Corporate Governance in Insurance: The EU General Data Protection Regulation and Its Implications for United States Companies



Authors from left to right:
Francoise Gilbert
Fred E. Karlinsky
Christian Brito

The protection of personal information remains one of the most significant concerns facing the insurance industry. New and evolving legal and regulatory requirements in the United States and abroad have shaped a new landscape that companies must learn to navigate. The ever-changing legal and regulatory requirements have made it more difficult than ever for companies to maintain a culture of compliance and avoid exposing themselves to regulatory and other legal risk.

Recently, the EU General Data Protection Regulation (GDPR) went into effect. With such a name, it would be easy to conclude that the law governs only the activities of businesses established in the European Union (EU) or European Economic Area (EEA), and that businesses operating or established elsewhere will not be impacted. This is not the case.

Under Article 3(2) of the GDPR, organizations that are not established within the EU or EEA are subject to GDPR when they process personal data of individuals who are in the EU or EEA if the processing activities are related to:

- The offering of goods or services to such individuals in the EU/EEA, even if payment is not required, or
- The monitoring of their behavior, to the extent that their behavior takes place within the EU/EEA. Profiling of individuals based on their use of the Internet is an example of such monitoring.

For U.S. insurers, this could be the case when an insurer is selling policies to cover assets located in the U.S. where the asset owner is established in the EU or EEA. There is no general rule; there have not yet been any case interpreting Article 3(2). Each situation must be evaluated in the full context of the actual activities of a specific business. The GDPR introduces new rules whose interpretation is uncertain at this moment. It is important for insurers to be aware of these new rules, and to evaluate the extent of their legal obligations under the GDPR, if any.

The GDPR imposes on entities that collect, use, store, share or process personal data of individuals in the EU or EEA significant obligations that go well beyond current common practices. For example, there are significant record keeping requirements as well as limitations to data retention.

The GDPR is a lengthy, complex document. Compliance efforts are expected to be commensurate with its complexity. For some businesses, evaluating their practices and conducting all activities that are required to achieve

New and evolving legal and regulatory requirements in the United States and abroad have shaped a new landscape that companies must learn to navigate.

compliance can take several months, and in the case of the largest companies, has taken several years — and will continue over time.

The GDPR drafters have identified a long list of obligations. The document is comprised of 272 provisions that are divided into 173 recitals and 99 articles. Since the document is written in 23 different languages there are also inconsistencies in the interpretation made at the time of the translation. Increasing the confusion and the complexity, several member states have adopted laws or amendments that relate to the GDPR, as permitted by numerous provisions of the GDPR, and those provisions may create new obligations.

The basic Regulation is also supplemented by Guidelines and opinions issued by the EU institutions, or the Member States themselves — about 500 pages at this time. So far, the EU's Article 29 Working Party has published at least 13 guidelines.

This article first appeared in the Summer 2018 issue of *The Demotech Difference*, a publication of Demotech, Inc., www.demotech.com

The Supervisory Authorities of Member States have also published guidelines on other relevant GDPR topics.

Nevertheless, it is important to keep in mind that the GDPR is very recent and there is currently little official guidance, and numerous questions. No cases have yet been adjudicated under the GDPR. Until there is more clarity in the interpretation of the GDPR, a cautious approach is recommended. U.S. businesses should educate themselves on the key components of the GDPR and properly evaluate the extent to which the GDPR might apply to their activities.

The GDPR protects the personal data of individuals or natural persons. The term "personal data" is broadly defined as "any information relating to an identified or identifiable natural person (data subject)."

A person is deemed "identifiable" if the person can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number (e.g., a policy number), location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that person. Examples of personal data include name, contact information, addresses, person characteristics, and can include IP address, location data, or even device information, as well.

Insurers should also be aware that some categories of personal data receive additional protection, and their use is much more restricted than non-sensitive data. Some of these data might be routinely collected as part of some insurance applications, for example in connection with life insurance or health insurance. This data includes, among others: racial or ethnic origin, data concerning healthcare, data concerning a person's sex life or sexual orientation, and in some cases, genetic and biometric data.

arka38/shutterstock.com

GDPR Art. 5 sets forth six principles governing the processing of personal data:

- Lawfulness, Fairness, Transparency;
- Purpose Limitation;
- Data Minimization;
- Accuracy;
- Storage Limitation; and
- Integrity and Confidentiality.

These six principles are the cornerstone of the GDPR. They must be addressed in any activity conducted, in the collection of personal data, in the design of a product, or in the preparation of a marketing campaign. And much more. A seventh principle defines a separate requirement for accountability, which makes entities responsible for compliance with the six principles, and requires that they be able to demonstrate compliance with these principles. In addition, entities that collect or process personal information must maintain a record of processing activities under their responsibility, and the record must contain specified information.

Nevertheless, it is important to keep in mind that the GDPR is very recent and there is currently little official guidance, and numerous questions.

It will be critical at all times for organizations to be able to prove, through written records and documented technical, physical and administrative measures that its management and staff understand the GDPR, and that its governance, its lead generation and marketing practices, and its products and services meet the six principles when processing personal data of individuals located in the EU/EEA.

In addition to the numerous disclosure, record keeping, and policy requirements, the GDPR grants data subject numerous rights. The exercise of these rights by any individual requires entities to respond within thirty days, which requires the affected entity to be prepared to act promptly and take the requested action, which may include for example, the correction of data and the provision of a complete file.

Violation of the GDPR exposes an organization to administrative fines of up to EUR 20,000,000, or in the case of an undertaking, up to four percent of the total worldwide annual turnover of the preceding financial year, whichever is higher. In addition, individuals could initiate lawsuits and seek compensation if they have suffered damages because of an infringement of the GDPR.

U.S. businesses are well-advised to audit their processes for the collection and processing of personal data to determine their exposure and compliance needs under the GDPR. To do so, businesses must understand how the entity interacts with personal data of individuals located in the EU, then identify the changes to be made to comply with the GDPR when collecting and processing such personal data. Some key steps in this process include:

- Data Inventory: Identify the universe of the personal data at stake.
- Data Mapping: Identify what happens to each category of personal data, how it is collected, with whom it is shared, how long it is stored.
- Current Internal Framework: Identify the rules that apply to the current uses of the data (e.g. the processes, procedures, contracts that govern these uses).
- Gap Analysis: Identify discrepancies with the requirements under the GDPR.
- Risk Analysis: Identify those action items that are the most important/urgent to prioritize the actions needed.
- Remediation Plan: Identify the steps necessary to remediate the identified gaps.
- Implementation: Develop new structures, policies, and documents to address the GDPR requirements.

Most companies looking to comply with the GDPR with respect to their processing of personal data of individuals located in the EEA are likely to have to address at least some of the following in connections with their processing of EEA personal data:

- Understand and address the company's obligations as a controller or processor
- Understand and address the restrictions to marketing, targeting, profiling
- Update the contracts with data processors, subprocessors
- Document the security program; update the security breach response plan
- Address the crossborder data transfer restrictions
- Identify the legal grounds for processing the personal data
- Update the privacy notice
- Develop processes to address obligations regarding data subjects' rights
- Update training for personnel
- Appoint a Data Protection Officer, identify an EU Representative, and in some cases, the lead supervisory authority.

The GDPR is having a tsunami effect well beyond the boundaries of the EU/EEA. Due to the interaction between U.S. and European businesses and customers, and the continued growth of multi-national operations, the GDPR has become a significant part of the U.S. Privacy and Security legal landscape. It is important for U.S. businesses to pay attention to compliance.

In a few months it has created havoc in the way U.S. businesses interact with personal data, and it has become the de facto primary privacy and data protection law or standard both in the United States and around the world for non-European firms that interact with individuals in the EU/EEA or exchange data with firms that do so.

Organizations will have to adhere to the GDPR if they want to be able to continue doing business with individuals located in the EU/EEA. Individuals and businesses located in the EU/EEA may soon inquire whether your company can demonstrate that it meets the GDPR mandates when collecting, using, sharing or processing personal data of individuals located in the EU/EEA. If you have ignored the GDPR or have been casual in implementing it, and are unable to respond adequately to due diligence questions that will be sent to you, potential customers or investors may take their business to other companies who have made the effort to comply.

Francoise Gilbert, a partner at Greenberg Traurig, is the author of the two volume treatise "Global Privacy and Security Law" (Wolters Kluwer Publishing), covering 68 countries. Her practice has focused on information privacy and security for more than 25 years. Francoise deals regularly with compliance challenges raised by the EU General Data Protection Regulation (GDPR), connected objects, smart cities, big data, mobile applications, wearable devices, social media, data analytics, artificial intelligence, internet of things, autonomous vehicles and other cutting-edge developments. As a practicing attorney, she advises a wide range of entities on the entire spectrum of domestic and international privacy and cyber security issues legal issues.

Internationally recognized as a thought leader and expert in data privacy and cyber security, Francoise Gilbert has been continuously praised for her experience and in-depth knowledge of this area. She was named "2014 San Francisco Lawyer of the Year" by Best Lawyers for her work in information privacy and security, and a "Cybersecurity and Privacy Trailblazer" by the National Law Journal in 2015. She is listed in Chambers USA and Chambers Global (since 2008), Best Lawyers in America (since 2007), and Who's Who in Ecommerce and Internet Law (since 1998). Françoise holds law degrees from Paris University (France) and Loyola University (Chicago, Illinois) and a graduate degree in Mathematics from Paris University (France). She is accredited as a Certified Information Privacy Manager (CIPM) and a Certified Information Privacy Professional (CIPP/US, CIPP/E).

Fred E. Karlinsky is Co-Chair of Greenberg Traurig's Insurance Regulatory and Transactions Practice Group. Fred has over twenty years of experience representing the interests of insurers,

reinsurers, health plans, managing general agencies, brokers, third-party administrators, claims companies and other insurance entities on their regulatory, transactional, corporate and governmental affairs matters. He is experienced in the formation, licensure and capitalization of insurers, business expansion activities, regulatory examinations, reinsurance and alternate risk transfer mechanisms and many other operational and regulatory issues. Recognized as one of the top insurance lawyers by Chambers and Partners, Fred's extensive knowledge of insurance compliance matters and insurance related legislative and regulatory initiatives is applicable nationally and internationally. Fred can be reached at 954.768.8278 or karlinskyf@gtlaw.com.

Christian Brito is a practice group attorney in Greenberg Traurig's Insurance Regulatory and Transactions Practice Group in Fort Lauderdale. He focuses his practice on national insurance regulatory and compliance matters. Christian represents a wide variety of insurance entities, including insurance companies, reinsurers, managing general agencies, brokers, third-party administrators, claims companies, and other insurance-related entities in connection with regulatory, transactional, corporate, and governmental affairs matters. Christian advises clients on operational, regulatory, and compliance issues, including start-up initiatives, product filings, licensure and corporate governance assessments, business expansion initiatives, and financial and market conduct examinations.

Christian received a Juris Doctor from The Pennsylvania State University Dickinson School of Law and a Bachelor of Arts from Florida International University. He is admitted to practice in Florida and Pennsylvania. He can be reached at britoc@gtlaw.com.

Greenberg Traurig, LLP (GTLaw) has more than 2,000 attorneys in 38 offices in the United States, Latin America, Europe, Asia and the Middle East and is celebrating its 50th anniversary. GTLaw has been recognized for its philanthropic giving, was named the largest firm in the U.S. by Law360 in 2017, and among the Top 20 on the 2016 Am Law Global 100. Web: www.gtlaw.com Twitter: @GT_Law.