Lowenstein Sandler

Business Insurance

April 2, 2018

GDPR fines: How can you be sure you're insured?

By Michael A. Barrese

On May 25, 2018, members of the European Economic Area will begin to enforce the General Data Protection Regulation, which governs the collection and processing of personal information regarding EEA residents.

Under the GDPR, EEA members can enforce the regulation against any person or entity anywhere in the world. Even a company with no physical presence in Europe is subject to the regulation if the company collects or accesses data concerning EEA residents. As a result, companies in the United States are scrambling to determine whether their insurance programs will provide coverage for GDPR fines.

While the costs of compliance with the GDPR are high, the cost of violating it is even higher. The GDPR breaks fines into two categories: lower-tier offenses, which can result in fines of up to €10 million ($12.24 million), or 2% percent of "total worldwide annual turnover"; and upper-tier offenses, which can result in fines of up to €20 million, or 4% of "total worldwide annual turnover." Given the nature of the GDPR, most companies will look to stand-alone cyber risk policies for coverage. Because the GDPR is a foreign regulation, it is imperative that a cyber risk policy issued to an entity in the United States have broad enough terms to cover the costs of a GDPR violation.

Unlike commercial general liability policies, there is no "standard" cyber risk policy. While the basic coverage options of cyber risk policies are similar — i.e., coverage for first-party losses arising out of a data breach, coverage for third-party costs associated with claims against the insured arising out of the failure to protect personally identifiable information, and coverage for regulatory investigations arising out of the failure to protect PII — each insurer has its own unique terms to define the scope of these coverages.

The first step in evaluating whether coverage is available for GDPR fines is to ensure that the cyber risk policy provides coverage for regulatory investigations and actions. While it is common for cyber risk policies to afford this coverage, there are several policy forms that limit coverage to other risks, such as responding to a data breach, media liability or technology errors and omissions. As a result, the insured must carefully evaluate policy options to ensure that regulatory investigations and actions are part of the coverage purchased.

After ensuring that regulatory investigations and actions are included in the scope of coverage, coverage for regulatory fines and penalties can be evaluated. Typically, cyber risk policies will either exclude coverage for fines and penalties or limit coverage to where fines and penalties are insurable under the applicable law and apply a sublimit to cap payouts. Because the GDPR is not in effect, no court has had the opportunity to evaluate whether GDPR fines are insurable. While many speculate that GDPR fines are not intended to be punitive, and thus will be insurable, this speculation will be of little consolation when insurers inevitably challenge coverage for GDPR fines.

When dealing with insurability of fines or penalties, the policy's choice of law provision can play a significant role because some jurisdictions permit coverage for fines and penalties while others do not. As a result, eliminating the choice of law provision is generally recommended. While some insurers may,

push back at this change, eliminating the choice of law provision allows policyholders to evaluate which potentially applicable law is most favorable to coverage and pursue its claim for coverage under such law.

To the extent that eliminating the choice of law provision is not possible, selecting the appropriate jurisdiction is imperative. Policyholders should evaluate the law of each jurisdiction to which it has ties and push for the jurisdiction with the most favorable law to be selected. For example, consider a policyholder incorporated in Delaware and headquartered in New York. This policyholder can broaden coverage by changing the jurisdiction selected in the choice of law provision from New York to Delaware because, in general, Delaware law recognizes punitive damages as insurable. As a result, regardless of whether GDPR fines are viewed as punitive, Delaware courts are more likely to find that they are insurable.

Another important consideration is whether definitions in the policy conflict with the choice of law provision. For example, the definition of fines/penalties often provides that insurability will be determined "by the law of the jurisdiction that most favors coverage." Where the policy contains a choice of law provision that designates a jurisdiction that does not favor coverage for fines and penalties and the policyholder has a connection to a jurisdiction that does, these terms conflict and an ambiguity is created. While ambiguities are interpreted in favor of the insured, the fact that the ambiguity exists portends a costly coverage dispute that could be avoided by modifying the choice of law provision to be consistent with the definition of fines/penalties.

Finally, some companies may benefit from going abroad for policies, as there are some countries, such as Bermuda, that broadly permit fines and penalties to be insured. The downside to a foreign market such as Bermuda is that the premiums for policies can be higher than those of domestic insurers and the capacity to insure is lower.

Given the uncertainty over the interpretation of GDPR fines and the manuscript nature of cyber risk policies, coverage counsel can provide invaluable advice regarding potential gaps in coverage, recommend modifications to policy language that increase coverage for GDPR fines, and avoid common pitfalls that lead to costly claim denials and coverage litigation.

Michael A. Barrese is an associate in Lowenstein Sandler's Insurance Recovery practice.

This article was originally published in *Business Insurance*®. The original article can be found at this link (subscription required).

Contact

MICHAEL A. BARRESE
Associate
T: 973.597.6182
mbarrese@lowenstein.com