GDPR Made Them Do It: The Response to Updated Privacy Terms and Other Implications of GDPR

Michelle Carter, The Hays Companies
Andrew Deutsch, nVent
Latosha M. Ellis, Hunton Andrews Kurth LLP
Laura Foggan, Crowell & Moring LLP
Colleen M. Yushchak, Ankura
GDPR Made Them Do It: The Response to Updated Privacy Terms and Other Implications of GDPR

TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTRODUCTION</td>
<td>1</td>
</tr>
<tr>
<td>WHAT IS GDPR</td>
<td>1</td>
</tr>
<tr>
<td>The Scope of GDPR</td>
<td>1</td>
</tr>
<tr>
<td>Compliance with GDPR</td>
<td>2</td>
</tr>
<tr>
<td>THE U.S. REGULATORY FRAMEWORK AFTER GDPR</td>
<td>3</td>
</tr>
<tr>
<td>OPERATIONAL EFFECTS OF GDPR</td>
<td>5</td>
</tr>
<tr>
<td>Discovery and Electronically Stored Information</td>
<td>5</td>
</tr>
<tr>
<td>Marketing and Business Development</td>
<td>5</td>
</tr>
<tr>
<td>UNDERWRITING CONSIDERATIONS</td>
<td>6</td>
</tr>
<tr>
<td>COVERAGE IMPLICATIONS</td>
<td>6</td>
</tr>
<tr>
<td>CONCLUSION</td>
<td>8</td>
</tr>
</tbody>
</table>
INTRODUCTION

According to the European Commission, the General Data Privacy Regulation (EU) 2016/679 ("GDPR") is “the most important change in data privacy regulation in 20 years.” The Commission believes that the new law, which replaces the European Union’s (“EU”) 1995 Data Protection Directive 95/46/EC, will reshape the way organizations across the region approach data privacy. GDPR is already transforming data privacy around the world.

WHAT IS GDPR

GDPR is a European regulation relating to data protection and privacy that seeks to create a harmonized data-protection law framework across the EU. The regulation aims to give citizens control of their personal data, while imposing strict rules on those hosting and processing personal data, anywhere in the world. The regulation also introduces rules relating to the free movement of personal data within and outside the EU.

Under GDPR, individuals have a set of rights relative to their personal data, including the right to information, access, rectification, erasure, restriction, objection and data portability (Art. 12-21, GDPR). According to the European Commission, “personal data is any information relating to an individual, whether it relates to his or her private, professional or public life. It can be anything from a name, a home address, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer’s IP address.” GDPR governs the search, preservation, collection, review, and processing of EU personal data in the EU and the forwarding (onward transfer) of such data out of the EU. Most relevant, GDPR applies to “processing”; the touching of personal data. The regulation requires that there must be a legal transfer mechanism in place for sending personal data that originates in the EU to outside of the EU.

The Scope of GDPR

GDPR has a broad territorial scope. It applies to:

1. Personal data processed by a controller (an entity that determines the purposes and means of processing data) or a processor (an entity that processes data on behalf of a controller) that is established in the EU.

2. Processing of personal data of data subjects in the EU if the controller or processor is not established in the EU and the processing activities are related to:

   a. Offering goods or services, regardless of whether payment is required, to data subjects in the EU; or

   b. Monitoring the data subjects’ behavior that takes place in the EU.
3. Processing of personal data by a controller not established in the EU but in a place where an EU Member State’s law applies.¹

Thus, GDPR applies to companies established in the European Economic Area (“EEA”) processing personal data, as well as non-EEA companies that process personal data of individuals located in the EEA, regardless of residency or nationality. Because the territorial scope of GDPR is so broad, it applies to citizens of other countries, such as the U.S., India, China, etc., if they are residing in the EU, or if the controller or processor is established in the EU.

The regulation provides for a data controller with responsibility and liability for ensuring and demonstrating that appropriate data-protection safeguards have been instituted, including with respect to an onward transfer of EU personal data to a third party. GDPR imposes obligations on processors, for example, to maintain a record of the processing activities within its responsibility.

Most relevant to insurance coverage, the regulation also requires insurers, reinsurers, and other companies to report data breaches within 72 hours.² Fortunately, not every breach has to be reported. Only breaches that are likely to result in a risk to individuals’ rights and freedoms must be reported to the regulator, and only those that pose a high risk to the individual require notification to the individuals themselves. High risk is not defined in the GDPR; however, the guidelines state that you should consider a combination of the severity of the potential harm and/or damage to the individuals and their likelihood. Examples of harmful or damaging impacts to an individual include financial loss, discrimination, identity theft or fraud, and damage to reputation.

**Compliance with GDPR**

A single set of rules applies to all EU Member States, but many provisions of GDPR allow EU Member States to further regulate at a domestic level (e.g., the age of children ranging from 13-16 years impacted by the regulation is determined by member states themselves). Each member state established an independent supervisory authority to hear and investigate complaints, sanction administrative offences, etc. These supervisory authorities are obliged to mutually assist each other.

Companies risk fines of up to 20 million € (£17 million or $22.3 million) or 4 percent of global turnover, whichever is higher, if they breach the EU’s formidable data regime. As previously mentioned, businesses with customers in the EU have a mere 72 hours to alert EU authorities of breaches. However, the clock does not start ticking until the controller becomes aware of a breach, such as when the controller has reasonable belief that personal data may have been compromised. Processors similarly have an obligation to notify the controller “without undue delay” after becoming aware of a personal data breach.³

---

¹ GDPR Art. 3.
² See id. Art. 33(1).
³ Id. Art. 33(2).
Businesses subject to GDPR had until May 25, 2018 to meet GDPR compliance requirements. During the first four months of entry in GDPR, or four months after the compliance deadline, the French Data Protection Authority (the “CNIL”) published a statistical review of personal data breaches.\(^4\) Between May 25 and October 1, 2018, the CNIL received 742 notifications of personal data breaches that affected 33,727,384 individuals located in France or elsewhere. Of those, 695 notifications were related to confidentiality breaches. Most breaches were, therefore, the result of hacking and intentional theft attributable to a malicious third party, or employees’ unintentional mistakes. In all other cases, the causes of the breach were unknown or undetermined by the notifying data controller, or the breach was the result of internal malicious actions. More than half of the notified breaches (421 notifications) were due to hacking via malicious software or phishing. Sixty two notified breaches were related to data sent to the wrong recipients, 47 notified breaches were due to lost or stolen devices, and 41 notified breaches were due to the unintentional publication of information. Organizations often had the means to retrieve data within the 72-hour time limit after an integrity or availability breach. (e.g., no GDPR fine).

By comparison, the United Kingdom saw an exponential increase in the number of self-reported breaches across Q2 of 2018, starting with around 400 reports in March and April, to 650 reports in May, and spiking to 1,792 reports across the month of June\(^5\), which was the first month of entry, one month after the GDPR compliance deadline. Health and education, solicitors, and local government led the way in reported breaches, as they did under the old Data Protection Act. The first UK GDPR enforcement action was against Canadian firm Aggregate IG (AIQ).\(^6\)

**THE U.S. REGULATORY FRAMEWORK AFTER GDPR**

As of March 2018, all 50 U.S. states, as well as the District of Columbia, Guam, Puerto Rico, and the U.S. Virgin Islands, had breach notification laws that require businesses to notify consumers if their personal information is compromised. These new and amended state data breach laws expand the definition of personal information and specifically mandate that certain information security requirements are implemented.\(^7\) South Dakota became the 49th state to enact a breach reporting notification law in March 2018. In April 2018, Alabama – the lone holdout – joined every other state in the country when it passed a relatively stringent breach reporting law that gives companies 45 days to disclose such incidents and requires them to implement reasonable data security measures.

Notably, GDPR seemingly influenced officials in some U.S. states to strengthen their own internet privacy regulations or to introduce new measures as well. As an example, days before


GDPR took effect, Vermont tightened its breach reporting law to begin regulating data brokers, which are essentially companies that buy and sell consumers’ personal information, including marital status, browsing history and education credentials, to other organizations.

Other states have been influenced by GDPR as well. In 2017, New York Attorney General Eric Schneiderman proposed an amendment to state law that would increase data security and breach notification requirements. The Stop Hacks and Improve Electronic Data Security (SHIELD) Act would have expanded the definition of “private information” to now encompass user name or email address along with a password, biometric data, and also unsecured protected health information subject to the federal Health Insurance Portability and Accountability Act (“HIPAA”). The SHIELD Act also proposed new cybersecurity and data breach notification requirements. The bill passed through the New York Assembly but stalled in the Senate.

A month after the GDPR protection regime was set, California Gov. Jerry Brown signed a landmark privacy bill that gives consumers the ability to control how online companies use and share their personal information and to request its deletion. The California Consumer Privacy Act, which is set to take effect in January 2020, will require online businesses, such as Google and Facebook, to tell inquiring consumers what kind of personal data they hold about them, the purposes for which data are used, and with whom they are sharing the information.

In Colorado, Governor John Hickenlooper signed into law House Bill 1128, effective September 1, 2018, which mandates that companies and government entities contact individuals within 30 days of a determination that a security breach has taken place. The law requires businesses to notify the Colorado Attorney General if the breach affects more than 500 Colorado residents, and must tell credit reporting agencies about episodes affecting more than 1,000 residents. The law expands the definition of “personal data” to include a Colorado resident’s first name or first initial and last name tied to their Social Security number; student, military or passport identification number; driver’s license number or identification card number; medical information; health insurance identification number; or biometric data. It also includes any information that could help a hacker unlock a Colorado resident’s online or banking account, including combinations of usernames and email addresses with passwords or security codes. Colorado’s new law also requires that companies maintain written procedures for disposing of data that is no longer needed and take “reasonable” steps to protect the personal data that they have, including data that is shared with third parties. The Attorney General’s office is tasked with enforcing the law.

States have also made efforts to bolster privacy and security requirements for insurers. In 2017, New York’s Department of Financial Services promulgated 23 NYCRR Part 500, also known as the Cybersecurity Regulation. It requires “covered entities,” such as insurers and other financial institutions, to implement, monitor, and audit a written information security program that protects, and responds to potential breaches of, data. The regulation has several deadlines through the final transition period that concludes on March 1, 2019.

In 2018, South Carolina became the first state to adopt the Insurance Data Security Model Law proposed by the National Association of Insurance Commissioners. The South Carolina Data Security Model Act, S.C. Code § 38-99-10, et seq., became effective on January 1, 2019. It requires “licensees”—any person licensed under the state’s insurance laws—to implement a
written information security program and create an incident response plan for, and give notice of, any data breaches. Ohio followed South Carolina and adopted its own Insurance Data Security Act in December 2018.

OPERATIONAL EFFECTS OF GDPR

Although many companies have already adopted privacy processes and procedures consistent with GDPR, coverage attorneys should think critically about the operational effects GDPR has on litigation and business development.

**Discovery and Electronically Stored Information**

Litigators seeking discovery from Europe have to be cognizant of GDPR. There is great potential for the privacy restrictions of GDPR and the comparatively expansive scope of discovery in the United States to conflict with each other. U.S. courts will have little patience for GDPR compliance requirements if the result is a failure to preserve electronically stored information, a substantial delay in producing requested documents and data, or an outright refusal to produce the materials requested. As a result, U.S. counsel, for both the plaintiff and the defendant in civil litigation and in responding to government requests, must carefully evaluate GDPR requirements and coordinate their efforts with clients as well as GDPR experts before the onward transfer of EU personal data to the United States.

EU personal data cannot be transferred outside of the EU unless a country has “adequate” data-protection laws. GDPR Art. 45. A company’s obligation to produce extensive electronically stored information (“ESI”) in civil and criminal litigation and government investigations commenced in the United States transcends geographical borders. The EU and EEA severely restrict the transfer of broadly-defined personal data to the United States. However, as the United States Supreme Court previously ruled in *Société Nationale Industrielle Aérospatiale v. U.S. District Court for the Southern District of Iowa*, 482 U.S. 522, 543-44 (1987), foreign data-protection laws cannot be used to limit the scope of U.S. discovery. Instead, courts are required to weigh the needs of the requesting party and the impact of U.S. discovery in foreign countries.

To avoid or minimize conflicts between U.S. discovery obligations and GDPR, attorneys should consider a three-stage approach: (1) a stipulation or protective order to extend special protections to EU personal data, (2) phased discovery to permit time to implement further data-protection processes, including completing a data protection impact assessment, and (3) a legitimization plan to maximize compliance with GDPR and U.S. discovery obligations.

**Marketing and Business Development**

Many insurers are active direct marketers, and GDPR also introduced new restrictions on direct marketing. The most significant of these is that “opt-out” mechanisms, such as pre-ticked boxes, are no longer a valid method of obtaining consent from individuals. In a post-GDPR world, microsites, blogs, and social media will become more valuable than ever. Companies that deploy them strategically will increase their relative visibility and accelerate the rebuilding of their opt-in distribution lists. They will also be less vulnerable to other growing pitfalls with email
marketing, such as blacklisting and aggressive spam filtering. The reality is that making a meaningful one-to-one connection with a prospect digitally is simply more challenging post-GDPR.

UNDERWRITING CONSIDERATIONS

As GDPR becomes the new reality in risk management and governance, the ability to transfer the imposed financial risks will likely change how insurance companies evaluate an applicant’s cyber risk profile. Underwriting may become even more onerous, as many expect a drop in new data collection to the minimum information needed and a general shift toward aggregated, anonymous data versus individual information. According to A.M. Best, these changes, while complying with GDPR, could harm underwriting.\(^8\) Specifically, insurers and reinsurers “anticipate that GDPR Art. 33, and particularly the 72-hour incident response requirement, are likely to put companies’ internal processes and functions under considerable pressure, making pre-event planning and training even more important.”\(^9\)

In response to GDPR, insurers are developing new and improved cyber policies that offer computer network monitoring or preemptive services to help businesses prevent data breaches and conform with GDPR. Experienced coverage attorneys should assist clients with auditing existing policies, renewals, and proposals. Cyber policies are anything but uniform, and continue to evolve. GDPR is likely to only accelerate the variety of policy forms, although there appears to be an industry push for more standardization.

COVERAGE IMPLICATIONS

Most aspects of GDPR should be covered by a solid cyber insurance policy. At any rate, there are a number of issues good insurance coverage attorneys should keep in mind when reviewing clients’ policies and providing gap analysis or legal counsel to businesses subject to GDPR.

✓ Insurability of Penalties Related to GDPR.

While insurance coverage for fines and penalties has traditionally been viewed as being against public policy due to concerns with giving policyholders a way to lessen the blow for sanctions that a regulator saw fit to bestow upon them, that attitude has begun to shift in the past few decades to allow for coverage of presumably less reprehensible civil penalties tied to compliance errors (although criminal penalties are still considered uninsurable). In a recent report, an insurance broker is quoted as saying that policyholders “should assume nothing” about whether their insurance policy will cover penalties under GDPR.\(^10\) Taking into account local law and public policy principles to determine whether indemnity agreements between insurers and policyholders would hold up in the legal systems of each country, experts have concluded that there are currently only a few jurisdictions in Europe where civil fines can be covered by

---


\(^9\) Id.

insurance and, even then, there must be no deliberate wrongdoing or gross negligence on the part of the insured.

At any rate, a solid cyber insurance policy is likely to cover potential GDPR risks and liabilities under its general regulatory coverage provisions even if the EU law isn’t explicitly mentioned, although some insurers and policyholders are moving toward including broader definitions of covered regulatory matters that specifically encompass GDPR as part of a “belt and suspenders approach.” Despite the uncertainty surrounding GDPR fines and penalties, the response of insurers in the U.S. and Canada regarding cyber policies has generally been positive. Several leading insurers for U.S. and Canadian companies have been adding coverage intended to account for GDPR for little or no additional premiums.

✓ Coverage Limits and Sublimits.

Because the fines and penalties under GDPR can be catastrophic, insureds and their brokers should be advised to review their limits.

✓ Policy Definitions.

Make sure, in addition to including “international” or “foreign” entities in the list of potential privacy regulatory bodies listed in the policy form, that European Data Protection Authorities are specifically added by endorsement.

✓ Insuring Language.

Look carefully at insuring language. To the extent the definition of “privacy law” in a cyber policy form is limited to laws regulating privacy breaches, note that GDPR will impose strict rules around a broader universe of privacy concerns, including the storage of data, and how it is accessed and managed. Insurers must be willing to expand coverage to include claims related to these potential exposures. Such an extension has been known as “wrongful collection” coverage, but make sure the coverage includes any claims of improper storage and/or the handling of data.

✓ Pay Attention to Coverage Triggers.

Some cyber policies have narrower triggers for regulatory fines and penalties compared to general privacy liability coverages, and are often limited to fines or penalties related only to privacy breaches. Make sure the cyber policy covers all aspects of the handling of data.

✓ Jurisdiction.

Think about most-favored venue and jurisdiction wording for fines and penalties. Push for provisions/endorsements that state that the insurer will take into consideration all reasonable venues to determine the insurability of a fine or penalty, such as where the company is located, headquartered or incorporated, or where the claim or event occurred.
✓ Directors & Officers Exposure.

It is widely anticipated that shareholders will seek to hold corporate leadership accountable for damages resulting from any alleged failure to provide adequate oversight in connection with GDPR compliance. Companies should evaluate their D&O coverage and liability limits in anticipation of this exposure.

CONCLUSION

Protecting data privacy under GDPR is paramount. As organizations around the world transition into this new era in data privacy, we expect the insurance industry to be no different as insurers, and subsequently insurance coverage counsel, adapt to provide solutions.