Aon Risk Solutions
Financial Services Group

Client Alert: Cyber Risk is D&O Risk – European Union General Data Protection Regulation

On May 25, 2018, the European Union General Data Protection Regulation ("GDPR") took effect in European Union ("EU") member states. The GDPR has already had significant impact on companies that serve EU residents. Further, the GDPR is expected to significantly increase exposure to directors and officers of those companies operating in the EU. This Client Alert will examine the background and requirements of the GDPR, as well as the potential directors' and officers' liability ("D&O") implications.

GDPR Overview

What is the GDPR?

The GDPR impacts organizations around the world that handle the personal information of individuals residing in the European Union, regardless of where the organization is physically located or domiciled. As the regulation imposes significant obligations and possible fines for non-compliance, it creates new challenges for global organizations.

What is applicable under the GDPR?

The GDPR applies globally to organizations that process the personal data of individuals in the EU in the context of offering goods or services or monitoring behavior, regardless of where the actual processing takes place. It applies to information which directly or indirectly identifies an individual, including but not limited to customer lists, contact details, genetic/biometric data, and online identifiers like internet protocol addresses.

What are some of the requirements of the GDPR?

The GDPR contains several requirements for businesses, including:

- Only collect personal data needed to fulfil specific, documented purposes, and where there is a permitted basis under the GDPR for the collection.
- Embed privacy controls into operations and implement mandatory privacy-risk impact assessments for any new project likely to result in a high risk to individuals' privacy.
- Appointment of a Data Protection Officer with expert knowledge for public authorities, organizations processing large amounts of special categories of data, or whose core activities involve the regular and systematic monitoring of individuals.
- 72-hour notification requirement for all personal data breaches to the relevant supervisory authority, except those which are unlikely to pose a risk to individuals. In the case of serious incidents, there will also be a duty to notify the affected individuals of the breach.

What are the enforcement measures? Are there associated fines?

In case of non-compliance with the GDPR, the regulator may impose fines up to EUR 20 million or, if higher, 4% of an organization's annual global turnover. The GDPR also allows the regulator to enforce compliance regardless of whether a breach of network security or privacy occurred. EU citizens have a private right of action under the GDPR.

We're here to empower results

If you have questions about your specific coverage or want more information, please contact your Aon broker.

www.aon.com

Empower Results®

Potential D&O Implications of the GDPR

There are several apparent D&O implications of the GDPR, including:

- **Direct Financial Impact:** Most obvious, the potential for a 4% fine of global revenue, as outlined by the GDPR, could have serious consequences. Particularly for companies and industries that operate in a highly-levered / low-margin environment, the four percent fine could have catastrophic financial implications, including potential non-compliance with loan covenants. Further, the four percent fine may be in addition to the costs of investigation, remediation, and business interruption, depending upon the nature of the cybersecurity breach. At the risk of stating the obvious, financial distress is a common source of D&O related claims.
- **Indirect Financial Impact:** Much like Sarbanes-Oxley, the GDPR is likely to have a difficult-to-quantify cost of additional compliance infrastructure. This can include heightened vendor scrutiny, and may preclude companies from working with some vendors. The increased compliance costs and potential frictional costs of vendor management are examples of potential indirect costs associated with the GDPR.
- **Reputational Loss:** Perhaps less obvious, is the potential for reputational damage resulting from violating the GDPR's privacy standards. While reputational damage resulting from a cyber-security breach is not unique to the GDPR-subject companies, the GDPR's strict requirements are likely to increase the potential for privacy violations (either, via a cybersecurity breach, or via simply non-compliance with the GDPR-mandated rights of consumers to control their private information). While difficult to quantify, reputational damage can, at a minimum, result in management distraction and can certainly lead to damaging loss of trust with customers, which ultimately impacts the top line.

Conclusion

While nascent in implementation, new GDPR requirements are likely to drive D&O liability. The regulation itself has direct potential to do so, as does follow-on civil litigation, as investors and others seek to hold companies liable for failing to fulfill the GDPR privacy requirements, and subjecting the company to penalties and reputational and financial damage.

Coverage for GDPR-related fines & penalties, specific to management liability, is available. For example, Aon's Cybersecurity Officer coverage, available as an endorsement to certain Bermuda lead Side A DIC policies, includes affirmative language with respect to the GDPR should the regulation be used to impose personal liability on data protection officers.