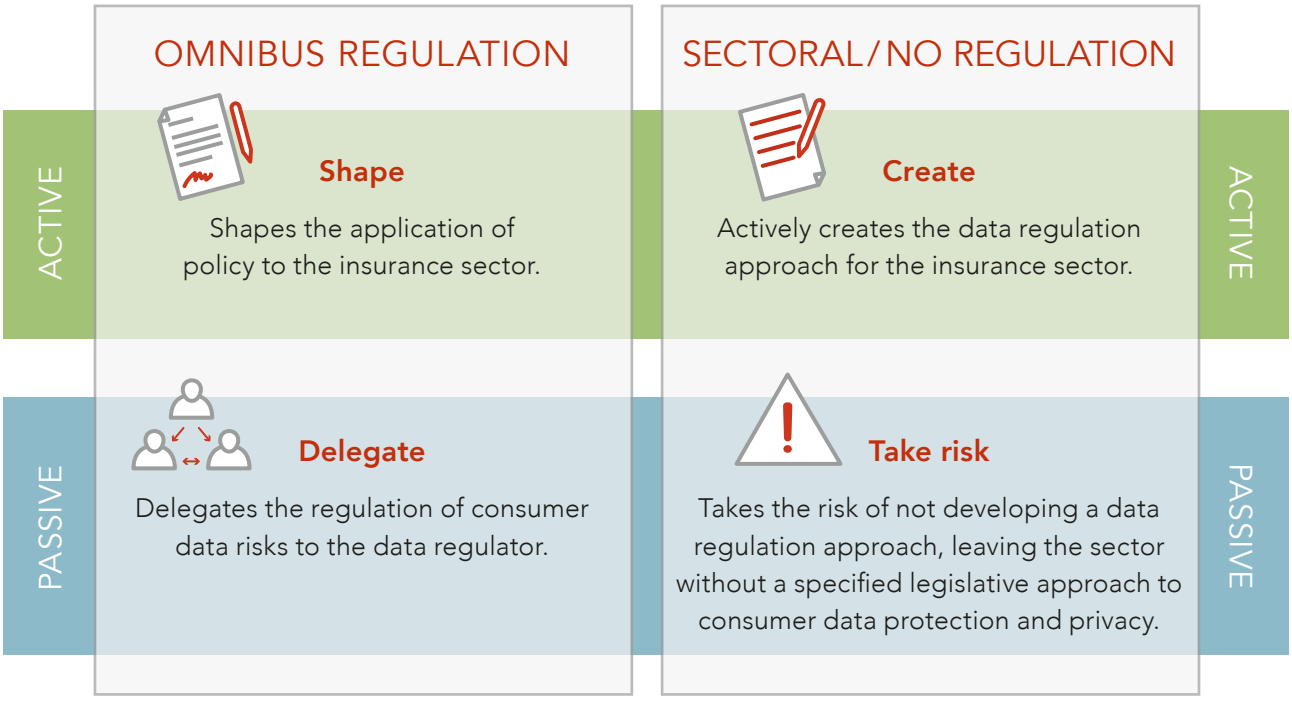
Globally, the pace at which technological change is occurring is more rapid than ever witnessed before. This has been complemented by the increasing use of large amounts of data. Big data[1] is now a prominent concept. Insurers and tech firms can store and use this data to better understand consumers and therefore develop better products and services. While data-driven technology has fostered an expanding innovation landscape, bringing with it the potential to improve value to consumers, it also leaves consumers vulnerable to new threats. As InsurTech companies develop new business models and use data to improve consumer experience and to cut administrative costs, consumer data is subject to risk, such as where cases of data breaches have been reported. Data-driven product development could also lead to certain customer segments facing higher premiums, being priced out of the risk pool or simply not being offered insurance.

This call was based on A2ii's thematic report on "Regulating for responsible data innovation." We encourage readers to read the report here. Based on the study, expert presenters on the call, Stefanie Zinsmeyer and Andrea Camargo, gave an overview of the main consumer data risks and the role that the regulator can play in dealing with these risks. The following authorities also shared their experiences: Elias Omondi from The Insurance Regulatory Authority (IRA, Kenya) and Tim Mullen from the National Association of Insurance Commissioners (NAIC, USA) highlighted the approaches that have been adopted to address consumer data protection and privacy concerns in their jurisdictions. Kathleen Koehn from The Federal Financial Supervisory Authority (BaFin, Germany) also gave an overview of BaFin's Study on "Big Data Meets Artificial Intelligence."

1 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" (Gartner, 2018). Examples include individual data on social media activity, call logs on a mobile phone and internet search history, among others. See the A2ii publication "Regulating for responsible data innovation" report here.

Brief overview of the study "Regulating for responsible data innovation"

In facilitating innovation, insurance regulators have to strike the balance between achieving positive consumer outcomes and protecting consumers. Key negative outcomes that may arise for insurance consumers are compromised safety and security, exclusion and lack of value, reputational risk, financial loss, the loss of privacy and manipulation. These outcomes may arise from risk drivers such as inadequate data governance and controls, error, involuntary or uninformed consent, unauthorised sharing and use, and data breaches.
The study identifies three legislative approaches that are prevalent globally: omnibus regulation, sectoral regulation and no existing regulation. The response of the insurance supervisor depends on its legislative context and constraints, within which there are four broad implementation strategies – shape, create, delegate and take risk.



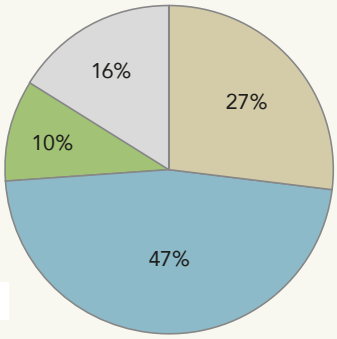
- Omnibus regulation – Cross-cutting data protection regulatory framework. Often also has a dedicated regulatory authority. e.g. in EU, South Africa, New Zealand and Argentina
- Sectoral regulation – No overarching national/regional data protection legislation. Each sectoral regulator is responsible for addressing data protection and privacy e.g. in USA, India and China
- No regulation – No laws/regulation governing consumer data protection and privacy e.g. in Kenya

Source: Regulating for Responsible Data Innovation (A2ii, 2018)

During the consultation call, supervisors also responded to a quick poll that sought to capture how regulators deal with consumer data risks and regulation. The questions and responses are as illustrated in the charts below:

How high or low do you assess consumer data risks in your jurisdictions?

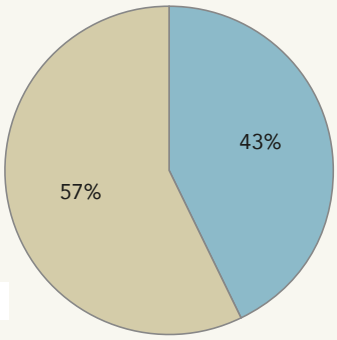
- Very high
- High
- Low
- Very low



79 Responses

Has your authority taken an active approach on data regulation ("shapes" or "creates" data regulation)?

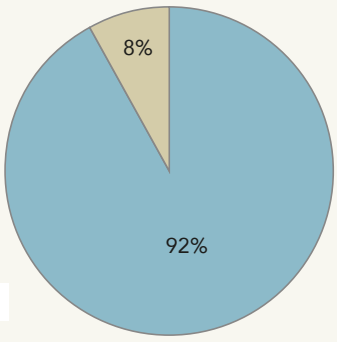
- Yes
- No



69 Responses

Do you think your authority should become more active in data protection?

- Yes
- No



64 Responses

CASE STUDY: KENYA

The Kenyan case study was presented by Elias Omondi from the Insurance Regulatory Authority of Kenya.

Currently, Kenya does not have a specific data protection legislation in place. However, a data protection bill was tabled in parliament in 2015. The focus on driving financial inclusion and building the innovation space in Kenya has allowed the entrance of new business models, but has also raised questions on how to provide coverage, promote innovation and competition while at the same time ensuring that consumers are protected. In this regard, the Insurance Regulatory Authority of Kenya (IRA) has three main roles when it comes to balancing between consumer risks and benefits:

- Maintenance of a fair, safe and stable insurance sector
- Protect the interest of insurance policyholders and beneficiaries
- Promote the development of the insurance sector

In the absence of an explicit data protection regime, the IRA follows a 'create' strategy to deal with data-related risks to consumers. The implementation strategies that IRA have adopted include:

- **Market Conduct Guidelines:** This entails amending and interpreting existing market conduct guidelines to ensure appropriate consumer protection against arising data risks
- **Treating Customers Fairly Model:** The TCF Model of Consumer Protection aims to raise standards in the way firms carry on their business by introducing changes that will benefit consumers and increase their confidence in the financial services industry
- **Regulatory Sandbox:** The IRA has developed a draft regulatory sandbox policy. The policy will allow for an experimental environment to exist where FinTech/InsurTechs can test new ideas and innovations in product design, product development and distribution with the ability to contain the consequences of failure.
- **Insurance Products Guidelines:** The guidelines offer guidance on principles to be adhered to in product design, pricing, marketing, disclosures and how applications for issuance of new and repackaged products are made to the regulator, including allowing for a company to pilot test the new products.

For questions or more information on IRA's approach, please contact
eomondi@ira.go.ke

CASE STUDY: GERMANY

Kathleen Koehn from The Federal Financial Supervisory Authority of Germany (BaFin) presented brief insights and key findings from the BaFin's study on Big Data Meets Artificial Intelligence.

The key questions that BaFin sought to address when developing the study are: What would be the possible impact of the use of big data, big data analytics and artificial intelligence on the financial market as well as on BaFin, as the supervisor? What would be the nature of supervision in future and would regulatory requirements need to adjust?

The study highlights that early supervisory and regulatory attention is key in the cycle of innovation especially in cases that entail the use of big data and artificial intelligence. This is because the use of big data and tools related to big data have a self-enhancing and self-supporting effect, in that consumers quickly engage in new digital processes, products and services, which in turn generates more data that companies can use. It is therefore vital for supervisory authorities to act early. The use of big data could have an impact on financial stability, micro-prudential supervision and consumer protection. Some of the regulatory principles that BaFin has applied in dealing with advances in big data and artificial intelligence include; being technology-neutral for all market players i.e. "same business, same risks, same regulation/rules," adopting a principle-based regulatory framework where all risks of new technologies are considered and developing big data and artificial intelligence capabilities as a supervisor.

For an in depth view of BaFin's study on "Big Data Meets Artificial Intelligence" the study can be accessed directly here.

CASE STUDY: USA

The USA case study was presented by Tim Mullen from the National Association of Insurance Commissioners (NAIC).

In terms of mandate, the NAIC is the U.S. standard-setting and regulatory support organisation in the US. In regulating for responsible data innovation, the NAIC encourages innovation, recognising the consumer benefits can accrue from a changing marketplace and the way insurance companies are operating. However, while encouraging innovation, it remains clear that consumer protection is necessary. To ensure this, the NAIC maintains that insurance companies need to be transparent with regulators in terms of the data and algorithms that firms use and the impact this would have on consumers.

Some consumer benefits that arise from the use of data include more accurate assessments of risk of loss, faster processing of quotes and claims, as well as enhanced risk management and loss prevention. The NAIC also identifies the following consumer concerns: accuracy and completeness of data, disclosure to consumers, consumer consent and privacy and cybersecurity. To address data protection and privacy, the NAIC has adopted various model laws and regulations, including the Standards for Safeguarding Consumer Information Model Regulation (2000), Privacy of Consumer Financial and Health Information Regulation (2002) and the Insurance Data Security Model Law (2017). In addition, the NAIC has under its committee structure several workstreams which are, among other things, reviewing how companies are utilising data and new technologies. This includes an Innovation and Technology Task Force and a Big Data Working Group.

Within the US market context, the NAIC highlighted a data breach case study experienced by a health insurance company in the US, which affected almost 80 million users. In responding to this breach, regulators conducted four stages of an exam:

- **Integration:** This entailed engaging the company personnel and the relevant state jurisdictions in addition to identifying the appropriate cybersecurity expertise needed to deal with the breach.
- **Initial assessment:** Key personnel and the company's cybersecurity experts were interviewed. US Insurance regulators in the corresponding states also obtained pre-breach technical documents and material of the insurer to understand the company's security environment and the efforts that took place post-breach to assess the vulnerabilities.
- **Breach assessment:** The exam team reviewed the company's technical scoping of the data breach, the analysis that was conducted to assess the breach and the technical conclusions that were reached. The examiners also looked at the actions taken by the company to detect, contain and respond to the data breach.

- **Cybersecurity assessment:** Cybersecurity experts conducted an in-depth review of the company's cybersecurity controls that were in place prior to and after the data breach. The cybersecurity experts also performed a test to examine whether the company's cybersecurity protocols were effective to detect and prevent another breach.

The examination findings revealed the response adequacy of the company and its cybersecurity preparedness prior to the breach. The findings showed that the company had an appropriate cybersecurity response program in place and responded rapidly to address the data breach. With regards to the post-breach cybersecurity findings, the company implemented new standards to reduce occurrences of similar types of breaches in the future. The corrective actions taken mostly addressed individual consumers where the company notified affected consumers about ongoing action to address the breach. The company also notified law enforcement and insurance regulators.

For any questions or more information on NAIC's approach and case study, please contact TMullen@naic.org

Questions and Discussion

› **Given the different approaches that regulators apply in addressing data protection and privacy, how does the NAIC cooperate with other actors in the financial sector in the US to deal with cybersecurity cases and other data security and risk concerns?**
State insurance regulators coordinate regularly with federal and state financial regulators to facilitate communication and consider ways to effectively coordinate regulatory approaches to managing and evaluating cybersecurity risk, as well as other data security and risk concerns. This includes going through the FBIIC (Financial and Banking Information and Infrastructure Committee), a committee comprising federal and state financial regulators that was set up to strengthen coordination and communication among financial regulators to improve the reliability and security of the financial sector infrastructure.

› **In applying an omnibus approach to regulation, how does BaFin cooperate with data protection authorities in their jurisdiction?**
The existing legal framework within the German market defines the functions of different authorities. The role of supervising data security does not fall within BaFin's mandate. Therefore, it might be advisable for supervisory authorities to liaise more closely with other competent authorities that are already familiar with new and emerging fields like Big Data and AI. This would foster the exchange of skills, knowledge and opinions and to minimise possible cases of double reporting. BaFin has had a positive experience establishing closer cooperation with the Federal Office for Information Security (BSI).

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@a2iiorg
Internet: www.a2ii.org

a2ii_org

Promoting access to responsible, inclusive insurance for all.