SAXE DOERNBERGER & VITA, P.C.

SDV INSIGHT
Aug. 29, 2019

Mitigating Franchisor Exposures for Systemwide GDPR Compliance through Cyber Insurance

The European Union's ("EU") General Data Protection Regulation ("GDPR") has been in effect for just over a year, and the full extent of the data privacy law's global impact is just now being fully realized.[1] The GDPR is a privacy law enacted under the guiding principle of privacy as a fundamental right, and as such, aims to protect all personal data of any identifiable natural person.[2]

Recent enforcement efforts highlight aspects of the GDPR that should be of particular concern to franchisors, most notably, the extra-territorial scope of the law, as it applies to all companies including U.S. based franchisors, that process, collect, organize, store and use the personal data of subjects residing in the EU[3], and associated fines that can total the greater of €20 Million or 4% of a firm's annual global revenue.[4] The consequences of GDPR non-compliance are not limited to monetary penalties, but can also include legal fees, costs associated with regulatory investigations and remediation orders, and costs to notify and compensate data breach subjects. Companies may even experience operational impacts such as a loss of revenue and market share, due to reputational harm resulting from GDPR non-compliance.

- **Marriott Data Breach & GDPR Fine**

In a highly publicized notice issued July 9, 2019, the U.K.'s Information Commissioner's Office ("ICO") announced its intent to fine Marriott International, Inc. ("Marriott") £99,200,396 ($123,705,870) in connection with a data breach the hotel chain revealed in November 2018.[5] Hackers accessed the Starwood guest reservation database in a massive cyberattack believed to date back to 2014. Marriott initially claimed that hackers stole the details of roughly 500 million hotel guests, which the hotel chain later reduced to 383 million upon further investigation. Marriott further reported that over 18.5 million encrypted and 5.25 million unencrypted passport numbers were stolen, and that 9.1 million encrypted payment card numbers and 385,000 unencrypted card numbers that were still valid at the time of the breach had also been stolen. Of those affected, roughly 30 million were residents of 31 countries in the EEA, 7 million of which were specifically UK residents.[6]

---

[1] The GDPR applies to all countries within the European Economic Area ("EEA"), which includes the EU, Iceland, Lichtenstein and Norway (hereinafter, referred to as the "EU").

[2] 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, art. 1, 2016 O.J. (L 119) (EU), https://publications.europa.eu/en/publication-detail/ /publication/3e485e15-11bd-11e6-ba9a-01aa75ed71a1/language-en; Decision of the EEA Joint Committee amending Annex XI (Electronic communication, audiovisual services and information society) and Protocol 37 (containing the list provided for in Article 101) to the EEA Agreement, 2018 O.J., (L 183/23) (EEA), https://www.efta.int/sites/default/files/documents/legal-texts/eea/other-legal-documents/adopted-jointcommittee-decisions/2018%20-%20English/154-2018.pdf.

[3] GDPR, supra Note 1, art. 3(1),(2).

[4] Id. art. 4(2).

[5] U.K. Info. Comm'r's Off., Intention to fine Marriott International, Inc more than £99 million under GDPR for data breach (July 9, 2019), https://ico.org.uk/about-the-ico/news-and events/news-andblogs/2019/07/statement-intention-to-fine-marriott-international-inc-more-than 99-million-under-gdprfor-data-breach;

Notably, the breach is believed to have occurred to Starwood's reservation system as early as 2014, however, Marriott only later took control of the system when it merged with Starwood in September 2016. Marriott's due diligence (or lack thereof) in the merger process was, consequently, heavily scrutinized – particularly since Starwood announced an earlier breach involving more than 50 properties in November 2015, around the same time it agreed to be acquired by Marriott.[7] The action against Marriott illustrates the GDPR's broad enforcement and applicability to companies with similar operations, including franchise systems that process the personal data of individuals within the EU.

Franchisors with operations within the EU face further GDPR-related exposure given the high volume and scope of information typically collected and stored by franchise systems, including personal data of franchise owners and employees, third-party vendors and affiliates, and current and prospective customers. The inherent nature of the franchise model, with each location being independently owned and operated, is itself a source of significant exposure as each location is a potential access point for a data breach or privacy incident. Given the broad enforcement and potential magnitude of GDPR-related liabilities, it is important that franchisors, and indeed all companies that process the personal data of individuals within the EU, have insurance in place that covers such liabilities as part of an effective risk mitigation and management strategy. The general scope of coverage and associated risks that are typically excluded under a standard cyber insurance policy are further addressed below.

- **GDPR Liability - Does My Cyber Insurance Cover That?**

Standard cyber policy forms offered in US markets typically provide some form of coverage for GDPR-related liabilities, including costs for support services such as forensic and investigatory measures and data breach or privacy event notification services. Standard cyber policies are also likely to provide coverage for defense costs related to a regulatory action commenced by an EU Member State Data Protection Authority, such as the ICO. Notably, the insurability of GDPR-related fines and penalties varies based on several factors and are often excluded under a standard cyber form. There are significant limitations associated with each of these forms of coverage. Policyholders must consider the effect of conditional language within the relevant insuring agreements and applicable sub-limits when reviewing and placing cyber insurance coverage.

Cyber Coverage Generally

Global Risks

US based companies that are subject to the GDPR must ensure that their cyber insurance policies cover risks globally, as opposed to being restricted to the US or a company's US-based operations.

Insurability of GDPR Fines & Penalties

Most cyber insurance policies restrict coverage to fines or costs that are "insurable by law", or state that coverage shall be determined by the "laws of any applicable jurisdiction that most favors coverage for such monetary fines or penalties." These provisions typically apply to restrict coverage in accordance with a vast majority of state's laws, which provide that punitive damages are not insurable.

---

[6] Id.

[7] U.K. Info. Comm'r's Off., Intention to fine Marriott International, Inc more than £99 million under GDPR for data breach (July 9, 2019), https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/statement-intention-to-fine-marriott-international-inc-more-than-99-million-under-gdpr-for-data-breach.

Choice of law provisions identifying a specific jurisdiction's laws as being applicable to the interpretation and enforcement of an insurance policy are also common. However, legal rules governing insurability are often derived from public policy principles, which can override a choice of law stated within a cyber policy. Cyber insurers may deny coverage based on such public policy determinations where the GDPR fine or penalty is clearly uninsurable in the relevant EU member state. Notably, there have been approximately twenty European countries that have taken the position that GDPR fines are not insurable, while another ten countries currently allow insurability or are otherwise undecided on the issue.[8] Because it remains unclear whether GDPR-related fines and penalties are insurable. Policyholders should seek to have such "insurable by law" language removed or revised to provide that the issue of insurability is to be determined under the laws of a particular jurisdiction within the US that is favorable to coverage.

► First-Party Coverages

Breach Response Services

Most standard cyber policy forms provide first-party coverage, which typically reimburses insureds for costs incurred in connection with a data breach, further includes investigation costs and costs to provide notification to those impacted by a breach.

Franchisors must pay close attention to the trigger language included within its cyber policy, as notification of a data privacy event under the GDPR is often required upon the mere suspicion of a breach or privacy event. Policyholders must confirm and/or request that the policy include language that triggers coverage for notifications where a data breach or privacy event is "actual or suspected" or "has actually occurred or is reasonably believed to have occurred," to ensure that they are covered to the full extent of its GDPR-notification obligations.

► Third-Party Coverages

Breach Coverage

Coverage for the daunting fines levied under the GDPR against companies such as Marriott and British Airways[9] for GDPR non-compliance, would likely be found under the third-party coverages of a cyber insurance policy. There are several cyber policy forms that purportedly provide coverage to franchisors and other companies based outside of the EU for governmental fines and penalties levied under the GDPR.[10]

Spam Coverage.

Standard cyber policy forms typically exclude coverage for "unlawful collection of data" or "unlawful communication", including specifically, violations of the Telephone Consumer Protection Act ("TCPA") arising out of text spamming and other similar targeted marketing activities. This is problematic for policyholders, because one of the more prominent areas of exposure under the GDPR is for spam related activities. Enforcement actions over the past year illustrate the types of violations that are the focus of consumers and data protection authorities and include as a point of emphasis the lawful basis for data processing and obtaining of proper consent.[11]

---

[8] Paran et al., Updated guide on the insurability of GDPR fines across Europe, DLA PIPER (July 11, 2019), https://www.dlapiper.com/en/uk/insights/publications/2019/07/updated-guide-on-the-insurability-of-gdpr-fines-across-europe/.

[9] U.K. Info. Comm'r's Off., Intention to fine British Airways £183.39m under GDPR for data breach (July 8, 2019), https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/ico-announces-intention-to-fine-british-airways.

[10] CP1100 (10/2016), at 1.

[11] Eur. Data Prot. Bd., 1 Year GDPR—Taking Stock (May 22, 2019), https://edpb.europa.eu/news/news/2019/1-year-gdpr-taking-stock_en; Eur. Data Prot. Supervisor,

Mishandling of Data/ Wrongful Collection

Franchisors must also consider whether their cyber policy forms cover certain exposures, for which insurers may not expressly provide coverage. For example, businesses can face GDPR fines for mishandling data, even when a data breach does not occur. A policy that covers fines/penalties may still not respond if the cause of liability was not a breach. It is essential that policyholders confirm that coverage will be triggered upon the occurrence or suspected occurrence of a "privacy violation" or "privacy event," which is otherwise broadly defined to expressly include any violation of the GDPR.

Claims for Compensation – Emotional Distress

The GDPR grants data subjects who have suffered "material or non-material damage" as a result of a GDPR breach to claim compensation against data controllers and processors. The inclusion of "non-material" damage provides individuals the right to claim compensation for emotional distress even where they are not able to prove financial loss. Data subjects have the further right to place a demand upon a consumer protection body to exercise rights and bring claims on their behalf. Many commentators view this right as being akin to a class action right and anticipate an increase in group privacy claims against organizations as a result.[12] It remains unsettled whether consumer protection bodies operating in such capacity on behalf of data subjects, and the resulting damages/ compensation/fines arising therefrom, will qualify as a governmental agency for purposes of coverage in connection with a "Regulatory Action" under standard cyber policy terms. Policyholders should be aware of this and other potential gaps in coverage that are likely to emerge as GDPR enforcement efforts and the cyber insurance intended to cover associated liabilities continues to evolve and mature.

- **Conclusion**

As data breaches and privacy events become seemingly inevitable, it is important that companies understand the scope and limits of their insurance programs to determine whether, and to what extent, they are covered for GDPR-related exposures. Policyholders should consult with their insurance broker and coverage counsel regarding cyber insurance to address any potential gaps in coverage for GDPR-related exposures.

For more information, please contact Richard W. Brown at 203.287.2115 or rwb@sdvlaw.com.
Co-authored by Summer Associate Jasjeet Sahani.

[12] See supra Note 8.