ZwillGen blog
Law Across the Wire and into the Cloud
Recent Developments in Internet Law

ONE MONTH TILL GDPR! SEVEN INSIGHTS AND PREDICTIONS

Published On April 25, 2018 | By Melissa Maalouf, Mason Weisz, Jon Frankel, Ken Dreifach, Kandi Parsons, Anna Hsia, Alexei Klestoff, Marci Rozen, Allison Bender, Michelle Anderson and Austin Mooney | *International, Practical Advice*

	Insight	Prediction
1 The Big Picture	Many companies have found that GDPR preparations, while burdensome, have had the ancillary benefit of helping them get their "privacy and security house" in order on a broader scale. Employees throughout companies are becoming more fluent in privacy/security issues and are starting to more fully integrate privacy and security into their business at all stages of product development. Despite the stress of the GDPR exercise, many in-house lawyers and privacy and security professionals have appreciated how the GDPR has validated concerns about privacy and security issues and helped them obtain company-wide buy-in.	While GDPR is a significant privacy regulation, it is not the only one, and compliance is not a one-time effort. Some companies may mistakenly equate their compliance with the GDPR as satisfying their obligations under privacy laws worldwide and as a one-time effort. While the steps required to comply with GDPR will be helpful for almost any privacy/security program, many jurisdictions have laws that differ from or are even more stringent than the GDPR (including the United States). Moreover, we expect continued guidance on GDPR compliance to be released over the coming months to clarify ambiguous GDPR provisions, and EU Member States will continue to update their data protection laws. Companies should be prepared to adapt to the inherent fluidity of the law – May 25th is not an end; it's actually only the beginning.
2 Data Protection Officer	Businesses are grappling with whether they are required to appoint a Data Protection Officer ("DPO"), and if so, who is best-suited to fill that role. Should the DPO be internal or external, where should the DPO be located (US v. EU), and what type of expertise should the DPO have (e.g., lawyer, infosec professional, auditor, etc.)?	The demand for DPOs has and will likely far exceed the available supply. The GDPR requirements for appointing a DPO are narrower than most think – for most companies, the GDPR requires a DPO only if their "core activities" involve either (1) regular or systemic monitoring of data subjects on a large scale or (2) large scale processing of sensitive data types. While many companies process some sensitive data and engage in certain monitoring activities (e.g., online tracking and advertising), the GDPR DPO requirement is not triggered unless these are "core" activities. We predict widespread variation in approaches to whether a DPO is needed, who that person should be, and exactly what his/her role should look like, especially with respect to companies mainly operating from the US. We also expect (perhaps long for?) further guidance from EU regulators.
3 Data Subject Rights	A company's policies and procedures for responding to data subject requests ("DSRs") are among the greatest risk factors under the GDPR. A failure to respond appropriately or timely to a DSR could result in regulatory or judicial scrutiny or a class action-like complaint from consumer organizations.	We expect that privacy advocates will make an increased number of DSRs post-May 25 to "test" compliance. Companies that have instituted DSR policies and have carefully considered how to respond will be better positioned to handle requests. Thorough data mapping and privacy-by-design techniques can help ease the burden of these requests. Indeed, going through these processes means these companies have already engaged in some data deletion or anonymization efforts and/or reduced their collection of new data, and can therefore more efficiently locate the remaining data to ensure that DSR responses are adequate and timely.

ZwillGen blog
Law Across the Wire and into the Cloud
Recent Developments in Internet Law

ONE MONTH TILL GDPR! SEVEN INSIGHTS AND PREDICTIONS (cont'd)

Published On April 25, 2018 | By Melissa Maalouf, Mason Weisz, Jon Frankel, Ken Dreifach, Kandi Parsons, Anna Hsia, Alexei Klestoff, Marci Rozen, Allison Bender, Michelle Anderson and Austin Mooney | *International, Practical Advice*

	Insight	Prediction
4 Data Processing Addenda	Review proposed Data Processing Addenda ("DPAs") with care. We've seen a number of customers of our Processor clients use the GDPR Data Processing Agreement negotiations as an opportunity to impose additional contractual obligations that are not legally required.	In the rush to GDPR compliance, companies have been hastily signing DPAs, sometimes with provisions that they cannot easily comply with or that are overly burdensome, particularly with respect to data security and audit rights. For companies paying close attention, this can impact their bottom line as the cost of compliance is increasing, even where they are able to push back in negotiations. For companies that are not paying close enough attention, we expect they may find themselves facing an increased risk of contractual breaches, and loss of business to companies that can comply with more onerous provisions.
5 Controller vs Processor	In some deal negotiations, the parties have trouble agreeing on their respective designations as Controllers or Processors under the GDPR. For example, a customer may insist on incorrectly treating certain vendors as Processors, even though these vendors contractually preserve the right to use personal data for their own purposes, which results in them being a Controller (at least with respect to some processing activities). In many cases, the deals close without accurate resolution of the issue.	While the consequences of failing to resolve these designations during closing may not be immediately apparent, they will create risk, especially when one party acts on a mistaken assumption about how the other party handles data and GDPR compliance. For example, a customer that misclassifies a vendor/Controller as its Processor may mistakenly assume that it doesn't need consent for its own sharing of data with the vendor, and the vendor may mistakenly assume that the customer has obtained consent on behalf of the vendor. Even when they cannot agree on formal designation as Controllers or Processors, all parties generally benefit from ensuring that topics such as transparency, legal basis (e.g., consent), and data subjects' rights are properly addressed. As enforcement begins to highlight these gaps, we expect many parties to revisit their DPAs and their Controller/Processor roles.
6 Data Retention/ Deletion	Anonymization, and in some cases pseudonymization, can significantly reduce GDPR compliance burdens. For example, because pseudonymization reduces the risk of harm to data subjects, controllers may be able to avoid breach notification to individuals regarding data that has been properly segregated and pseudonymized.	Companies will increasingly use anonymization and pseudonymisation techniques to give themselves more flexibility in how they process data, and also to avoid opening their doors to further regulatory review. More vendors will offer anonymization services, perhaps associated with a code of conduct. This will likely be similar to what happened in the US following the HIPAA de-identification rules.
7 Litigation	In addition to enforcement by EU regulators, under the GDPR, data subjects are also guaranteed a "right to an effective judicial remedy," including monetary damages, for violations. This right can be exercised by nonprofit organizations on behalf of consumers, and these nonprofits have deeper pockets to fund plaintiffs' lawyers than individuals would.	While it will likely be a while before the EU has a class action model for data privacy/security claims that mirrors the scale and popularity of such actions in the US, companies that fail to do the basics under GDPR (such as updating their privacy policy, responding appropriately to SARs, getting consent right (if required), and adequately protecting data), likely will be early targets of such litigation or regulatory scrutiny. And, with EU courts considering many of these issues for the first time, the first few years of judicial resolutions are likely to be unpredictable.