MAYER·BROWN

@ INSURANCE SNAPSHOT.
TECHNOLOGY & INNOVATION NEWS & VIEWS

January 14, 2019

Keeping It Private: GDPR and Developments in Data Privacy in 2018

By Larry Hamilton, Charles-Albert Helleputte, Sanjiv Tata, Oliver Yaros, Kendall C. Burman, Diletta De Cicco and Evan M. Wooten[1]

By any measure, 2018 was a major year for data privacy regulation. The most significant regulatory development in this area was the European Union's General Data Privacy Regulation ("**GDPR**"), which went into effect on May 25, 2018 and establishes what is probably the most rigorous data protection regime currently in existence. As adopted, GDPR includes numerous restrictions on the use of individual personal data, coupled with an expansive extraterritorial reach that makes compliance with its provisions a concern for many business who maintain even relatively minor connections with the European Union. Also in 2018, the State of California enacted the California Consumer Privacy Act ("**CCPA**"), which establishes a data protection regime that is in many ways inspired by GDPR and will come into effect on January 1, 2020.

GDPR and the heightened restrictions it establishes regarding the use of personal information will have a major effect on insurance industry participants that are subject to GDPR and to regulatory initiatives in other jurisdictions, such as California, that choose to adopt a similar framework. The collection and use of personal information is a core business practice of the insurance industry worldwide. Personal information is obtained by insurance companies, agents, brokers and other service providers in order to design, underwrite and distribute insurance products and services to consumers. Consequently, a data protection regime that could restrict such entities in accessing and processing personal information would require significant reevaluation of their foundational operational practices.

The General Data Privacy Regulation

GDPR is the result of a multi-stage negotiation process among the members of the European Union, originally proposed by the European Commission to replace the 1995 European Directive (95/46/EC) (the "**Directive**"), which set out the previously existing data protection regime for the European Union. Adopted by the European Parliament and the Council of the European Union on April 14, 2016, GDPR became enforceable on May 25, 2018. As a regulation (as opposed to a directive) it is directly binding and applicable in all Member States of the European Union.[2]

GDPR defines personal data as "information relating to an identified or identifiable natural person,"[3] and establishes a number of protections for and restrictions on use and transfer of such personal data. Crucially, GDPR sets a very low bar for what is considered "identifiable": if a natural person can be identified using "all means reasonably likely to be used,"[4] the information would be

considered "personal data." Accordingly, data may be considered personal data even if the entity holding such data cannot itself identify the natural person to whom such data pertains. Indeed, the name of a natural person would not be required to establish that information is "personal data" – any identifier, including an identification number, location data, online identifier or other similar factor may be considered an identifying factor for a natural person.

While the GDPR includes many requirements, most relevant to insurers may be the significantly enhanced rights provided to individuals, and these enhanced rights are coupled with specific provisions that make it easier for such individuals to claim damages for compensation for violations of such rights. These rights include, with exceptions: (i) a right to access personal data in a concise, transparent and easily accessible form; (ii) a right in certain circumstance to have personal information erased ; (iii) a right to receive or have transmitted to another controlling entity all personal data concerning them in a structured, commonly used and machine-readable format; (iv) a right to object to the processing of personal data; and (v) a right not to be subject to automated decision making processes, including profiling.

As a practical matter, the extremely expansive definition of "personal data" means that organizations that must comply with GDPR will need to institute compliance practices across a far wider range of data processing and utilization practices than ever before. Further, even if an organization is not established within the European Union, it can still be subject to GDPR if it processes the personal data of individuals who are in the European Union where the processing activities are related "to the offering of goods or services"[5] to such individuals in the European Union or "the monitoring of their behavior"[6] to the extent that their behavior takes place within the European Union.

In order to comply with GDPR, organizations need to be in a position to affirmatively demonstrate to supervisory authorities and data subjects that they have affirmatively complied with the relevant provisions of the regulation. GDPR particularly sets out enhanced governance obligations, including requirements to: (i) keep a detailed record of processing operations; (ii) provide a fair processing notice to individuals whom personal data is being processed about that explains the purposes and legal basis of the processing as well as other information; (iii) perform data protection impact assessments for high risk processing; (iv) designate a data protection officer to advise on compliance with GDPR and generally monitor data protection efforts; (v) maintain a comprehensive record of data breaches, including notifying individuals where necessary; (vi) impose specific contractual requirements on third parties that personal data is shared with; and (vii) implement "data protection by design and by default."[7]

The California Consumer Privacy Act and the Consequences of GDPR in the United States

While its expansive territorial scope may make compliance with GDPR a top priority for large multinational holding companies (including those based in the United States), such companies will now need to consider privacy legislation adopted in the United States as well.

On June 28, 2018, the CCPA was enacted in California, and comparisons were immediately drawn to the GDPR. For purposes of the CCPA, "personal information" is defined as "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household,"[8] a definition that has a similar broad scope to the definition utilized by GDPR.

The CCPA, like GDPR, imposes a number of restrictions on organizations beyond the physical borders of California, including on any organizations that control personal data and do business in California, albeit only subjecting those organizations to the extent that they process data of California residents. However, unlike GDPR, the

CCPA has not set out any principles regarding the lawful processing of personal data – though given how recently the CCPA was passed and its effective date of January 1, 2020, there is a significant likelihood that California regulatory authorities, including the Attorney General, may issue guidance on this point. Indeed, the CCPA requires the Attorney General to issue regulations implementing certain of its provisions (for example, instructing how businesses can "reasonably verify" consumer requests) and authorizes the adoption of additional regulations as necessary to further the CCPA's purposes.

Similarly, the CCPA grants consumers who are California residents a number of rights, some of which are broadly analogous to the rights established by GDPR, including (with certain exceptions): (i) a right for consumers to receive affirmative disclosures from organizations covered by the CCPA of such organizations' sale, collection or disclosure of such individuals' personal information, and the requirement that such organizations respond to requests for information from such individuals; (ii) a right for consumers to access specific pieces of information collected about them by an organization; (iii) a right for consumers to request the deletion of their personal information from organizations that hold such information; (iv) a right for consumers to opt-out of the sale of personal information to third parties; and (v) a right of consumers not to be subject to discrimination for exercising their rights under the CCPA. The Attorney General may sue to enforce these rights, although private citizens may only sue to redress the unlawful exfiltration or disclosure of very limited categories of personal information (name, social security number, driver's license number and certain financial, medical and health insurance information).

In addition, a number of states have updated their data breach notification laws in the months following the effective date of GDPR, including Alabama, Arizona, Louisiana, Oregon and South Dakota. This would seem to indicate the growing importance of data privacy concerns to governmental authorities throughout the United States.

Likely Effects of GDPR in 2019 and Beyond

There is a significant likelihood that GDPR, with its increased protections for consumers, could reset the standard for how businesses, including insurance industry participants, handle personal data. Further, if protections of the type established by GDPR and the CCPA are adopted more widely, it is likely that individuals will become more aware of the advantages afforded to them by businesses that are compliant with those protections and may choose (to the extent feasible) to provide their data to those businesses rather than to businesses that are not obligated to provide GDPR-style protections. Another potential consequence is that standard contracts customarily used throughout industries would need to be revisited with an eye towards compliance with an enhanced data privacy regime, including reexamination of commercial terms given the increased costs of compliance with and higher risks of non-compliance under such a regime.

Ultimately, laws such as GDPR represent a paradigm shift for data-centric industries, like insurance, which are anchored in the use of personal information. While many insurance industry participants have begun to adjust for the increased restrictions of GDPR, these regimes present more than cosmetic legal and compliance challenges, but require companies to overhaul their thinking on the way that they collect, process, store, share and discard personal data. If regimes similar to GDPR and the CCPA are adopted more widely, basic services provided by insurance companies, agents, brokers and other service providers, down to the issuance of policies and processing of claims, will have to be reevaluated in the light of the enhanced protections for personal data and increased consent rights for individuals. Although it remains to be seen whether and to what extent lawmakers and regulators in the United States and other non-EU countries will adopt GDPR-like laws and regulations, companies would do well to remain attuned to and anticipate the changing regulatory

environment that is increasingly sensitive to safeguarding the privacy of personal data. It will also be important for industry representatives to engage with their legislators and regulators in order to have a voice in shaping future legislative and regulatory initiatives.

Endnotes

[1] Larry Hamilton leads Mayer Brown's US insurance regulatory practice within the Insurance Industry group. He advises insurance companies, insurance agencies and investment companies on a broad range of regulatory matters, including those associated with formation, licensing, portfolio investments, reinsurance, e-commerce, cybersecurity and outsourcing. He is also a member of Mayer Brown's Cybersecurity & Data Privacy practice. Charles-Albert Helleputte is a transactional and cyber security and data privacy lawyer. In the transactional context, he focuses his practice on domestic aspects of cross-border transactions, acquisitions, disposals, restructurings, financing and refinancing. Charles heads the cyber security and data privacy team in Brussels. Sanjiv Tata is an associate in Mayer Brown's New York office and a member of the Corporate & Securities practice, specializing in insurance regulatory work. Sanjiv advises insurance companies, insurance intermediaries and investment companies with respect to a broad range of insurance regulatory and corporate matters, including formation and licensing of insurance companies, mergers and acquisitions of insurance companies, reinsurance transactions, and enforcement, corporate governance, cybersecurity, enterprise risk and general compliance matters. Oliver Yaros is a partner in the Intellectual Property & IT Group as well as the Technology Transactions and Cybersecurity & Data Privacy Practices of the London office of Mayer Brown. He advises clients on technology and outsourcing transactions with a particular focus on fintech and digital transformation projects, as well as clients operating within a broad range of sectors on data protection matters and cybersecurity incidents, intellectual property transactions and related issues. Kendall Burman is a Cybersecurity & Data Privacy counsel in Mayer Brown's Washington DC office. Kendall advises a broad range of clients, including financial services and technology companies, on legal, regulatory, and policy issues involving emerging technologies, security, privacy, and the flow of information across borders. Diletta is an associate in the Brussels office. Her practice focuses on privacy and cyber security. Diletta advises clients regarding a wide range of global data privacy and security issues. She assists organizations in complying with EU and national privacy laws, including developing global data transfers mechanisms, privacy statements, data breach notification policies and procedures, etc. Diletta regularly publishes articles on those matters and is a speaker on such topics. Evan Wooten is an experienced civil litigator, focusing on privacy, consumer class action defense and actions by public officials and public enforcement bodies. Evan also assists clients in crafting contracts, policies, and terms of use to minimize litigation and government investigations. Evan is a member of Mayer Brown's consumer class action and commercial law groups and co-chairs the editorial team for the Firm's privacy and security newsletter and publications.

[2] As of July 20, 2018, GDPR was also adopted by the three of the four nations in the European Free Trade Association – Iceland, Lichtenstein and Norway.

[3] Art. 4 of GDPR.

[4] Recital 26 of GDPR.

[5] Art. 3(2)(a) of GDPR.

[6] Art. 3(2)(b) of GDPR.

[7] With respect to this last point, Article 25 of GDPR introduces the dual concepts of "data protection by design and by default." "Data protection by design" requires organizations to take into account the risks that could be presented to protecting an individual's personal data during the process of designing and implementing a new process, product or service. "Data protection by default" requires organizations to put in place mechanisms to ensure that, by default, only personal data that is strictly necessary for specific purpose is processed.

[8] CAL. CIV. CODE § 1798.140.