Corporate Counsel Business Journal
September ▪ October 2018
ccbjournal.com

CCBJ

New GDPR Law Triggers New Risks – And a Panoply of Coverage Issues

DANIEL J. HEALY
ANDERSON KILL

▶ Daniel J. Healy of Anderson Kill's cyber insurance recovery practice sorts out the complex coverage issues raised by the EU's General Data Protection Regulation.

GDPR, the European Union's General Data Protection Regulation, has arrived with much ado. So far, however, there has been little discussion about which insurance coverage will apply and what losses insurance will cover.

The new regulation protects European Union data subjects' right to privacy and protection of their personal data, imposing stiff penalties for violations. While considerations of GDPR liability often focus on the potentially large penalties, the liability takes other forms as well. The types of liabilities faced, and the reasons for the liabilities, raise important insurance considerations.

As recently as April 2018, it was reported that only 5 percent of likely affected companies were prepared to meet the stringent GDPR standards. "The British Standards Institution (BSI) surveyed 1,800 firms and while 97 percent agreed the regulation would affect them, only 5 percent were fully prepared and 33 percent were halfway to complying."[1] These statistics indicate that despite best efforts to prepare – including the many opt-in cookie pop-ups companies are using on their websites – there likely will be losses from violations and alleged violations of GDPR.

Non-Penalty Losses Under GDPR

An example of a potentially large expenditure that is not a fine and that may arise under GDPR rules is the cost of notifying persons whose data you hold when there is a *suspicion* of a breach. While some states have required notification to be sent when there is a breach and a company reasonably suspects that consumer data may have been compromised, GDPR backs that analysis up even further.[2] It establishes that notification requirements apply where there is a suspicion – as opposed to confirmation – of a breach itself. And, of course, GDPR applies to everyone in the EU. Just measuring the extent of notification that is required could prove cumbersome, when the extent of a suspected breach itself remains unconfirmed. Such notification being required even before a business has yet to determine definitively that a breach took place and data was in fact compromised could be costly.

In such a notification scenario, a cyberpolicy may be triggered and provide coverage for those notification costs. Policyholders should be wary, however, of any limiting language for breach notification policies. Language limiting coverage for such costs to instances where there is a confirmed breach could be problematic. Similarly, if a particularized type of determination as to the necessity of breach notification is required to trigger coverage, policyholders should be careful to make sure the language includes instances where a breach is suspected. Even where there is limiting language, coverage may still be

Daniel J. Healy is a partner in Anderson Kill's Washington, D.C., office. He is the deputy co-chair of Anderson Kill's cyber insurance recovery practice group and a member of the firm's blockchain & virtual currency and regulated products groups. Reach him at dhealy@andersonkill.com.

available and policyholders should take care to demonstrate that they are complying with coverage requirements.

In some circumstances, GDPR notification rules can require that notice be sent within 72 hours. This kind of time pressure could present a herculean and expensive task, depending on the number of records involved.

Another type of GDPR-mandated cost that may well be covered under cyberpolicies is also collateral to the fines and penalties. GDPR requires in some circumstances that a "controller" of personal data be in place to notify the relevant authorities "without undue delay." Additionally, in the event of a breach a response team, forensic analyses and remedial action may be needed, as well as replacement of data, equipment and other items. Many of these costs may be covered, including costs to perform them in a manner compliant with GDPR.

D&O policies often apply when violations and liability result from board-level decisions or actions.

Losses From Penalties and Fines

Of course, the potentially draconian fines that GDPR may impose on a company should not be overlooked. Policyholders should not assume that they have no coverage for any such fines. Policy language can be divergent and ultimately critical to whether coverage is available. Cyberinsurance policies often specifically provide coverage for "fines and penalties." That policy language should make coverage for GDPR fines and penalties relatively straightforward.

Other cyberpolicies may not contain specific coverage for such fines and penalties. Those policies will present more of a potential problem in seeking coverage. Policy language that may need to be considered might include the scope of the third-party liability coverage grant, which may provide coverage for all amounts owed to third parties, including government entities. Language providing coverage when "unauthorized access" to data takes place can be broad and provide coverage for the various losses stemming from the unauthorized access to personal records.

Additional coverages that, if worded broadly, may provide applicable coverage include regulatory liability coverage and network security liability coverage. If these coverages have no geographic limitations, then that would only further support coverage for GDPR fines and penalties.

The basis for the fine may matter. The tier of higher-dollar fines can be assessed for a variety of reasons, including processing personal data without express consent or alternative justifications; failure to provide data subjects with transparent information about their rights; failure to provide access to an individual's own data; failure to correct inaccurate data; and transferring data outside the EU without following the rules. Many of these fines could be incurred based on mere negligence and mistake. Depending on the conduct underlying a violation, different coverage may apply and, in the absence of exclusionary language, provide coverage for a resulting fine.

Policyholders still need to check for limiting language and for exclusions elsewhere in the policy that insurance companies may cite to avoid coverage. Those could be specific to fines and penalties, could be geographic limitations or could be drafted in a manner to exclude violation of GDPR-specific requirements.

Other Policy Language That May Provide Coverage

Since many companies are adopting, or will soon adopt, compliance programs to meet GDPR standards, it may be important to review the terms of any applicable cyberpolicy for limitations as to internal compliance programs. At one end of the spectrum, the facts that a particular loss or liability arose from the breach of

an internal privacy policy may serve as a trigger for coverage. In other words, the fact that an employee breached the employer's privacy policy and the breach resulted in liability may suffice to trigger coverage. Policyholders may be wise to draft internal security and compliance programs (for many reasons) to reflect applicable GDPR standards, particularly if they expect to face GDPR risks and would like to seek coverage for those risks.

Depending on the conduct underlying a GDPR violation, different coverage may apply.

Potentially Exclusionary Language

Exclusions intended for spammers that defeat coverage for unlawful collection of data or communications could be used inappropriately to deny coverage for alleged violations of GDPR. GDPR has stringent restrictions on data collection and on using data to communicate. Policyholder businesses should be careful not to permit insurance companies to label certain events as unlawful collection or communications, particularly where the collection is of information voluntarily provided by consumers.

A major exclusionary issue will be for jurisdictions – European countries – that specifically enact law that does not allow policyholders to insure against the fines and penalties. Insurance policies containing exclusions for uninsurable interests will not likely cover fines and penalties levied by governments that also pass law stating the fines and penalties cannot be paid by insurance. Less clear will be where insurance policies do not have explicit exclusionary language or where a particular law addresses only some of the fines and penalties that may be levied for particular violation.

Choice of law issues may be central to coverage. If a U.S. policyholder faces fines from a foreign state and seeks coverage under a policy issued in the U.S. and that is subject to U.S. law for purposes of determining coverage, there may be routes to coverage. Those disputes may turn on the exact policy language, the applicable state law and other nuances, but policyholders should not assume there is no coverage just because a foreign statute says a particular loss is not insurable.

Other Policies

Lastly, policyholders should not forget to review other lines of coverage. In many cases, depending on the allegations and facts of the alleged violation, E&O and D&O liability policies may provide coverage. E&O policies often apply when a violation took place during an employee's performance of her job in providing a service. D&O policies often apply where the violation took place because of a board-level decision or action that led to liability. Where these policies do not have broad exclusions for electronic data-related liability, they often apply to data-related losses. ■

[1] "Most Organisations Unprepared for GDPR, survey finds," Emmanuel, Zach, ComputerWeekly.com, (April 27, 2018) (available at https://www.computerweekly.com/news/252440114/Most-organisations-unprepared-for-GDPR-survey-finds)

[2] *See, e.g.*, Maryland Personal Information Protection Act, Md. Code Com. Law § 14-3504.