THOMSON REUTERS
Westlaw®

GDPR is here. Is your cyberinsurance ready?

By James E. Scheuermann, Esq., Lucas J. Tanglen, Esq., and Reymond E. Yammine, Esq., *K&L Gates*

AUGUST 3, 2018

The European Union's General Data Protection Regulation, which took effect May 25, is designed to protect individual privacy. Cyberinsurance policies are predominantly — though not exclusively — focused on insuring losses arising from cybersecurity failures.

As U.S. corporations readied themselves for GDPR compliance, some reached out to their brokers and coverage counsel to determine the extent to which their current cyberinsurance policies would provide coverage for potential GDPR-related liabilities.

Even though the GDPR has now taken effect, it is not too late for corporate policyholders to review their cyberpolicy terms in light of the new exposures created by the GDPR. This article provides a brief overview of new liabilities created by the GDPR and explores some of the key cyberinsurance questions that it raises.

GDPR OVERVIEW

Broadly speaking, the GDPR is a far-reaching regulation intended for "the protection of natural persons with regard to the processing of personal data."[1] Its broad definition of "processing" encompasses many aspects of the usage of personal data, including its collection, storage, alteration, use and transmission.

> The GDPR imposes obligations on individuals and organizations that may have no presence in the EU but process data (or monitor behavior) of individuals in EU nations.

The statute has a broad geographical reach: It imposes obligations on individuals and organizations that may have no presence in the EU but nonetheless process data (or monitor behavior) of individuals in EU nations.

The GDPR recognizes various individual rights including, among others, rights to access one's personal data, to rectify inaccurate personal data and thereby ensure the integrity of data, and to erase personal data (the "right to be forgotten").

It also imposes certain requirements to promptly notify the relevant supervisory authority in the event of a personal data breach and, where the breach is likely to result in a high risk to rights and freedoms, to notify the affected individuals.

Violations of GDPR provisions can give rise to both private causes of action and public enforcement actions. Individuals can seek to enforce their GDPR rights by lodging a complaint with the appropriate supervisory authority or filing a lawsuit for damages in the courts of a relevant member state.

In terms of public enforcement, each member state has the authority to enforce the GDPR, including by imposing fines, through its designated supervisory authority.

Depending on the nature and severity of a violation, GDPR fines could reach up to 20 million euros or 4 percent of a company's total worldwide annual revenue, whichever is higher. EU member states may also enforce their own more specific data-related rules.

GDPR INSURANCE CONSIDERATIONS

Because there is no industry "standard" cyberinsurance policy form, we will not attempt to provide a comprehensive analysis of policy wording that may be relevant to GDPR liabilities. Rather, the following discussion is a starting point for assessing your company's cyberinsurance in light of the GDPR.

Does the policy cover GDPR claims that do not involve an actual breach of 'personal data'?

The GDPR imposes requirements related to the "processing" of personal data. It also recognizes individual rights related to personal data, including with respect to data integrity.

Cyberpolicies commonly provide coverage with respect to actual (or even potential) breaches of "personal data." However, the GDPR can impose liability for a broad range of conduct relating to "personal data" independent of a breach involving such data.

For example, a cyberpolicy might cover certain "privacy perils," defined to include the unauthorized release of private information, identity theft and the failure to protect private information.

If a policyholder is found liable under the GDPR for storing "personal data" beyond the permissible storage period, the insurer might argue that the violation was not a covered "privacy peril."

While policyholders certainly may assert strong arguments that such "breach-centric" coverages apply to a variety of GDPR claims, for some policyholders it may be worthwhile to pursue an endorsement that defines the insured risk to more clearly cover

liability arising not only from data breaches, but from all the various activities within the GDPR's scope of "processing."

This scope includes the collection, storage, alteration, use and transfer of "personal data," as well as the failure to provide individuals with information regarding their rights as to their "personal data."

Notably, some policies on the market seem to take a broader approach to defining the scope of coverage with respect to personal data-related liabilities.

For example, one cyberform broadly defines the term "privacy breach" to include:

- The unauthorized collection, disclosure, use, access, destruction or modification, or inability to access, or failure to provide private information."
- "An infringement or violation of any rights to privacy."
- "Failure to comply with any federal, state, local or foreign statute, rule, regulation or other law pertaining to the Assured's responsibilities with respect to private information."

This approach to defining the scope of insured conduct strongly suggests an intent to provide broad coverage for many categories of conduct covered by the GDPR.

Of course, even with wording suggesting a relatively broad scope of covered conduct, policyholders may find it productive to carefully consider their current policy language in light of the types of acts or omissions from which GDPR liability might arise.

How does the policy define 'personal' or 'private' information?

To trigger coverage for a GDPR claim, a policyholder may need to establish that the data at issue falls within the policy's definition of "personal information," "personally identifiable information," "private information," or a similar term. The operative term in the GDPR, "personal data," is defined quite broadly as:

> *any information relating to an identified or identifiable natural person* ('data subject'); an identifiable natural person is one who can be identified, *directly or indirectly*, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. (Emphases added.)

The next step is to consider whether your cyberinsurance policy's definition of "personal information" (or a similar term) captures the type of "personal data" and related conduct that is at issue in the claim asserted.

Some policies provide flexible definitions of "personal information" that seem likely to encompass the full scope of GDPR "personal data."

For example, one cyberpolicy form defines "private information," in relevant part, as either "information that can be used to determine, distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual," or "any information that is linked or linkable to a specific individual and that is subject to any privacy law" (with "privacy laws," in turn, defined as "statutes, rules, regulations, and other laws associated with the confidentiality, access, control, or use of private information").

> Depending on the nature and severity of aviolation, GDPR fines could reach up to 20 million euros or 4 percent of a company's total worldwide annual revenue, whichever is higher.

Some other policies define "personal information" descriptively (e.g., by providing specified categories of information such as name, Social Security number, account numbers or telephone numbers), by reference to specified privacy-related statutes (e.g., "protected health information" within the meaning of the Health Insurance Portability and Accountability Act), or by a combination thereof.

This more descriptive approach may create gaps between the very broad GDPR definition of "personal data" and a more circumscribed policy definition of "personal information" (or a similar term).

An insurer that issued cyberinsurance using the descriptive approach may be willing to issue a policy endorsement expressly confirming that the policy's definition of "personal information" (or a similar term) is at least as broad as the GDPR's definition of "personal data."

Does the policy cover fines?

The potentially enormous regulatory fines that are authorized under the GDPR have captured the attention of many U.S. executives and risk managers. If a company is subject to a GDPR fine, will its cyberinsurance pay?

Assuming that the GDPR-violating conduct at issue is within the scope of a policy's coverage, and that the policy provides worldwide coverage (as most do, and which prudent U.S. policyholders may wish to confirm), the question of coverage for a potential fine might require consideration of at least three issues.

1. Does the policy wording provide that the insurer must pay for regulatory fines?

The analysis begins by considering whether your cyberpolicy covers regulatory actions in addition to claims for damages brought by individuals (or classes of individuals) whose "personal data" is affected.

Even if regulatory coverage is specified, a careful review of all pertinent definitions (e.g., "damages," "loss," "regulatory loss," "penalties") and coverage exclusions may be necessary to confirm that the policy language consistently provides that the policy is intended to pay civil fines.

2. Do the law and public policy that govern the insurance policy prohibit or restrict coverage for fines?

Some U.S. jurisdictions may prohibit or restrict the insurability of civil fines as a matter of law or public policy, regardless of the policy wording.[2]

In other words, even where both the insurer and the insured intended coverage for fines, a court might hold that allowing the insurer to pay the fine would impermissibly relieve the insured of the consequences of its own illegal action.

The markets seem to be aware of this tension between corporations' interest in obtaining broad coverage for fines and potential judicial resistance to enforcing such coverage.

Some insurers appear willing to include flexible policy wording intended to limit the chances that bargained-for coverage for fines could be judicially unwound on public policy grounds.

> The GDPR can impose liability for a broad range of conduct relating to "personal data" independent of a breach involving such data.

For example, one cyberform provides that fines will be covered "if insurable by law" and that "insurability shall be determined pursuant to the applicable law of the jurisdiction that most favors coverage."

3. Will the EU regulators prohibit the use of insurance funds to pay the fine?

Certain European nations might prohibit or restrict coverage for fines as a matter of law and public policy.

This raises a question whether the supervisory authorities that are authorized to impose fines under the GDPR might prohibit their payment with insurance funds even if the relevant policy wording and the law governing the insurance contract would otherwise permit coverage.

In that case, it may be that there is nothing the policyholder or the insurer can do by way of policy wording to ensure coverage for GDPR fines.

It should be noted that even in the event that a regulatory fine is not covered, cyberinsurance may nonetheless provide valuable coverage for the costs of defending against GDPR regulatory actions.

Does the policy contain any limiting exclusions?

In any review of insurance policy wording, it is important to consider coverage exclusions that have the potential to divest your company of what first appeared to be very broad coverage.

For example, a cyberpolicy might cover a broad range of data-related conduct extending beyond actual data breaches (e.g., claims based on the company's use and retention of personal data) in the first instance, but also incorporate an exclusion that restricts coverage for certain categories of GDPR-related activities.

One cyberform contains an exclusion for "gathering or distribution of information," which excludes coverage for claims arising out of "the unlawful collection or retention of personally identifiable information or other personal information of the insured organization; but this exclusion will not apply to claims expenses incurred in defending the insured against allegations of unlawful collection of personally identifiable information."

Some insurers might argue that such an exclusion might divest the insured of valuable coverage for fines, judgments or settlements based on a subset of potential GDPR violations (although apparently leaving defense coverage intact).

Does the policy cover the cost of providing GDPR-required notices?

Cyberpolicies commonly cover the costs of providing notice of data-related incidents to the individuals whose data is affected and to appropriate authorities.

In the absence of express coverage for the costs of notifying supervisory authorities, as may be required by the GDPR, a policyholder might successfully argue that ambiguous policy wording covering, for example, the costs to "comply with any legal obligation to notify affected parties" or to "minimize harm" should be construed to cover the costs of any notice required to the supervisory authorities charged with enforcing the GDPR.

Insurers may be willing to issue an endorsement making explicit their intent to cover notice-related costs.

Does the policy provide sufficient limits?

The financial terms of cyberpolicies — limits, deductibles, waiting periods and so on — are just as important in managing cyber risk as the coverage terms.

Are your policy limits sufficient in light of the massive potential fines? Deductibles or self-insured retentions may limit the policyholder's ability to access coverage until after it has incurred substantial costs.

In addition, sublimits may limit the policyholder's recovery. For example, some cyberpolicies may provide a "regulatory" sublimit that caps the insurer's liability with respect to regulatory actions at an amount substantially less than the policy's per claim or aggregate limits.

CONCLUSION

There is no time like the present to review, with assistance of counsel, your company's cyberinsurance with respect to these and other coverage issues that may arise under the GDPR.

Taking a proactive approach to negotiating appropriate coverage may provide valuable protection for the corporate bottom line.

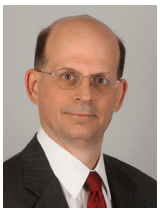
NOTES

[1] Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) 2016 O.J. (L 119) 1.

[2] *Compare City of Fort Pierre v. United Fire & Cas. Co.*, 463 N.W.2d 845, 848-49 (S.D. 1990) (civil penalties for Clean Water Act violation uninsurable as a matter of public policy), with *Weeks v. St. Paul Fire & Marine Ins. Co.*, 673 A.2d 772, 775 (N.H. 1996) (insurer may be liable for fines and penalties not expressly excluded by policy language).

This article first appeared in the August 3, 2018, edition of Westlaw Journal Insurance Coverage.

ABOUT THE AUTHOR



James E. Scheuermann (L) is a partner in the Pittsburgh office of **K&L Gates**, where he represents policyholders in insurance coverage matters. He has provided counsel on, litigated and mediated a wide variety of cyberinsurance matters. **Lucas J. Tanglen** (C) is a senior associate in the firm's Pittsburgh office. He represents policyholders, including with respect to the review and placement of cyberinsurance policies. **Reymond E. Yammine** (R) is also an associate in the firm's Pittsburgh office, where he has a broad-ranging, litigation-focused practice.