MARSH

INSIGHTS | SEPTEMBER 2018

GDPR Fines and Penalties: Insurability will Vary by Location, Policy Details, and More

Following two years of preparation, the EU General Data Protection Regulation (GDPR) took effect on May 25. GDPR's wide-reaching provisions are revolutionizing the data protection landscape worldwide, obliging subject companies to review and enhance their privacy and data protection practices — or face significant fines, penalties, and other costs, including for notification, defense, and restoration.

Insurability of Fines and Penalties is the Central Question for Many Organizations

Three months after enactment of the GDPR, a primary question for many stakeholders is how the various costs of compliance and non-compliance will interplay with organizations' insurance policies. While numerous scenarios have been postulated, it's critical to keep in mind that any consideration of GDPR and insurability must begin with the insurance contract itself.

For many organizations, fines and penalties are top of mind due to their potential size, variance according to local law, being as yet untested in court, and the issue's resonance with board members. Under the two-tier structure, the most serious GDPR infringements could bring fines as high as €20 million or 4% of global revenue, whichever is greater. For other breaches, authorities could impose fines of up to €10 million or 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

> *"Insurability of GDPR fines is more grey than a black or white certainty."*

A common question from insureds is: "Will our insurance policy respond in the event that we are faced with a fine or penalty?" The answer is likely to depend on the circumstances, including the policy wording and applicable governing law.

Answering the insurability question begins with a review of an organization's insurance program and an understanding of which policies might provide coverage. After identifying which policies might respond, a detailed review of the terms and conditions of each relevant insurance contract should be undertaken. The review should identify whether the policy expressly provides coverage for an administrative fine under the GDPR, the insured's domicile, and the choice of law provision in the policy — all key factors in determining the policy's response.

Because the ability to recover the costs for such fines will vary greatly depending upon these factors, we believe that the insurability of a fine for non-compliance with the GDPR is more of a grey area than a black or white certainty, with varying degrees of uncertainty depending on the geography and relevant insurers. In developing an informed view about insurability, companies should assume nothing: Consult your policy, insurers, insurance advisors, and legal counsel.

GDPR Considerations in the European Union

Data protection liability coverage is not a new concept in the EU. A number of policies traditionally provide cover for insureds that face liability in the event of a data protection breach. So which policies might an insured turn to following an instance of non-compliance? Typically, these would include casualty, professional indemnity (with and without cyber extensions), legal expenses, D&O, and cyber.

For organizations that do not have a cyber policy, the limited nature of coverage available within casualty and professional indemnity policies could make it necessary to look to obtain insurers' agreements to enhance their standard coverage, likely at some additional premium cost. This is particularly the case where organizations are looking to obtain coverage for some of the additional costs often incurred following discovery of a data breach.

Coverage: Varies in Scope and Availability, but Can Include Fines and Penalties

CONTINENTAL EUROPE

Cyber coverage, generally, is responsive only to post-breach or incident costs under the types of policies listed above, although Marsh has in many instances negotiated coverage that responds to a broader set of triggers. Any coverage review must consider how these policies may assist with the financial consequences when your organization is faced with a data breach or cyber incident. This means reviewing the nature of the insuring clause that could trigger the coverage, and then considering exclusions and sub-limits.

In Continental Europe, since about 2010, cyber policies as drafted are likely to cover the majority of consequences around non-compliance with GDPR, including fines if they are insurable within the respective jurisdiction. This leads to determining whether it is necessary to amend cyber coverage to make it apply to post-breach or incident costs.

UNITED KINGDOM

Standard cyber policies in the UK vary as to how they might respond to a regulatory event. Most cyber policy forms we see provide some level of coverage for fines where insurable. However, the exact nature of the insuring agreement may vary significantly so, as in Continental Europe, a review of that trigger is important. For example, coverage from one leading insurer would be triggered only for fines and investigations pursuant to a loss of personally identifiable information (PII) or corporate data, meaning the wider GDPR exposures, such as alleged non-compliance with the right to erasure, would not be covered.

Within the UK, leaving cyber policies aside, certain classes of insurance will provide some form of cover following a data breach, such as public liability, employers liability, professional indemnity, and legal expenses. Standard insurer-based wordings in these classes tend only to provide indemnity for third-party compensation for breach-related distress or damage, along with legal defense expenses. Generally, these wordings will not provide indemnity for additional costs and expenses an organization faces following a data breach, such as data breach support, notification, and public relations costs.

Further, the existing cover within public liability and employers liability policies is often expressly tied to breaches of the UK Data Protection Act (UK DPA) of 1998, so policy amendments need to be made to ensure that equivalent cover is provided in the event of a breach of the 2018 UK DPA and the GDPR. Notably, casualty and professional indemnity policies will normally exclude cover for fines and penalties.

Following the introduction of GDPR, UK insurers generally are looking to retain the cover available. At the same time, Marsh is seeing sublimits introduced in some cases on public liability and employers liability policies, as well as additional insurer requests for information related to handling of PII and measures taken to prepare for GDPR implementation. Although the existing cover typically is being maintained, it may now be further restricted in terms of limits available. In any event, it is unlikely to provide financial compensation for administrative fines an organization may face.

Insurability: Uncertain, Depends on Country-by-Country Determinations

CONTINENTAL EUROPE AND UNITED KINGDOM

The insurability of GDPR fines and penalties may not have uniform application in the EU. GDPR itself is silent on the issue. A key consideration is whether the relevant regulator has stipulated that its fine cannot be recovered from any third party. Within the UK, the Financial Conduct Authority has expressly prohibited the insurability of fines imposed by it on FCA regulated firms. To date, we do not know the position of the UK Information Commissioner's Office on the recoverability of an administrative fine levied for non-compliance with the GDPR.

Another factor in considering insurability is forum. Because GDPR is silent on the insurability of fines and penalties, there is likely to be variability across member states and regulatory authorities. Some expressly ban the insurability of administrative fines, others have not as yet commented, some remain unclear, while yet others are supportive of coverage.

The choice of law where the insurance policy was written will also be a factor. GDPR fines are civil in nature, but the regulation permits member states to impose their own penalties for personal data violations. If those penalties are criminal, or involve deliberate wrongdoing or gross negligence on the part of the insured, they are unlikely to be covered by insurance.

Given the variance by country, it would be incorrect to make any blanket statements about insurability for Europe as a whole. More importantly, it is not a question to be answered solely by individual insurers, companies, or brokers — decisions of insurability are likely to be clarified in the first instance as a matter of case law in each country.

It is useful to note that some cyber insurers have indicated they will look to pay under affirmative grants where permitted and, in some instances, have taken advice to support their intent to pay in certain circumstances, although without elaborating upon what those circumstances would be.

"Given the variance by country, it would be incorrect to make any blanket statements about insurability for Europe as a whole."

Conclusions for EU Countries

For organizations based in EU countries, it is generally possible to obtain a policy that contains an insuring clause for regulatory fines and penalties, such as for fines that may be levied in the event of non-compliance with the GDPR. However, organizations should be mindful that while a policy may contain such an insuring clause, this is no guarantee that the policy will respond.

There are potential impediments to recovery of fines and penalties, and there are instances of variance. For example, certain factors will need to be taken into account by the supervisory authority, including the potential impact of exclusions for deliberate or intentional acts.

It is important to work closely with your insurance advisors and check your insurance contract language in an effort to optimize coverage. As part of the process, you should also consider, with your legal counsel as appropriate, the laws of local member states and where the policy originated.

GDPR Considerations in the United States and Canada

Coverage: The Evolution of US and Canadian Markets

In the US and Canadian insurance markets, most "off-the-shelf" cyber policies provide some form of GDPR coverage where a cyber incident is the trigger, namely with respect to breach response costs, such as forensics and personal notifications. Standard cyber policies also likely provide coverage for related defense costs resulting from a regulatory action commenced by an EU Member State Data Protection Authority.

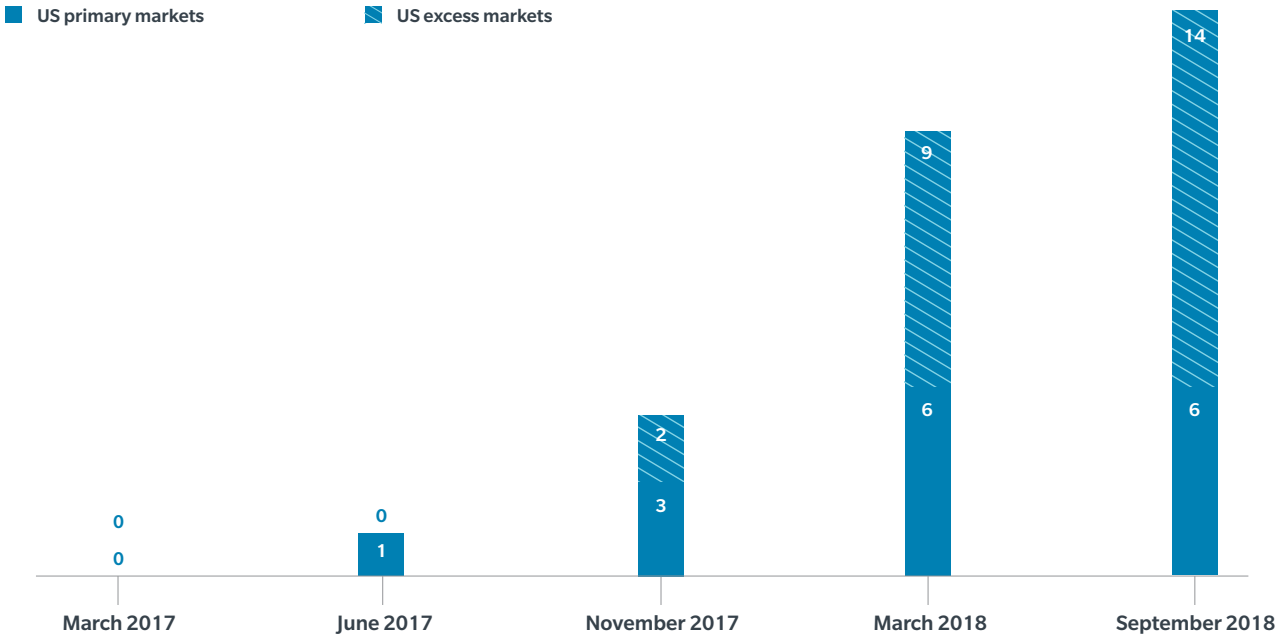
However, until recently, the intent of most cyber policies written in the US and Canada was to not provide coverage for fines and penalties pertaining to organizational privacy practices and compliance where a cyber incident was not necessarily the trigger. Identifying this potential gap, Marsh has worked with major US and Canadian insurance markets to secure broad coverage for GDPR fines and penalties for multiple clients, where lawfully insurable.

At this writing, at least six major US primary markets — collectively comprising a significant share of the US cyber insurance market — and five major Canadian primary markets have either agreed to provide this coverage by amending their policy language, or confirmed the intent of existing language to include GDPR fines and penalties.

With a regulatory exposure as comprehensive and unpredictable as the GDPR, insurers in the US and Canada vary considerably in how and to whom they will provide this coverage. Some carriers provide coverage for GDPR fines only on a case-by-case basis; others do so more broadly. Similarly, some require interested insureds to fill out additional underwriting questions or provide other supplementary information. The scope of coverage also varies, and negotiations regarding additional exclusion waivers or policy rewording may be required to ensure the policy responds as intended.

Number of US insurance markets providing broad coverage for insurable GDPR fines and penalties

SOURCE: MARSH ANALYSIS



As of September 2018, US markets that are providing coverage for GDPR fines and penalties by amending their policy language, or confirming their intent to include GDPR fines and penalties within their existing policy language.

Insurability: Domicile may Influence Ability to Recoup Fines and Penalties

UNITED STATES

The question of insurability of GDPR fines and penalties in EU countries seems to depend largely on EU member state laws and ensuing judicial determinations; however, in the US, domicile may influence the ability to recoup fines and penalties.

As of September 2018, Marsh has confirmed with several major insurers their intent to pay covered claims for US companies, so long as such fines are presumed to be insurable under relevant US state laws governing insurance contracts. It is possible, however, that other carriers may deny a claim based on public policy determinations where the GDPR fine or penalty is clearly uninsurable in the EU member state where levied.

Despite this variance, the key takeaway is that the insurability of a fine or penalty according to the laws of the issuing EU member state is not the only factor for insurance recovery by US companies. With several major primary and numerous excess markets currently agreeing to provide this coverage broadly to US companies, it is difficult to envision valid related claims not being paid. And, in the event an insured negotiates a claim settlement with its carrier, that settlement may offer alternative recovery options.

> *"Marsh has confirmed with several major insurers their intent to pay covered claims for GDPR fines and penalties for US companies."*

CANADA

The insurability of fines and penalties in Canada is not yet clear. Canadian courts have not directly resolved the issue, although there is commentary suggesting that where such losses are criminal or penal in nature it would be contrary to public policy to insure such losses. An open question is whether civil or non-criminal fines and penalties are insurable in Canada. Until Canadian courts resolve this issue, express coverage for GDPR fines and penalties provides policyholders with the opportunity to argue that they are covered.

CONCLUSION FOR US AND CANADA

Despite the uncertainty surrounding GDPR fines and penalties from a business risk standpoint, the predicted response of insurers in the US and Canada regarding cyber policies is generally positive. Several leading insurers for US and Canadian companies are adding this coverage for no additional premium. The question of insurability also shows considerable progression in both markets over the past 12 to 18 months, with an increasing number anticipating that they will pay claims for GDPR fines and penalties.

Marsh's GDPR Assessment and Coverage Solutions

Marsh worked for several years preceding the implementation of GDPR — with considerable success in many markets — to draft wording around the world to help our clients secure optimal coverage for all costs related to GDPR, including for fines and penalties where permitted by law. As part of our commitment to meeting client needs, we have in many markets developed proprietary GDPR coverage forms, which in our view offer broader, more responsive coverage for GDPR-related risks and losses than off-the-shelf or carrier wordings.

Our proprietary assessment and coverage solutions encompass the broad scope of risks related to GDPR data breach, both within the EU and beyond, as well as the financial consequences of cyber events that trigger GDPR issues. These best-in-class tools and forms can integrate seamlessly and efficiently into clients' overall cyber risk management programs, providing solutions to mitigate the severity of potential losses and complement the role of other cybersecurity or risk transfer products that address cyber-attack frequency.

ASIA

In Asia, several carriers are offering policies with coverage for insurable GDPR fines and penalties. Marsh has received advice from counsel foreseeing no prohibitions to insurability of GDPR fines and penalties across most major Asian markets. Insurers offering such coverage have signaled that they anticipate paying related claims if legally permissible. Insureds should, of course, seek specific legal advice on insurability of GDPR fines and penalties within the relevant jurisdiction in Asia.

AUSTRALIA

Similarly to the UK, insurance policies for Australia-domiciled companies typically are structured to provide privacy breach coverage for many aspects of GDPR, including fines and penalties to the extent they are insurable under Australian law. The general consensus among insurers in Australia is that GDPR fines and penalties will be insurable for Australia-domiciled organizations; however, it is important to note that cover continues to specify "to the extent insurable at law." It is currently untested in Australia whether public policy considerations may render any GDPR fines or penalties uninsurable.

BERMUDA

Apart from the insurance markets noted above, alternatives may be available. For example, Bermuda markets have long been a resource for punitive wrap coverage for fines and penalties that otherwise might not be insurable in traditional markets. For example, one Bermuda insurer will soon provide a "layer wrap" product for GDPR fines and penalties, and several others are finalizing policy wordings for "layer wrap" or difference in conditions "tower wrap" coverages. Depending on the primary insurer leading the program, however, these coverages may not be necessary for US companies in certain circumstances.

LATIN AMERICA

Various regulators in Latin America have been silent regarding GDPR fines and penalties. However, several insurers have indicated to Marsh their intent to provide coverage so long as the insurability does not contravene local laws or regulatory directives. In Mexico, Panama, and Peru, although coverage for regulatory fines or penalties for data privacy violations is not prohibited by local law, that coverage is not currently being offered by local insurers.

In Brazil, although the regulator (Superintendência de Seguros Privados) has been silent regarding GDPR fines and penalties, it changed local regulation to allow insurance of fines levied by regulators and agencies. As with some other regional markets, the issue will be determined by local courts. In Argentina, fines and penalties for regulatory violations are not insurable.

In Colombia, sanctions imposed by supervisory entities, including the local regulator for data privacy violations, are not insurable. In Venezuela, there is no regulatory prohibition for this type of coverage, but as it is a new insurance product it would need to be approved by the local regulator (Superintendencia de la Actividad Aseguradora).

In conclusion, the insurability of GDPR fines and penalties in Latin American markets should be treated on a case-by-case basis with local insurers and regulators, as is the case in all worldwide markets.

Conclusion

The GDPR is a significant addition to global data protection and privacy regulations, with a potentially high cost for organizations found not to comply. The potential size of fines and penalties has raised concern at many companies, and led to questions regarding the applicability of insurance toward future claims. Marsh's view is that, while the answer will vary depending on factors such as policy wording and applicable law, coverage is available in certain markets and under certain circumstances..

In this environment — particularly in the US and Canadian markets, which represent approximately 90% of global cyber premium — many insureds expect that their policies will pay for a wide range of related claims, including GDPR fines and penalties. Based on Marsh's discussions, a number of major US and Canadian carriers have indicated they anticipate paying claims.

The relationship of financial and professional products to the GDPR is new and as yet untested, with many grey areas and issues that will take time to develop in the courts and within the insurance marketplace. It's important that any discussion of insurability begin with the insurance contract as the foundation for coverage and recovery outcomes. Insurability will vary for a number of reasons related to such areas as local laws, regulators, and policy wording.

It's also important to remember that fines are not the only financial exposure organizations face. In the event of non-compliance with the GDPR that leads to regulatory action by the appropriate supervisory authority, there will likely be a price for such things as forensics, breach notification, breach support services, legal liability to pay damages to impacted data subjects, and defending legal and/or regulatory actions. Thus, it's critical to check your policy limits to see that they are sufficient to cover the potential financial exposure — it is possible that limits could be eroded before a fine is even levied.

Finally, don't assume fines and other costs will or won't be covered. Work with your advisors to understand and, where possible and advantageous, try to add policy wording that gives your organization the best chance at recovery should it face an issue under the GDPR.

Key Takeaways

With the GDPR's sweeping privacy and data protection regulations now in effect, many organizations are asking: "Will our insurance policy respond if we face an administrative fine or penalty?"

Marsh's view is that the answer is not black or white in most markets — the insurability of GDPR fines and penalties will depend on several factors, including:

The specifics of a given insurance contract.

The nature of the fine or penalty, whether civil or criminal, and potentially how egregious the instance of non-compliance.

Decisions by courts in relevant jurisdictions once the issue enters the legal system.

Domicile of the insured organization. In the US, domicile may influence the ability to recoup fines and penalties.

ASIA

NAUREEN RASUL
Cyber Practice Leader
naureen.z.rasul@marsh.com
+852 2301 7206

BERMUDA

CARTER FRITH
Senior Vice President
Bowring Marsh (Bermuda) Ltd.
carter.frith@marsh.com
+1 441 299 8896

CANADA

CATHERINE EVANS
Cyber Practice Leader
catherine.evans@marsh.com
+1 416 868 7353

CONTINENTAL EUROPE

JEAN BAYON DE LA TOUR
Cyber Development Leader
jean.bayondelatour@marsh.com
+33 1 41 34 50 05

LATIN AMERICA AND THE CARIBBEAN

EDGAR TAUTA
Business Continuity Management &
Cyber Practices Leader
edgar.tauta@marsh.com
+57 3132894287

MIDDLE EAST AND NORTH AFRICA

SIMON BELL
Financial and Professional Lines
Practice Leader
simon.bell@marsh.com
+971 4 520 3846

PACIFIC

KELLY BUTLER
Cyber Practice Leader
Kelly.butler@marsh.com
+61 429 084 858

SOUTH AFRICA

JUSTIN KEEVY
Divisional Executive
justin.keevy@marsh.com
+27 11 060 7377

UNITED KINGDOM

DAVID ARNOLD
Senior Vice President
david.arnold@marsh.com
+44 (0)207 357 1759

UNITED STATES

JEFFREY BATT
Client Advisor, Cyber Center of Excellence
jeffrey.batt@marsh.com
+1 202 263 7880

THOMAS REAGAN
Cyber Practice Leader
thomas.reagan@marsh.com
+1 212 345 9452