JONES DAY

COMMENTARY

NOVEMBER 2018

IN SHORT

The Situation: The European Union's General Data Protection Regulation ("GDPR") has raised questions regarding the scope of coverage and protection afforded by current cyber policies, especially with respect to potential GDPR fines.

The Recommendation: Along with other actions, policyholders should amend their policies to ensure they have coverage for *processing* violations, confirm their policies expressly cover regulatory fines, and evaluate whether their policies carry sufficient limits to respond to the potentially enormous fines under the GDPR.

Looking Ahead: Companies subject to the GDPR should continually evaluate their policies to ensure they have adequate coverage under the new regulations.

The European Union's GDPR has created significant legal risks for companies conducting business in Europe, and it has also generated increased demand for cyber insurance. Questions exist, however, regarding the scope of protection provided by cyber policies, and companies may find it necessary to modify policies to obtain adequate coverage.

The GDPR includes many new requirements to strengthen protections for personal data. Companies could face significant penalties for noncompliance, which can reach €20 million or four percent of annual revenue, whichever is higher. For companies that suffer a data breach, the GDPR creates mandatory notification obligations and the risk of individual damage claims. Taken together, these factors have dramatically changed the risk exposures for companies that collect or process data within the European Union.

To date, we have not seen the emergence of EU-specific cyber policy forms. Instead, insurers have tried to address GDPR risk by adding language or endorsements to existing policies. One insurer is offering a GDPR endorsement that covers defense costs, damages, and penalties resulting from:

> any Claim first made against any Insured during the Policy Period for a violation of the EU General Data Protection Regulation (or legislation in the relevant EU jurisdiction implementing this Regulation).

Another insurer is offering pre-breach network monitoring services by a third-party vendor as a way of mitigating GDPR risk.

> Under the laws of some EU Member States, regulatory fines are uninsurable as a matter of public policy. The issue is whether such a rule should apply to a GDPR fine imposed for mere negligence in safeguarding personal data.

Lurking beneath these efforts is a fundamental uncertainty as to whether cyber policies will cover GDPR fines. Under the laws of some, but not all, EU Member States, regulatory fines are uninsurable as a matter of public policy. The issue is whether such a rule should apply to a GDPR fine imposed for mere negligence in safeguarding personal data. This is a pressing question for policyholders—one that regulators and brokers have been unable to answer.

A spokeswoman for the Information Commissioner's Office, Britain's data protection regulator, has said, "there is nothing in the GDPR which either permits or prohibits insurance coverage against fines." Also, one major insurance broker has warned that policyholders should "assume nothing" regarding the insurability of GDPR fines. In the absence of better guidance, it will be up to policyholders and their coverage counsel to develop strategies for enhancing coverage for GDPR risks.

Recommended Actions

When reviewing existing policies, corporate policyholders should consider the following:

Cyber insurance typically covers first- and third-party losses arising from the *disclosure* of personal information in a data breach or cyber incident. The GDPR, however, regulates the *processing* of personal data. Processing violations could result from the length of time an individual's data has been stored or the failure to erase personal data upon request (the "right to be forgotten"). Some current cyber policies would not cover such processing claims because they do not involve the unauthorized disclosure of data.

Policyholders should amend their policies as necessary to ensure they have coverage for processing violations.

The question of whether GDPR fines are insurable may not be resolved any time soon. Yet insurers continue to sell cyber policies that promise to cover GDPR fines. Policyholders should take advantage of this market reality to: (i) obtain the best available coverage for GDPR risks; and (ii) include provisions that reduce the likelihood that coverage will be voided on public policy grounds. Companies should ensure their policies expressly cover regulatory fines, particularly where the fine is not the result of intentional misconduct. Regulatory coverage should include a specific reference to the GDPR.

Policyholders should also ensure that other policy terms do not operate to limit coverage for civil fines. In addition, it may be useful to include a choice of law provision based on "most favorable jurisdiction," similar to those used for punitive damages coverage. Policyholders should undertake an analysis, with the assistance of counsel, to determine which jurisdictions might give rise to a GDPR proceeding and whether policy language can be added to select a governing law favorable to coverage.

Policyholders should assess whether their cyber policies afford sufficient limits to respond to the potentially enormous fines under the GDPR. This will involve consideration of the nature and scope of the company's business operations, the strength of its cybersecurity, and the specific exposures it faces under the GDPR. Corporate policyholders must also pay close attention to deductibles, self-insured retentions, and sub-limits, which are often used to limit regulatory coverage.

The GDPR is already in place and applies to companies operating in the European Union as well as companies outside the European Union that offer goods or services to EU residents.

Any company subject to the GDPR should evaluate the issues described here when placing or renewing cyber insurance programs, to ensure their policies address the risk exposures created by the new regulatory regime.

THREE KEY TAKEAWAYS

1. Cyber insurance typically covers losses arising from the *disclosure* of personal information in a data breach or cyber incident. The GDPR, however, regulates the *processing* of personal data.
2. As a matter of public policy, regulatory fines are uninsurable in some EU Member States.
3. Companies subject to the GDPR should make certain their policies address the risk exposures created by the new regulatory regime.


Matthew L. Jacobs
Washington


Richard DeNatale
San Francisco


Mauricio Paez
New York


Undine von Diemar
Munich

Irene Robledo, an associate in the Madrid Office, assisted in the preparation of this Commentary.

All Contacts >>>

YOU MIGHT BE INTERESTED IN: **Go To All Recommendations >>**

Belgium Publishes Data Protection Laws Implementing

Is Your Insurance Program Ready for California's New Data Privacy

Italian Data Protection Decree Harmonizes National Law with

GDPR | Law? | GDPR Provisions

SUBSCRIBE SUBSCRIBE TO RSS 

Jones Day is a global law firm with more than 2,500 lawyers on five continents. We are One Firm Worldwide℠.