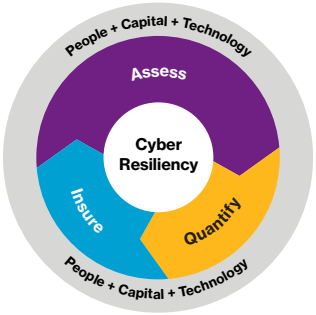


Decode privacy.

Ready or not, GDPR is here. Will you navigate your way to success?

By Gamelah Palagonia, FIP, CIPM, CIPT, CIPP/E, CIPP/US, CIPP/G, ARM, RPLU+

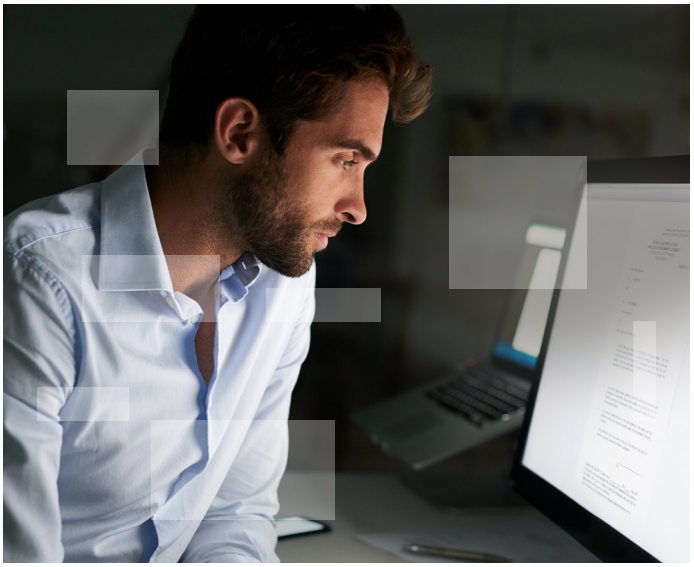
The General Data Protection Regulation (GDPR), which went into effect on May 25, regulates the processing by an individual, a company or an organization of personal data relating to individuals in the European Union (EU). Processing is a key term and it is defined broadly as any operation or set of operations which is performed on personal data or on sets of personal data, either manually or by automated means. This includes collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

The 28 member states which make up the EU had until May 25, 2018 to implement GDPR into their national law. In instances where a local member state's law has a higher standard than GDPR, local law applies.

There have been many recent articles and blogs about the potential for the high GDPR fines and penalties and the insurability of those fines and penalties. However, this is only one risk management consideration associated with GDPR.

The new liability paradigm

The U.S. has had its share of hacker attacks and mega data breaches that resulted in costly first-party losses covered under cyber liability insurance policies. However, third-party claims brought by alleged data breach victims have yet to develop, primarily due to courts' findings that these plaintiffs lack Article III standing and/or failed to show that they suffered harm. The GDPR represents a new liability paradigm; Article 82 (1) makes it clear that any person who has suffered material or nonmaterial damage as a result of a GDPR



infringement has the right to receive compensation from the controller or processor for the damage suffered. In addition to potential civil suits and class actions, alleged victims have several potential avenues to seek recourse.

Contractual liabilities

Businesses could be exposed to contractual liability. Under the GDPR, standard contractual clauses, approved by the European Commission (EC), and strictly binding when signed, do not require prior authorization of supervisory authorities and such clauses may be adopted by the EC as well as by national supervisory authorities. Ad hoc contractual clauses may also be used for GDPR compliance, although they must receive prior supervisory authority approval and are potentially an additional burden for controllers.

Binding corporate rules

Binding Corporate Rules (BCRs) are a significant development in the area of international data transfers under GDPR. BCRs are a compliance mechanism available to controllers and processors to legitimize transfers within corporate groups. Similar to rules of conduct, BCRs are an internal set of rules for data transfers within multinational companies and allow multinational companies to transfer personal data internationally within the same corporate group to countries that do not provide an adequate level of protection.

EU-U.S. Privacy Shield

The EU-U.S. Privacy Shield, effective since August 1, 2016, provides companies on both sides of the Atlantic a mechanism for complying with the EU's data transfer requirements when transferring personal data from the EU to the United States. To participate, a company must self-certify to the U.S. Department of Commerce that it complies with the Privacy Shield Principles and related requirements. The Department of Commerce maintains a site where it lists the companies that have current self-certifications.

The Federal Trade Commission (FTC) enforces the Privacy Shield and pursues organizations that have made false claims of participation. To date, there have been three such false claim actions. No fines were levied in these cases, but each organization is subject to 20 years of FTC scrutiny and are required to submit compliance reports until 2037.

When the FTC issues a consent order on a final basis, it carries the force of law with respect to future actions. Each violation of such an order may result in a civil penalty of up to $40,654. Additionally, FTC consent order submissions (compliance reports) must be truthful and accurate, subject to the penalty of perjury under the laws of the United States.

Fines and penalties

There are two tiers of fines, the lower tier applicable to violations of controller/processor responsibilities, and the higher tier, applicable to violations of data subjects' rights and the failure to comply with National Data Protection Authorities' (DPA) investigatory and corrective powers.

All fines have to be "effective, proportionate and dissuasive" and they can be imposed in conjunction with the exercise of the DPAs' investigatory and corrective powers, meaning that serious GDPR breaches can be met with multiple responses. Nevertheless, if the controller or processor breaches various requirements of GDPR, the total amount of the fine cannot exceed the amount that is specified for the most serious breach.

While enforcement actions issued by DPAs are relatively rare in most EU member states, with the exception of the U.K.'s Information Commissioner's Office, many believe the enhanced powers granted by GDPR will inspire DPAs into increased action.

Under GDPR's Article 83, before a fine can be imposed, DPAs need to consider a number of different factors, including but not limited to:

- The nature, gravity and duration of the infringement, as well as the number of data subjects affected and the level of damage suffered by them
- The intentional or negligent character of the infringement
- Any action taken to mitigate the damage suffered by the data subjects and the degree of cooperation with the supervisory authority
- Any relevant previous infringements

Cyberinsurance

Cyberinsurance differs from most professional liability insurance products as it was created to respond to, among other exposures, data breaches on a first-party basis, defend regulatory actions and fines and penalties. This is a specialized area of insurance that not only requires professional liability expertise but also a deep understanding of constantly evolving cyber and privacy exposures. A thorough understanding of U.S. federal and state privacy laws, sector-based regulations and now global privacy regulations, are also necessary.

Depending on the insurer, a well-drafted or endorsed cyber liability insurance policy would typically cover GDPR liabilities, including fines and penalties, where insurable. Current market conditions for cyberinsurance are relatively soft and, as such, insurers are more flexible on terms and conditions and on premium.

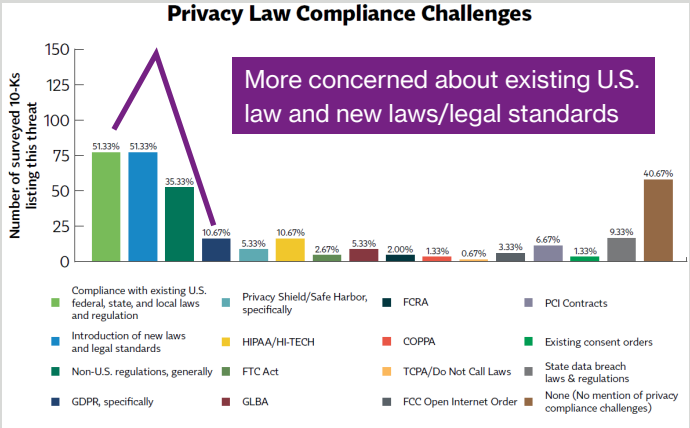
It is important to note that GDPR violations may not stem from a data breach or security incident, which generally is the coverage trigger in most cyber policies. For example, Article 30 requires controllers and processors to maintain extremely comprehensive "records of processing." The failure to comply with Article 30 may trigger a regulatory proceeding and result in fines up to 10 million euros or 2% of the fined entity's annual worldwide revenues. Therefore, if the insurance policy at issue doesn't contain a broad definition of Privacy Wrongful Act inclusive of the failure to reasonably implement privacy or security practices as required by law; or the failure to comply with the insured company's privacy policy and/or privacy notice, regulatory proceedings and resulting fines may not be covered. This type of coverage will need to be negotiated and may not be available to every organization.

Another critical policy enhancement to consider is whether there is coverage for the unauthorized collection and use of personal data. As the governing GDPR principle is to only collect a data subject's personal data for an authorized purpose with the data subject's explicit, freely given consent, violations of this principle can be met with regulatory actions and fines up to €20 million or 4% of the fined entity's annual worldwide revenues, which would likely not be covered in the absence of such an enhancement.

Finally, the insurability of GDPR fines and penalties will turn on the facts and applicable law in each individual case. Preliminary legal research on this topic has opined that the majority of member states are unlikely to view these fines and penalties as insurable. However, until those member states are presented with such issues, the answer to these questions is not yet definitive. Compliance with GDPR is certainly one way to avoid fines and penalties.

GDPR compliance

The International Association of Privacy Professionals' 2017 10-K Study of the 150 largest publicly-traded companies in the U.S. found that these companies are more concerned about existing and developing U.S. laws than GDPR. Their concerns about GDPR are in line with the Health Insurance Portability and Accountability Act, in effect since 1996. The 2018 study may reflect a different picture as GDPR implementation advances.



Source: The International Association of Privacy Professionals' (IAPP) Privacy Risk Study 2017: PII Remains Top Information Risk. iapp.org.

Small and mid-sized enterprises (SME) are understandably more challenged. Studies indicate that approximately 25% of SMEs in the U.S. are compliant and many are unaware that they are in GDPR's scope. This will change as GDPR requirements are enforced and SMEs must demonstrate accountability.

A journey, not a destination

No doubt, GDPR is forcing a fundamental culture change and those businesses, large and small, that embrace it will benefit the most. GDPR lays the foundation for trust and transparency, which correlates in increased consumer satisfaction – a competitive advantage that directly impacts the bottom line.

U.S. businesses are accustomed to regulation and may inherently be more prepared to comply with GDPR than their European counterparts. Recognizing that GDPR compliance is a journey and not a destination is vital to the success of a compliance program.

Contact

Gamelah Palagonia, FIP, CIPM, CIPT, CIPP/E, CIPP/US, CIPP/G, ARM, RPLU+
+1 212 915 8575
gamelah.palagonia@willistowerswatson.com

About Willis Towers Watson

Willis Towers Watson (NASDAQ: WLTW) is a leading global advisory, broking and solutions company that helps clients around the world turn risk into a path for growth. With roots dating to 1828, Willis Towers Watson has over 40,000 employees serving more than 140 countries. We design and deliver solutions that manage risk, optimize benefits, cultivate talent, and expand the power of capital to protect and strengthen institutions and individuals. Our unique perspective allows us to see the critical intersections between talent, assets and ideas – the dynamic formula that drives business performance. Together, we unlock potential. Learn more at willistowerswatson.com.

willistowerswatson.com/social-media

WTW-NA-2018-WTW76711

willistowerswatson.com

Willis Towers Watson