2018 CLM Cyber Summit
October 12 from 3:20 to 4:20 pm, New York, NY

Title: **GDPR, 5 Months after Implementation: How Issues like Enforcement, Compliance, and Insurability are Playing Out**

I. GDPR - From May 2018 Launch through Present: Original Intent and Subsequent Developments

The Scope of GDPR

The General Data Protection Regulation (GDPR) requires organizations that operate in the European Union (EU), or which collect or process data on EU residents to manage and protect personal data. The purpose of GDPR is to strengthen the privacy rights of individuals within the EU, providing them with the right to information, information rectification, erasure of erroneous data, and data portability. It's important to recognize that GDPR is "extra-territorial" in nature; it applies to organizations based both within and outside the EU, so long as collect or process data on EU residents. A key feature of GDPR is the need to obtain explicit "opt-in" consent from EU residents with respect to certain sensitive data. Public bodies and certain other entities processing large quantities or special categories of data must appoint a Data Protection Officer. Organizations are required to data breaches in less than 72 hours unless the breach is "unlikely to result in a risk to the rights and freedoms of natural persons." Furthermore, individuals have a right to access the data an organization collects and processes about them, and to request erasure of such data unless there is good cause for the organization refusing such a request. Organizations are required to demonstrate and verify compliance with GDPR.

Why did the European Union Believe that GDPR was Necessary?

The previous regulatory framework was the EU Data Protection Directive 95/46. It was passed in 1995. To put matters in perspective that was the year Amazon was launched, but still predates Facebook and Google. There has been a dramatic increase in data collection and sharing since then as a result of technological advancements. Both public and private entities are now able to make use of such data on an unprecedented scale. The impetus for the European Commission's proposals to update and modernize the Directive was thus twofold: first, to empower individuals by guaranteeing the right to the protection of personal data that is embodied in the Charter of Fundamental Rights of the European Union, and second, to help build trust in an online environment, which plays a central role in the wider plans to create a Digital Single Market throughout Europe.

Requirements of GDPR

GDPR requires that organizations protect data as well as the privacy rights of individuals. GDPR also requires certain breach notification procedures, and imposes two tiers of penalties on entities that are found to have violated its requirements. Under Article 83 of the GDPR, "General Conditions for

Imposing Administrative Fines," the GDPR will impose a maximum penalty of 2% of global revenue, or 10 million Euros (whichever is greater) for process-related compliance failures, while the more severe threshold of 4% of 20 million Euros (again, whichever is greater) will apply to violations of the regulation's core tenets.

Enforcement of GDPR

Enforcement authority rests with the individual EU member states (*here we will insert examples of enforcement actions taken since May of 2018*)

II. Cyber policy coverage and response – May 2018 through present

Coverage – as of May 2018 and market evolution

To a certain extent, standard "off the shelf" policies provide limited coverage for events arising under GDPR: these include the first party costs associated with responding to a breach, such as forensics and personal notifications, or the legal fees resulting from a regulatory action commenced by an EU Member State Data Protection Authority.

However, there are other types of developments, such as loss of data, failure to designate a Privacy Officer, or failure to file required reports, which could also give rise to a regulatory proceeding under GDPR. These "status offenses" are not necessarily predicated upon there being a breach incident, and such a standard Cyber policy might not be worded in such a way as to respond. It's analogous to a police officer writing a motorist a ticket for an expired registration or a busted taillight, which is grounds for enforcement even though these violations may not have actually led to an accident. As a result, some insurers are offering enhancements, either within their base form or by endorsement, which expressly contemplates coverage for such events, regardless of whether an actual breach has occurred.

Also consider the availability of coverage for reputational harm resulting from a GDPR-related regulatory investigation. Such policies can pick up the costs incurred in connection with engaging a public relations firm or other external expenses. Some insurers even offer coverage for reputation-based income loss as a result of the adverse publicity stemming from an event, although this form of coverage often comes with a higher retention, or is sub-limited in terms of the amount the insurer is prepared to pay.

An insured may wish to consider whether coverage under other policies (public liability, employers' liability, professional indemnity, and legal expenses) may cover some portion of these expenses as well. (*Here, we will insert content describing how the coverage has evolved since May 2018, as well as examples of claims and non-compliance events which have been reported since the enactment of GDPR*).

Ethical Considerations

From an ethical standpoint, an insurance broker or agent should be careful not to make representations to an Insured about the scope of their coverage which is factually incorrect. For example, an insurance broker should not represent to his or her client that the worldwide territory provision of their Cyber insurance policy means that coverage is in place for claims arising under GDPR. As noted above, the answer is more nuanced than that because compliance issues could give rise to a regulatory proceeding independent of a breach event, which historically is what would trigger coverage under a Cyber policy. Additionally, it would be imprudent for an insurance broker to advise a prospective client how their coverage might respond to a hypothetical claim scenario under GDPR without first having reviewed the policy to understand the triggers for regulatory proceeding coverage.

III. Insurability of Fines and Penalties – Significant market variance

An Unsettled Area of Law

Apart from the legal fees associated with responding to a regulatory proceeding brought by an EU member state Data Protection Authority, the insurability of fines and penalties imposed under GDPR remains somewhat unsettled. Notably, even if a category of loss is "covered" under a global policy issued in the U.S., having those funds repatriated locally to cover the cost of a fine or penalty may present tax or regulatory challenges. There are 29 member states, and they local law and custom may dictate how such fines and penalties are viewed from a coverage standpoint.

Factors in Determining Insurability

The first place to look in terms of the insurability of such fines and penalties is the controlling language of the insurance contract. Some other factors to consider include whether there has been a stipulation by the regulatory body as to the insurability of such fines and penalties, whether the penalty is the result of civil or criminal conduct, whether there is a finding of deliberate malfeasance as opposed to negligence, the legal forum in which the member state has brought the action, and the domicile of the Insured.