Finding Coverage for GDPR Liabilities

by Robert M. Horkovich and Daniel J. Healy

With the European Union's General Data Protection Regulation (GDPR) taking effect this past May, companies need to consider the application of liability insurance to cover certain losses and liabilities related to the new rule. On July 6, 2018, the Information Commissioner's Office (ICO) issued the first GDPR Enforcement Notice against Aggregate IQ Data Services Ltd (AIQ), a Canadian tech company that focuses, among other things, on digital advertising

relating to political issues. The notice highlighted AIQ's use of personal data to target advertising for U.K. organizations. The use of personal data was found to violate the GDPR because AIQ "processed personal data in a way that the data subjects were not aware of, for purposes which they would not have expected, and without a lawful basis for that processing."

The ICO gave AIQ 30 days to cease all improper processing of personal data, or be subject to penalties consisting of the higher of either €20 million or 4% of AIQ's total annual worldwide turnover. Faced with this tight timeline and huge fines, AIQ appealed and the appeal remains pending.

This first Enforcement Notice underscores the importance of considering how insurance coverage may come into play. While considerations of GDPR liability often focus on the potentially large penalties, the AIQ notice demonstrates that the significant costs may be in forms other than fines and raises important insurance considerations.

NOT ALL GDPR LOSSES ARE FINES

One example of a potentially large loss imposed by GDPR rules is the cost of notifying persons whose data you hold when there is a suspicion of a breach. While some U.S. states require notification to be sent after a known breach even for data that is suspected to be compromised (see for example, Maryland Personal Information Protection Act, Md. Code Com. Law § 14-3504), GDPR goes further, potentially including situations where a breach itself only is suspected. GDPR also applies to any customers in the EU. Just measuring the extent of required notification could prove cumbersome.

But from a conceptual standpoint, notification under the GDPR is not necessarily different from notification in the United States. A cyber policy may be intended to cover exactly such notification costs. Policyholders should take note of what policy language they have and what constitutes a covered notification. Even where there is limiting language, coverage still may be available and policyholders should take care to demonstrate that they are complying with coverage requirements.

Similar GDPR-mandated costs may include appointing a "controller" of personal data, forming a breach response team, conducting forensic analyses, and taking remedial action to contain a breach. Coverage should not be overlooked for such steps and costs just because they are performed in compliance with GDPR.

PENALTIES AND FINES STILL REMAIN A CONCERN

Of course, the potentially draconian fines that GDPR may impose on a company cannot be ignored. Some cyber insurance policies specifically provide coverage for "fines and penal-

RISK MANAGEMENT

Reprinted with permission from Risk Management.

www.rmmagazine.com

ties." That policy language should make coverage for GDPR fines and penalties relatively straightforward.

Other cyber policies may not contain specific language, but may include broad liability coverage of all amounts owed to third parties, including government entities. Coverage for instances of "unauthorized access" to data can be broad and focused on the means of access rather than the form of loss. Other coverage grants that may provide applicable coverage include regulatory liability coverage and network security liability coverage.

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.

TAKE NOTE OF POLICY LANGUAGE SPECIFICALLY APPLICABLE TO LIABILITY

One example of variant policy language that may be dispositive concerns companies adopting compliance programs to meet GDPR standards. A point to consider is whether an employee's breach of an employer's privacy policy, and the resulting liability, triggers coverage. Where a policyholder-company has compliant procedures in place which are not properly followed, coverage for the employee's conduct may not be lost just because the consequent liability is under GDPR.

BEWARE OF POTENTIAL EXCLUSIONS

Insurance companies may argue that exclusions intended for spammers purportedly defeat coverage for unlawful collection of data or communications. They may attempt to use these exclusions—inappropriately—to deny coverage for alleged GDPR violations. Policyholders should be prepared to explain why these exclusions should not apply to GDPR claims.

Insurance companies can also be expected to point to the laws of European countries that specifically bar insurance against fines and penalties. These arguments may successfully defeat some, but not all, coverage obligations. For example, a U.S.-based company relying on an insurance policy delivered in the United States and subject to U.S. law may have arguments against the application of European laws to a coverage dispute, including based on which laws apply to coverage determinations and policy interpretation.

CONSIDER NON-CYBER 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. Companies doing business in Europe and with EU citizens that could potentially face GDPR losses and liabilities should consider the application of these existing liability policies as well. ■

Robert M. Horkovich is managing partner and shareholder in the New York office of Anderson Kill. He is a trial lawyer who has obtained more than $5 billion in settlements and judgments for policyholders from insurance companies. **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 and virtual currency and regulated products groups.

RISK MANAGEMENT

Reprinted with permission from Risk Management.

www.rmmagazine.com