Image: NASA / Unsplash.com

Melissa Maalouf Shareholder
melissa@zwillgen.com

Michelle Anderson Attorney
michelle@zwillgen.com

ZwillGen PLLC, Boston and Washington, D.C.

Après 25 May: how has the GDPR most impacted US companies?

After the daily deluge of privacy policy update notification emails this past spring and the dramatic, 11th hour passage of GDPR-inspired legislation in California this summer, it has been almost impossible to avoid hearing about the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR') in the US. But now that May 25 has come and gone, what are US companies actually doing to comply with the GDPR, and how has the GDPR impacted both their day-to-day operations as well as their overall privacy and security programmes and strategies? Melissa Maalouf and Michelle Anderson, Shareholder and Attorney respectively at ZwillGen PLLC, provide their perspective on what US companies are doing, the challenges they're facing, and the ways in which the GDPR has affected the US privacy landscape.

What approaches are US companies taking to GDPR compliance?

Over time, reports have changed as to how prepared US companies were for the GDPR. In fall 2017, one report found that 84% of US companies expected to be GDPR-compliant by its effective date of 25 May 2018[1]. However, by April 2018, another survey indicated that only 13% of US companies considered themselves 'fully compliant,' with an additional 23% reporting being 'mostly compliant[2].'

These reports are consistent with what we've seen with many US companies. Leading up to the GDPR, there was wide-spread panic about the need for comprehensive compliance; however, as US companies began assessing their unique practices and regulatory concerns, most settled on a risk-based approach, commensurate with the nature and geographic scope of their processing activities. Specifically, US companies with significant EU operations have taken the most thorough approach to GDPR compliance, hiring outside consultants and even setting up internal privacy and security compliance teams. In contrast, companies with only US operations and limited contacts in the EU (such as companies with English-language websites that are globally accessible but not targeted to EU individuals), have updated their website privacy notices to incorporate GDPR principles of transparency and choice, but have not taken other significant steps. Others, including those with no EU presence but with a meaningful number of EU customers, have tried to comply with what they believe to be the most significant GDPR requirements for their operations, such as data breach preparedness, implementing data subject request processes, and employee training. Still others with either small numbers of EU customers, limited resources, or both, have taken another approach entirely, to block EU IP addresses from accessing their services.

Key challenges for US companies under the GDPR

US companies that have implemented more comprehensive GDPR programmes have faced a number of new challenges. Three of the biggest hurdles we've seen are:

Maintaining records of privacy compliance:

While many US companies had privacy and security policies in place, along with varied informal or unwritten policies to respect privacy, the GDPR has driven them to put more of their processes into writing and more formally document their data collection and use practices. Certain GDPR articles impose record-keeping requirements for select issues (e.g. Privacy By Design and Data Protection Impact Assessments), but the GDPR's general requirement that companies be able to demonstrate compliance has prompted many to develop more comprehensive records of their privacy and security programmes. Developing and maintaining such documents has been resource-intensive and requires significant cross-functional efforts. And, many US companies have struggled with striking the right balance between 'papering' their practices for GDPR compliance while simultaneously avoiding the creation of an endless trail of discoverable documents that may be misinterpreted or used against them in future litigation or regulatory investigations.

Developing mechanisms to respond to data subject rights requests:

The GDPR enhanced the privacy rights of EU individuals while also creating a labyrinth of fact-specific exceptions to such rights, making the creation of template responses and automated processes for data subject requests challenging for many companies. Compounding that problem, data subjects may not clearly state their requests or accurately state the relevant GDPR right. This is a particular risk for English-speaking companies in the

1. IAPP and TrustArc, Getting to GDPR Compliance: Risk Evaluation and Strategies for Mitigation, Fall 2017).
2. CompTIA, The State of GDPR Preparedness in the US, April 2018.
3. See e.g. Standards for the protection of personal information of residents of the Commonwealth 2009 (201 CMR 17).
4. *FTC v. Sandra L. Rennert* et al., Civ. Action No. CV-S-00-0861-JBR (Dist. Nev. 12 July 2000).
5. FTC, Start with Security: A Guide for Business, June 2012.
6. ePrivacy Directive (2002/58/EC).
7. Transcript of Zuckerberg's appearance before House Committee, The Washington Post, 11 April 2018.

continued

US, for which requests may get lost in translation or be misunderstood, and then result in a complaint to a data protection authority. Many US companies are struggling with whether to apply such data subject rights worldwide or only apply them only to EU users; in the face of requests from US customers asking if a company provides GDPR rights to US citizens, US companies face a difficult choice of balancing customer service with trying to make strategic legal decisions about cross-border privacy compliance.

Managing vendors:
The GDPR Article 28 requirement to ensure that controller-processor relationships are governed by a contract with specified provisions has caused companies to spend significant time and resources negotiating data processing agreements ('DPAs'). In our experience, many companies were unable to implement DPAs with all vendors prior to May 25 and their vendor management efforts are continuing. These efforts include identifying vendors processing EU personal data, developing template DPAs and negotiation playbooks, and in some instances needing to educate vendors as to why Article 28 requirements are non-negotiable. Given that under the GDPR, controllers remain liable for acts of processors, many companies have also been working hard to enhance, or in some instances create for the first time, vendor diligence and third-party risk management processes. This has resulted in a noticeable cultural shift at many companies where, pre-GDPR, different groups had authority to contract with vendors directly, often using standard, online click-through agreements, without much thought or concern. The GDPR has complicated the vendor management process, and companies are being more careful about the vendors with which they will do business.

The silver linings of GDPR compliance

Particularly for small to mid-sized companies, complying with the GDPR, while burdensome, has also had the positive side effect of enhancing their privacy and security programmes. For example, compliance with the GDPR has put many companies in better compliance with US data security laws and in a better position with managing their vendors under such laws. US states have long required that companies protect personal information and mandate that their vendors do the same[3], and the Federal Trade Commission ('FTC') has issued data security enforcement actions for the last two decades[4], repeatedly warning that failure to oversee vendors is an unfair practice subject to FTC enforcement[5]. Despite such precedents, many US companies were previously unaware of their US data security obligations or perhaps did not view them seriously enough. However, in considering the impact of Articles 28 and 32 of the GDPR, and the potentially high fines attached to GDPR violations, many smaller US companies finally had a strong incentive to develop or update their data security programs and, as noted above, evaluate and improve their contractual relationships with vendors.

Similarly, companies that have taken steps toward GDPR compliance have generally re-assessed and improved their marketing and advertising practices. Marketing and advertising laws have been in place in the EU since the early 2000s[6]. Still, the threat of potentially high GDPR fines has compelled US companies to more thoroughly vet their practices against these established laws and revamp their marketing programmes. Notably, many companies have improved transparency in their marketing practices, implemented more consumer-friendly marketing consent flows, and have implemented consistent marketing practices across their companies.

EU and US privacy laws inching closer together

Beyond compliance with the GDPR's technical requirements, perhaps the biggest impact we've seen in the US is that the GDPR has contributed to a shift in expectations regarding what privacy means and what companies must do to protect data. For example, in April 2018, Senators on both sides of the political aisle questioned Mark Zuckerberg about how Facebook was complying with the GDPR and suggested that GDPR-like protections should be extended to Facebook's US users[7]. In late June, the California Governor signed into law the California Consumer Protection Act of 2018 ('CCPA'), which gives California consumers greater control over how businesses use their personal information, including mirroring some GDPR principles, such as the rights to access and deletion. Given increased consumer awareness about privacy issues and the fact that the GDPR has been so widely discussed, it is probably more likely now than ever before that US consumers and lawmakers will continue to push for comprehensive privacy rules.

What that ultimately looks like remains to be seen. Will other states pass laws similar to California? Or will the pressure on US companies from both the GDPR and the CCPA push federal lawmakers to make privacy legislation a priority? Regardless of what comes, companies that have taken steps toward GDPR compliance are already further along in their compliance with US privacy laws, and companies that take steps toward compliance with the CCPA are also taking steps toward GDPR compliance. However, while we anticipate a persistent trend of US and EU privacy laws coming closer together, there will likely continue to be significant differences for some time that will make cross-border compliance programmes challenging. US companies should be mindful of how EU regulators enforce (or don't enforce) the GDPR and the lengths they go to exercise jurisdictional reach.