HUNTON ANDREWS KURTH

Lawyer Insights

May 16, 2018

With the EU's Global Data Protection Regulation Quickly Approaching, Policyholders Should Act Now to Maximize Insurance Coverage for Its Potentially Staggering Liabilities

by Lorelie S. Masters and Paul T. Moura

Published in SA Financial Regulation Journal


May 25, 2018 should be a day circled on many company calendars. On that day, the European Union's long-awaited Global Data Protection Regulation ("GDPR") will go into effect. It is crucial for U.S. companies to prepare for the GDPR, as they, too, will be required to comply with a new set of data privacy rules if they are handling data from EU-based customers, suppliers, or affiliates. As long as you collect personal or behavioral data from someone in the EU, you must comply with the GDPR.

Those not in compliance with the GDPR stand to face potentially crippling fines for the unlawful collection of data. Specifically, companies that violate its rules may be assessed fines of up to 4% of their previous year's annual global turnover or 20 million Euros, whichever is ***greater***. It is therefore incumbent upon policyholders to create a careful risk management strategy to prepare for and minimize these potential risks well before any adverse enforcement action occurs.

Insurance Options for GDPR Fines

Almost overnight, the GDPR will make the impact of cyber liabilities much more serious. Of utmost importance, then, is what companies can do now to make sure that their insurance coverages respond to the new liabilities imposed by the GDPR. Savvy companies and risk managers are thinking ahead, shopping for insurance coverages to cover GDPR exposures and fines; and the number of these types of policies on the market is growing. However, the tricky—and too often unnoticed—issue is that these policies typically cover fines only where "insurable by law." That phrase should resonate, and should serve as a reminder and warning that fines and penalties in many jurisdictions are *not* "insurable by law." Companies considering these coverages should consider closely whether they are paying for actual protection, or just words on paper.

In many jurisdictions, damages that are "punitive" or "penal" in nature are not insurable. Typically, the rationale is that allowing insurance coverage for such damages would be against public policy. *See, e.g., U.S. Concrete Pipe Co. v. Bould*, 437 So. 2d 1061, 1064 (Fla. 1983) ("Florida public policy prohibits liability insurance coverage for punitive damages assessed against a person because of his own wrongful conduct.").

Whether regulatory fines are "punitive" in nature is a frequently-litigated issue, and court decisions are in disarray. Some courts have held that regulatory fines, similar to the ones that GDPR will impose, are

meant to be punitive and are thus uninsurable. *City of Fort Pierre v. United Fire & Cas. Co.*, 463 N.W.2d 845, 848 (S.D. 1990) (civil penalties prayed for by the federal government were punitive in nature and not insurable).

However, there is a gray area, as courts in some jurisdictions will allow coverage for regulatory fines that are arguably "compensatory" in nature, as opposed to purely penal. For example, in *Terra Nova Insurance Co. v. Fray-Witzer*, 869 N.E.2d 565, 420 (Mass. 2007), the Supreme Judicial Court of Massachusetts, applying New Jersey law, held that because fines under the Telephone Consumer Protection Act are intended to go to the consumer who suffered the injury, the fines were "remedial" in nature and thus potentially insurable. Likewise, in *Columbia Cas. Co. v. Hiar Holding, L.L.C.*, 411 S.W.3d 258, 268 (Mo. 2013), the Supreme Court of Missouri held that statutory fines can be "remedial" and thus insurable where they in part act as a proxy for damages that are difficult to quantify. In *Standard Mut. Ins. Co. v. Lay*, 989 N.E.2d 591, 600 (Ill. 2013), the Illinois Supreme Court explained that statutory penalties can be insurable where they are "intended as a supplemental aid to enforcement rather than as a punitive measure." And finally, in *Navigators Ins. Co. v. Sterling Infosystems, Inc.*, 145 A.D.3d 630, 631, 42 N.Y.S.3d 813, 814 (1st Dep't 2016), the First Appellate Department of New York held that statutory damages under the Fair Credit Reporting Act were compensatory and thus insurable, given that the statute also provided consumers an option to seek actual damages.

But are GDPR fines arguably "compensatory" and not "penal?" The answer to that question may depend on exactly how the law will be enforced by data protection authorities and the manner in which civil penalties are assessed. Courts interpreting cyber insurance policies will likely reach varying conclusions, but there are steps that policyholders can take now to increase their chance of coming out on the winning end.

What Can Policyholders Do Now to Maximize Coverage?

Given the uncertainty surrounding the insurability of GDPR violations, policyholders who handle data from EU-based sources should take extra care in maximizing their coverage opportunities as soon as possible. First, policyholders should work with qualified coverage counsel to closely review their existing cyber coverages and obtain enhancements to their policy language and limits in order to encompass GDPR liabilities.

Second, policyholders should evaluate whether specific jurisdictions provide stronger coverage options for fines and penalties. Certain states in the U.S. provide greater insurability of these types of losses, and international options—such as Bermuda Form coverages—are known to provide more expansive coverage for losses that are considered "punitive."

Finally, policyholders should also take steps to prepare for the more distant financial consequences of GDPR fines and penalties. Importantly, policyholders should review their Directors' and Officers' insurance policies to remove any cyber-related exclusions and implement language that would maximize coverage for any shareholder suits that may arise following an adverse GDPR enforcement action. Shareholder suits are becoming an increasingly routine event following a major data breach. Given the significant fines imposed by the GDPR (up to 4% of a company's global turnover), there is little doubt that shareholder suits will become even more prevalent in the GDPR's regulatory landscape. Policyholders should ensure that their D&O policies are equipped to respond.

With the EU's Global Data Protection Regulation Quickly Approaching, Policyholders Should Act Now to Maximize Insurance Coverage for Its Potentially Staggering Liabilities
By Lorelie S. Masters and Paul T. Moura
SA Financial Regulation Journal | May 16, 2018

May 25, 2018 is quickly approaching, and a creative and multi-jurisdictional approach to a GDPR-ready cyber insurance program can potentially save millions of company dollars down the line.

Lorelie S. Masters *is a partner at Hunton Andrews Kurth in the Washington, DC office. A nationally recognized insurance coverage litigator, she handles all aspects of complex, commercial litigation and arbitration. She may be reached at (202) 955-1851 or lmasters@HuntonAK.com.* ***Paul T. Moura*** *is an associate in the firm's New York office. He represents consumer product manufacturers, technology companies and multinational brands in high-stakes litigation and commercial disputes. He may be reached at (212) 309-1106 or pmoura@HuntonAK.com.*