Privacy and data governance:
risk and opportunities for leading insurers

April 2018

Insurance Governance Leadership Network

IGLN

VIEWPOINTS

Privacy and data governance: risks and opportunities for leading insurers

Competitive pressures are driving insurers to seek the greatest possible advantage from the large amounts of data at their disposal. At the same time, security and privacy concerns are limiting their ability to do so. Regulation and customer expectations are elevating standards for privacy and data governance, and insurers need to develop systems, personnel, and governance policies to meet these higher standards. *"Both from a regulatory standpoint and from the point of view of information security and customer expectations, you need to build privacy requirements into the DNA of how you work as an organization,"* a participant said.

"You need to build privacy requirements into the DNA of how you work as an organization."

—Executive

The obligation to safeguard data is made more challenging by the imminent enforcement, on 25 May 2018, of the EU's General Data Protection Regulation (GDPR). The stakes are high. Violations of GDPR could result in fines of up to 4% of global revenues; further, the potential for civil lawsuits in the wake of a data breach multiplies the direct financial risk. Equally significant is the potential reputational damage resulting from a data breach, a high-profile fine, or the misuse of consumer data.

Yet even while they face greater constraints in how customer information can be deployed, insurers are using big data to improve underwriting, risk management, operating efficiency, customer relations, and product innovation. The ultimate challenge for the industry is to manage the tug-of-war between deriving strategic value from data and safeguarding consumers' rights.

IGLN participants met in London on 13 March 2018, to explore these issues. This *ViewPoints* synthesizes the key themes that emerged from those discussions as well as conversations with participants ahead of the meeting:

- **Regulation and consumer expectations are creating challenges for strategic uses of data**
- **Insurers struggle to capitalize on the strategic opportunities afforded by growing data use**

Regulation and consumer expectations are creating challenges for strategic uses of data

New regulations and heightened awareness of privacy issues are altering the landscape for the collection, processing, and use of consumer data. The threat of heavy fines and reputational damage from the loss or misuse of data are focusing senior leaders' attention and shaping the context for how firms approach data governance.

GDPR is raising the bar on privacy and data protection

The GDPR codifies and enshrines new consumer rights and organizational responsibilities. Insurers, like other businesses with customers and operations in the EU, are scrambling to be ready for GDPR implementation and it is high on boardroom agendas. One participant called the regulation *"one of the furthest-reaching pieces of EU legislation ever."*

Among its key provisions, the GDPR does the following:

- Directs that contracts governing consent to use data be clear and easy to understand. Consumers must give unambiguous, affirmative, informed consent; data processors may no longer rely on "opt in by default" or implied consent. Consumers have the right to withdraw consent, a right that must be disclosed before consent is provided.
- Creates new rights, including the right to know whether and how a firm is using an individual's data, rights to data access and portability, and the "right to be forgotten"—to have individual data erased and no longer disseminated.[1]
- Imposes a 72-hour mandatory breach-notification requirement in cases where a breach is likely to "result in a risk for the rights and freedoms of individuals."[2]
- Requires organizations that process large amounts of sensitive personal data of EU residents to appoint a data protection officer, who should report to the "highest management level," which could be the board of directors.[3]
- Imposes heavy penalties for violations, as much as 4% of the firm's annual global revenue or €20 million, whichever is higher.[4]

Although the GDPR only applies to firms that collect personal data on any EU resident, firms outside Europe cannot afford to ignore it. *"Across the globe, organizations that had assumed that GDPR didn't apply to them are realizing that they are processing data on EU citizens,"* one participant said.

"Across the globe, organizations that had assumed that GDPR didn't apply to them are realizing that they are processing data on EU citizens."

—Executive

Moreover, GDPR may represent the leading edge of privacy regulation. A recent analysis noted that the European Union has catalyzed a global dialogue on individual data privacy, and a number of countries—including Canada, Israel, and Japan—are moving to align their privacy laws with the GDPR.[5] Observers expect other countries to follow suit. One participant suggested that just as a number of Asia-Pacific firms adopted capital requirements first imposed in the EU, these firms would also follow the EU's lead on privacy regulation.

Some analysts expect companies, especially smaller ones, to adhere to GDPR worldwide to avoid the expense of running multiple compliance systems.[6] Moreover, GDPR is derived from privacy and data protection principles that enjoy broader social acceptance.

GDPR fundamentally shifts assumptions about data ownership

GDPR, which one participant said embodies *"an extreme view of privacy,"* represents an attempt to put control of data back in the hands of consumers. *"Our legacy, technology, and data systems are built on the assumption we can use all that data,"* a participant said. Now, that assumption is no longer true as GDPR *"brings back rights to the consumer, and says, 'That's our information. I give you information for a specific purpose and entrust it to you to secure it. If you are not doing that, there will be consequences.'"*

"GDPR is not designed for organizations with legacy technologies, where the right to be forgotten cannot be written in."

—Participant

Some participants pointed out, however, that privacy and data protection are not entirely new issues. One regulator said, *"The rules may be changing, but there are data protection issues already today. We always have been and will continue to be interested in data protection."*

Compliance represents a major challenge, especially for insurers

Participants recognized that few insurers, if any, will be fully compliant by the time GDPR goes into force. Even regulatory authorities charged with enforcement acknowledge that many firms will not be ready. One participant reported that the UK Information Commissioner's Office, the national body charged with GDPR enforcement, conceded, *"We know you won't be ready."* Nonetheless, it wants to make sure that organizations are taking steps toward compliance.

Several factors are contributing to compliance challenges:

- **Legacy systems.** Legacy systems make compliance with GDPR requirements, such as the right to be forgotten and data portability, difficult. One executive said, *"GDPR is not designed for organizations with legacy technologies, where the right to be forgotten cannot be written in."*

- **Long-tail data.** GDPR requires that organizations hold data for no longer than is necessary for the purpose for which it was originally obtained. However, as one industry analyst recently noted, insurers have "a completely different perspective on data" than those in other industries: they keep data longer, not only for historical analysis and fraud prevention, but also because of the nature of some insurance products.[7] Within the industry, participants noted that life insurers face a more challenging situation than property and casualty firms. One director said, *"Long-held data in life insurance needs to be well protected for a long time."* Fortunately, regulators *"recognize some data will have an enormous long tail. You may have a legal hold that says you have to keep it or other regulation that says you need to keep it for longer."*

"It is difficult to say we will not do business with a provider if they are not [GDPR] compliant."

—Director

- **Third-party relationships.** Suppliers, cloud providers, and partners all complicate firms' ability to assure compliance. One participant raised the question, *"How do we ensure that insurers and third, fourth, fifth parties are compliant?"* Another noted that their firm is *"asking 1,100 suppliers to use an online tool to help us assess GDPR compliance,"* while another is re-contracting all of the firm's third-party partners. Another participant said, *"It is ludicrous to have to ask all your suppliers to amend their contracts*." While one participant suggested that the risk of noncompliance from a third party might be grounds to contract out of a relationship, another said, *"If a major supplier of our technology is not compliant and there are few companies in the market providing this, it is difficult to say we will not do business with such a provider."* One participant noted, *"It will be impossible to turn all our GDPR programs green, in part because we are unlikely to have gotten evidence from all our outsourcers on the 25th of May.*"

- **Technical challenges.** The mandate for data portability requires that data be easily transferrable between organizations, but standards and protocols have been slow to emerge. One industry observer noted, "It would be wonderful to transfer data to another insurer, but they have their own systems and it will cost an absolute fortune to be able to write the code for all the other potential systems out there to be able to transfer this data."[8]

Consumer expectations create additional challenges

While compliance with GDPR and other regulations is commanding attention, shifting consumer expectations about data privacy and protection are also influencing how organizations collect, store, and use data.

Consumer expectations are changing and inconsistent

Consumer advocates are increasingly expressing concerns about both data privacy and the ethical use of data in the industry. The director general of the European Consumer Organization recently asserted, "Insurance companies are trying to collect data that is not risk relevant and I do not buy the argument that you need to collect more data to enhance the customer experience. You can have a limited amount of data and still maintain a very good customer relationship."[9]

"We sell a promise, and part of that is protecting information."

—Executive

Many consumers are increasingly concerned that large organizations are unable or unwilling to keep their personal information secure. A 2016 survey, for example, found that roughly half of Americans believed their personal information was less secure than it had been five years earlier.[10] High-profile breaches in the intervening months have done nothing to allay their fears.

As with other industries, insurers face inherent tensions around privacy. Consumers often demand an easy and seamless online experience but can be reluctant to provide the data necessary to deliver it. The balance may be shifting with younger consumers, who, as one participant said, *"will trade security for convenience, for less worries, for less work."* Participants speculated, though, that those customers who are *"very willing to give their data"* might change their attitudes if they experience adverse consequences such as failing to gain university admission or employment, or problems securing insurance coverage.

Changing consumer expectations heighten reputational risk

While the fines resulting from GDPR violations could be severe, participants stressed that the reputational damage associated with the loss or misuse of customer data could be even worse. *"In the insurance business we sell a promise, and part of that is protecting information, so we try our best to do that. So it is mostly a reputation and brand issue,"* one participant said.

A vivid demonstration of the reputational risks associated with the misuse of data came not long after IGLN participants met in London, when news broke that a third party had harvested and used Facebook data from 87 million users. This created a reputational crisis at the social-media giant. Numerous high-profile observers called for a boycott of Facebook, the company lost $60 billion in market capitalization in just a few days, and CEO Mark Zuckerberg was grilled by US congressional committees.

Even the prospect of a regulatory fine threatens damage to a firm's reputation. A director said, *"The problem with the fine, and it could be quite a big one, is also the transmission of the idea that you are guilty of not looking*

after customer data as you should; the fine confirms that. That opens you up to claims that you haven't done this properly—it's official—so how the hell do you defend yourself?"

GDPR could alter consumers' views of their privacy rights and may raise additional expectations. To avoid unnecessary reputational damage, insurers will need to educate consumers about the limits of their rights under GDPR and the conditions under which companies can legitimately use individuals' data. For instance, even in the absence of explicit consent, organizations can legally hold and process data in order to fulfill the terms of a contract, to meet a legal obligation, or to pursue a legitimate interest, as long as that interest is necessary and balanced against the rights and interests of the individual. Participants acknowledged, however, that public perceptions of GDPR requirements might be different. One participant suggested, *"Some will want to invoke the right to be forgotten, and bring a lawsuit and ask for that data,"* even where insurers have a right to hold the data in order to provide the customer with the product or service for which they have contracted.

"Will there be companies that try to farm for complaints, and how can we defend ourselves against lawsuits?"

—Director

Insurers can expect opportunistic actors, as with claims-management companies in property and casualty, to push consumers to assert their rights under GDPR, even where the insurers have acted properly. One participant wondered, *"Will there be companies that try to farm for complaints, and how can we defend ourselves against lawsuits?"*

IFRS 17: promoting transparency and comparability?

In a briefing session, participants discussed International Financial Reporting Standard (IFRS) 17, which is "the first comprehensive and truly international IFRS standard establishing the accounting for insurance contracts."[11] The new standard will take effect in 2021, replacing IFRS 4, which, as one participant pointed out, *"is not a consistent standard—it treats insurance products differently in different countries."*

The major goals of IFRS 17 are to improve the transparency and comparability of insurers' financial results and strength. By more accurately capturing the profitability of insurance contracts, and by moving to a more consistent standard, IFRS 17 "*could improve the level of transparency and remove the 'opacity discount' that exists for insurers.*" This, it is hoped, will promote comparability, both between insurers and with firms in other industries. One participant explained, *"Transparency without comparability is a waste of effort. Investors ask for*

IFRS 17: promoting transparency and comparability?

transparency, but what they really want is something they can understand so they can decide where to deploy capital, which requires comparability."

IFRS 17 has three major components: new approaches to provisioning, which mostly affect property and casualty; the contractual service margin, which allows for some smoothing revenue in life contracts; and the recognition of profit over the lifetime of a contract.

The jury is out on whether IFRS 17 will succeed, especially in enhancing comparability. Some participants suggested that IFRS 17 might fail in its major objectives, primarily because it gives companies some discretion on the timing of revenue and profit when calculating the contractual service margin. On the other hand, one participant suggested that although insurers' financial statements might be *"less comparable now, they will be more comparable in the long run."* Another asserted that *"it will drive more comparability eventually"* while also acknowledging the complexity of insurance accounting: *"If you want an economic measure that also smooths profits and brings that together in a complex insurance product, you can't avoid the complexity."*

Participants largely agreed that, whatever its flaws, IFRS 17 will be the only viable accounting standard for the industry. *"At this stage,"* one participant said, *"it's IFRS 4 or IFRS 17,"* and most agreed that staying with the status quo is not an option.

Insurers struggle to capitalize on strategic opportunities afforded by growing data use

"Using data doesn't have to stop—it can continue, but with the right controls."

—Executive

While focused on compliance, legal, and reputational issues, insurers are also looking to identify positive aspects of data governance through an improved user experience, more tailored products, and more accurate pricing of risk.

IGLN participants emphasized that the dramatic increase in the amount and kind of data available to insurers represents a significant change in the way insurers are doing business. One said, *"For my first 20 years in the industry, what I did would have been familiar to an underwriter working 100 years ago. In the last few years, it's fundamentally changed. The potential for disruptive change and the societal implications are profound."*

Another participant, however, pointed out that insurers have always used data in underwriting. *"We've always asked family history, which is a primitive*

kind of genetic data, so it's a matter of working out boundaries like we've always done. Using data doesn't have to stop—it can continue, but with the right controls."

Several participants suggested that the legal and reputational risks associated with collecting, storing, and using data might prevent companies from taking advantage of opportunities created by the availability of the data. One director said, *"On my board, I'm keen that all conversations around data focus on the opportunities that data brings as well as the challenges and threats we all face. We want to be focused on what could be growing; however, we also want to lock everything down, and that is squeezing out positive conversations that could lead to positive outcomes."* Other participants warned that data protection regulation *"has the potential to limit innovation"* and noted that differences in requirements could make some countries and regions less competitive. One participant said, *"The fact that data may not be used as fully in the EU or the UK is a serious innovation disadvantage versus the US."*

At the same time, according to one participant, tougher data protection regulation is forcing companies to focus on the customer and consider *"how customer data comes into our organization, how we deal with it internally, and how we share it."* This renewed focus on customer data may generate important insights for companies: *"Understanding where their data resides has got companies thinking about what the customers will want and putting the customer journey at the forefront, asking what customers expect, what's our brand, what are the expectations customers have of us."*

"The pursuit of data could drive both good and bad outcomes for customers."

—Executive

Participants identified several strategic opportunities arising from the improved use of data:

- **Improved customer experience.** One industry executive pointed out, *"It's about being able to use data to provide seamless products and services to customers in a quick and easy fashion."* An executive said that as a customer, *"you should only have to call one time with a change of address. We can share your information across the businesses; the customers expect that, and we are allowed to do that because we are serving the customer. We are bringing down the silos to share data across the company to serve the customer."*
- **More accurate risk identification.** Advanced data technologies can permit better analysis of risks. One director described a recent development: *"We realized that the incidence and severity of car accidents had increased"* because of the prevalence of distracted driving. They further realized the

need to segment the risk of distracted driving *"in a new and different way, as opposed to just younger drivers versus older drivers—a lot of that distracted driving is around phones and people using GPS for directions and looking down, so we are putting cameras in cars to pick up on that distracted driving."*

- **Better customer identification and segmentation.** Better data has the potential to both widen and narrow the scope of coverage by generating a more nuanced understanding of risk pools. One participant said, *"The pursuit of data could drive both bad and good outcomes for customers."* For example, as another pointed out, *"A genetic test can show not only that someone is uninsurable—it can also bring into the pool those who you thought were uninsurable."*
- **New types of coverage.** More data can enable insurers to develop new product lines for specific types of consumers. For example, insights from telematics that monitor driving habits can enable insurers to offer usage-based policies. A participant said, *"One thing that's coming is per-kilometer charging. That's great for me, but not so good for the insurance companies: I don't drive a lot, I live in the city, I'm absolutely that customer. These technologies are going to change everything."*

***

Insurers recognize that data strategy will be a critical part of their future success or failure. As a result, GDPR and larger issues around privacy and data governance are important in the boardroom. One executive noted, *"This gets a lot of board time. We have 99 different compliance issues mapped across different work streams, clustered by themes."* Another said, *"Risk appetite discussions related to data use need to take place at the board."*

As regulation and consumer expectations demand greater privacy control and better data governance around the world, failure to comply with regulations or a major data breach could bring substantial fines and, more importantly, significant reputational damage. Successful business models will require the ability to gather and analyze data on a massive scale. Whether and how well firms will be able to do so while balancing evolving notions of privacy and individual rights to their data remains an open question.

Regulatory developments

Over dinner, participants discussed emerging issues in insurance industry regulation, focusing on the themes of conduct regulation and regulatory consistency and convergence.

While there are no major developments in prudential regulation on the immediate horizon, participants expect continued developments in conduct regulation. Prudential regulation is largely a matter of, in the words of one participant, *"an adaptation of the current system with no great changes"* through the implementation of the EU's Solvency II Directive. However, conduct regulation remains high on the agendas of politicians and regulators, particularly in the following areas:

- **Pricing.** One regulator, noting that insurers often charge a premium on renewal pricing and sometimes use other factors to set prices, such as time of day or device used to request a quote, asked, "*What constitutes fairness in pricing?*" Industry leaders saw the value of regulatory involvement in pricing, with one participant saying, "*Pricing is a tough one. It's a classic prisoner's dilemma, so you want regulators to step in. But* how *you want the regulator to step in is the question. The challenge is finding the right price for value.*"
- **Fintech.** The emergence of fintech firms and technological innovations in product design and distribution raise additional regulatory questions: *"What is the scope of regulation? Who is within the scope? Where is the boundary? The value chain is changing, so how we supervise how they're using big data or algorithms raises big challenges."* Another regulator noted that regulators were working with *"early-stage firms to experiment with new products that bring new challenges."*
- **Insurance Distribution Directive.** This EU directive, according to one regulator, *"is changing the way the insurance business is done"* by *"creating a bridge between governance and how you manage the business and how you design your product. Product design has to be high on the board's agenda, and it has to put the customer at the center."*

Regulatory consistency and convergence, while widely desired, face significant roadblocks because of varying supervisory cultures and unpredictable political developments. One participant noted, *"The regulators are generally working well together, but the politics are so different."* Another said, *"Different jurisdictions have different cultures and capacities for supervision, so the question is how to put them together in a way to have a common culture of supervision."* Brexit will heighten these challenges, but it is unlikely to lead to a serious relaxation of the UK regulatory regime, with one

Regulatory developments

participant suggesting that post-Brexit standards will be *"significantly similar, but there will be changes around the margins."*

About ViewPoints

ViewPoints reflects the network's use of a modified version of the Chatham House Rule whereby names of network participants and their corporate or institutional affiliations are a matter of public record, but comments are not attributed to individuals, corporations, or institutions. Network participants' comments appear in italics.

About the Insurance Governance Leadership Network (IGLN)

The IGLN addresses key issues facing complex global insurers. Its primary focus is the non-executive director, but it also engages members of senior management, policymakers, supervisors, and other key stakeholders committed to outstanding governance and supervision in support of building strong, enduring, and trustworthy insurance institutions. The IGLN is organized and led by Tapestry Networks, with the support of EY. ViewPoints is produced by Tapestry Networks and aims to capture the essence of the IGLN discussion and associated research. Those who receive ViewPoints are encouraged to share it with others in their own networks. The more board members, members of senior management, advisers, and stakeholders who become engaged in this leading-edge dialogue, the more value will be created for all.

About Tapestry Networks

Tapestry Networks is a privately held professional services firm. Its mission is to advance society's ability to govern and lead across the borders of sector, geography, and constituency. To do this, Tapestry forms multistakeholder collaborations that embrace the public and private sector, as well as civil society. The participants in these initiatives are leaders drawn from key stakeholder organizations who realize the status quo is neither desirable nor sustainable and are seeking a goal that transcends their own interests and benefits everyone. Tapestry has used this approach to address critical and complex challenges in corporate governance, financial services, and healthcare.

About EY

EY is a global leader in assurance, tax, transaction, and advisory services to the insurance industry. The insights and quality services it delivers help build trust and confidence in the capital markets and in economies the world over. EY develops outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, EY plays a critical role in building a better working world for its people, for its clients, and for its communities. EY supports the IGLN as part of its continuing commitment to board effectiveness and good governance in the financial services sector.

Appendix: Discussion participants

On 13 March in London, Tapestry and EY hosted an IGLN meeting on GDPR, privacy, and data governance. In the meeting and in preparation for it, we conducted numerous conversations with directors, executives, regulators, supervisors, and other thought leaders. Insights from these discussions inform this *ViewPoints* and quotes from these discussions appear throughout.

The following individuals participated in these IGLN discussions:

IGLN Participants

- Claudia Arney, Governance Committee Chair, Aviva
- Marty Becker, Board Chair, QBE
- Doug Caldwell, Chief Risk Officer, Transamerica
- Jan Carendi, Senior Advisor, Sompo Holdings
- Lawrence Churchill, Senior Independent Director, Bupa
- Angela Darlington, Chief Risk Officer, Aviva
- David Fried, Advisor, QBE
- Sheila Hooda, Non-Executive Director, Mutual of Omaha
- Keith Jackson, Director of General Insurance and Protection, Financial Conduct Authority (UK)
- Bill Kane, Audit Committee Chair, Travelers
- Paul Matthews, Executive Mentor and Advisor, Merryck & Co
- Eileen Mercier, Audit Committee Chair, Intact Financial
- Mike Morrissey, President and CEO, International Insurance Society
- Fausto Parente, Executive Director, EIOPA
- Kevin Parry, Senior Independent Director, Standard Life Aberdeen
- Bertrand Peyret, Director of Insurance Supervision, ACPR (France)
- Sabrina Pucci, Non-Executive Director, Generali Group
- Eric Spiegel, Audit Committee Chair, Liberty Mutual
- Tim Tookey, Chief Financial Officer, Old Mutual Wealth
- Cathy Wallace, Chief Risk Officer, State Farm

EY

- Shaun Crawford, Global Insurance Leader
- Cheryl Martin, Partner, FSO UK Insurance - Cyber Security & GDPR Lead
- Phil Vermeulen, Partner, EMEIA Insurance - Finance, Risk and Actuarial Leader

Tapestry Networks

- Dennis Andrade, Partner
- Eric Baldwin, Senior Associate
- Jonathan Day, Vice Chair and Chief Executive
- Simon Wong, Partner

Endnotes

[1] "GDPR Key Changes," EU GDPR Portal, accessed 15 April 2018.

[2] "GDPR Key Changes," EU GDPR Portal.

[3] EY, *GDPR: Demanding New Privacy Rights and Obligations Perspectives for Non-EU Financial Services Firms* (London: EYGM Limited, 2017).

[4] "GDPR Key Changes," EU GDPR Portal.

[5] Nuala O'Connor, "Reforming the U.S. Approach to Data Protection and Privacy," Council on Foreign Relations, 30 January 2018.

[6] AP, "Watch out, Facebook: How New EU Data Rules May Reach the US," *CBS News*, 26 March 2018.

[7] Cintia Cheong, "Insurers Struggle to Interpret GDPR," *Insurance ERM*, 12 September 2017

[8] Cheong, "Insurers Struggle to Interpret GDPR."

[9] Paul Walsh, "Further Research Needed to Safeguard 'Black Box' Insurance Data" *InsuranceERM,* 22 November 2017.

[10] Kenneth Olmstead and Aaron Smith, "Americans and Cybersecurity," Pew Research Center, 26 January 2017.

[11] IFRS Foundation, *IFRS 17: Insurance Contracts* (London: IFRS Foundation, May 2017), 2.