GDPR goes global

INSURANCE HORIZONS SERIES

13 MAR 2019

By: James Clark | Jim Halpert | Marcella Hill | Paula Mena Barreto

The introduction of the EU General Data Protection Regulation (GDPR) in May 2018 represented, for many insurance companies, the culmination of a multiyear transformational compliance project. Now, as we approach GDPR's first year anniversary, the regulatory trend that began in the EU looks set to spread across the globe.

In this article, we examine how the insurance sector may be affected by significant new privacy laws in California, Brazil and India. We do so in the context of three key issues at the confluence of privacy and insurance:

- Data-led decision making
- Customer rights
- Data breaches and liability

The impending wave of new laws modeled, to a greater or lesser extent, on GDPR promises both benefits and drawbacks for insurance companies. The laws bring well-documented compliance challenges, including in respect of notice, consent, individual rights and data breach reporting. But as more countries bring their standards broadly in line with the EU, companies have an opportunity to adopt a more global, harmonized and consistent approach to privacy compliance.

Data-led decision making

Data has always been vital to insurance: accurate customer profiles and well-developed actuarial models help to drive better risk assessments, more accurate pricing and, ultimately, more profitable businesses. And there have never been more opportunities to collect data about customers. Third-party providers specialize in delivering access to rich databases that pull data from a range of sources, and insurers can collect additional data directly from customers through a variety of methods, such as personal fitness devices, telematics boxes in cars, or the location settings on mobile apps.

Big data not only helps with underwriting and premium setting; it can lead to superior recognition of fraudulent claims. The validity of a claim may be gauged in part by an analysis of anything from your social media footprint to your credit score. Even your voice – captured when you notify your claim – may be analyzed for red flags that denote fraud propensity.

When big data analytics is looking to pull in data from a wide range of sources, it is vital to understand which elements are regulated as personal data. GDPR's definition of personal data is notoriously broad. The definition of *personal information* under the California Consumer Privacy Act 2018 (CCPA) is, however, wider even than GDPR's, and potentially covers de-identified data, provided it simply relates to, describes, or is capable of being associated with a particular consumer, device or household. This could present challenges for big data analytics, which often relies on de-identified or indirectly identifiable information, including in contexts such as actuarial analysis.

In data-rich environments like insurance, regulators are acutely focused on transparency and the duty of businesses to explain how and why personal data is used in clear but comprehensive terms. Privacy notices under GDPR are required to contain a wealth of information, and businesses can struggle to balance this with the competing requirement for accessibility.

The privacy notices required under CCPA are less detailed those under GDPR. The notice, however, relates to data practices over the previous 12 months, and CCPA is highly prescriptive as to how the notice and a *do not sell my personal information* link (see below) must be presented. California residents may also request detailed additional information relating to the sharing or selling of personal information. Unlike GDPR, CCPA requires a business to specify whether personal information has been sold, and whether it has been disclosed to third parties for business purposes.

Customer rights

Under GDPR, we have seen an expansion and strengthening – and greater awareness – of personal privacy rights. Insurance companies now face customers who are empowered to access, correct, restrict and in some cases erase the personal data held on them by those companies, and to object to certain forms of processing, such as profiling and automated decision making.

Each of these rights has the potential to create challenges for the industry. Imagine a claimant who disputes the handling of their claim, and then submits a subject access request in order to obtain access to their claim file, including all relevant email correspondence. Consider also the importance of an insurer being able to retain policy data for actuarial purposes, and then square this with the implications of a wide-ranging erasure request from an outgoing policyholder. Finally, consider the right for an individual to object to, and request human intervention in respect of, certain automated decisions, such as a computer algorithm used in a claims management process.

Many of the new privacy laws take influence from GDPR's emphasis on individual rights. For example, Brazil's new General Data Protection Law, which comes into force in February 2020, provides individuals with rights regarding access, rectification, erasure, objection, and data portability. Just as with GDPR, insurance companies will need to consider what these rights mean in an insurance context. For example, when will the erasure of policyholder data be possible, and when will such a request be impossible on the grounds of necessity to comply with competing laws and regulations, or to provide the requested insurance service?

CCPA is more distinct from GDPR in the area of data subject rights. Indeed, there are several GDPR data subject rights that have no equivalent under CCPA. These include the right to object, to the restriction of processing, and not to be subjected to automated decision making. Conversely, there are some CCPA rights that do not (expressly) feature in GDPR. For instance, the right to opt out will allow consumers or designee organizations to direct, at any time, a business to cease selling their personal information. Trade in personal information is, of course, prevalent in the insurance industry, from insurers looking for large datasets to bolster underwriting and actuarial models, to claims management companies buying leads.

Although a data subject may be able to achieve this same objective under GDPR, the right under CCPA is distinct in that it provides a direct path to preventing the sale of personal information. In this light, businesses must provide a link on their website homepage entitled *do not sell my personal information*. Further, CCPA expressly prohibits price discrimination against consumers who choose to exercise a right, while allowing companies to offer fair and reasonable incentives to those who opt in to the sale of their data. Under GDPR, although price discrimination would be challenging (for instance, as a contravention of the fairness principle), it is not explicitly prohibited.

In India, the draft Personal Data Protection Bill 2018, which is still in the early legislative stages, omits a number of GDPR

rights. These are the right not to be subjected to automated processing, the right to object and the right to opt out of direct marketing. The right to access is limited to a brief summary of personal data and its processing. In contrast, the right to rectification goes further than under GDPR, and requires any third-party recipients to be notified of amendments made to the personal data. Similarly, the right to data portability is also broader than GDPR, encompassing personal data that the controller has generated or added themselves.

Data breaches and liability

The widely reported potential for significant liability under GDPR (whether from a regulatory fine or a group claim from affected data subjects) is both an opportunity and a threat for the sector. At the same time as the industry has worked hard to strengthen its own compliance and increase readiness for data breaches, brokers and sales teams have also been driving a huge growth in cyber and privacy coverage. The companies purchasing this coverage are nervous about the twin threat of tightening privacy legislation, and ever more prevalent and sophisticated cyberattacks that target a company's information systems.

In relation to data security breaches (a major, but by no means exclusive cause of liability under privacy laws), we again see some parallels with GDPR. Under Brazil's new law, it is mandatory to report personal data breaches, and these must be notified in a reasonable time period to the competent authority. In California, data breach notification requirements actually predate both CCPA and GDPR, such notifications being a well-established principle in the US.

Looking at liability more broadly, though there are notable differences between the three new laws, the GDPR model of creating powerful incentives for compliance is apparent in each. CCPA provides for fines (up to US$7,500 per intentional violation, and US$2,500 per unintentional violation), and allows individuals to file class action lawsuits for minimum statutory damages in the event of a notifiable data breach. True class action claims for significant statutory damages are also permitted under CCPA. As an opportunity for the industry, it is worth noting that class action damages and defense costs are generally insurable losses, whereas state attorney general fines and civil penalties are generally not.

In India, the fines that can be imposed pursuant to the Personal Data Protection Bill mirror those under GDPR (i.e. up to 4 percent of worldwide annual turnover). Although purportedly independent, the Data Protection Authority of India, which will impose these fines, will be bound by any written requirements of the government on questions of policy, and such requirements are unlikely to be subject to judicial review. This is in stark contrast to the position in the EU, where supervisory authorities are obligated to act with complete independence.

Finally, in Brazil, entities that infringe the new General Data Protection Law can be penalized with a number of sanctions, including the simple or daily fine of up to 2 percent of the company's (or group's) preceding year's gross sales in Brazil, up to a limit of R$50 million.

Conclusion

In an increasingly data-driven industry, comprehensive laws regulating the use of personal information have the potential to cause significant repercussions. However, the considerable time and resource in working towards GDPR compliance can be a shortcut regarding conformity with new laws that often overlap with GDPR in key areas. By building increasingly consistent global privacy programs (which are nevertheless sensitive to important gaps between the laws), insurance companies can be more efficient in their approach. These laws present an opportunity to help customers to manage the risk of exposure in a tightly regulated new environment through new forms of coverage.