KILPATRICK TOWNSEND

5 KEY INSIGHTS

How GDPR has Impacted American Companies & the Future of Transatlantic Data Transfers

By Amanda Witt, Partner, Kilpatrick Townsend

The European Union's General Data Protection Regulation ("GDPR") marked a turning point in privacy and data protection practices globally and transformed how American companies approach the protection of personal data. Because of the large potential fines and complexity of the GDPR, American companies devoted significant resources to developing privacy and compliance programs to prepare for the effectiveness of the GDPR in 2018. GDPR has also proven to be an inspiration for comprehensive privacy laws that have been adopted and proposed in the United States.

In the last few years, however, arguably the most important aspect of the GDPR for American companies has been the issue of transatlantic data transfers and whether the EU is slowly moving towards requiring data localization. While updated Standard Contractual Clauses ("SCCs") from the European Commission and guidance from the European Data Protection Board provided guidance on how to accomplish EU-US data transfers following the invalidation of the Privacy Shield by the Court of Justice of the EU ("CJEU)" in Schrems II, recent enforcement decisions issued by European regulators since then have made it increasingly difficult for US and European companies to transfer personal data to the United States – or to understand their obligations going forward.

On October 18, **Amanda Witt**, Co-Lead of the Technology, Privacy and Cybersecurity Team of **Kilpatrick Townsend**, participated in a legal training sponsored by JP Infonet in Stockholm, Sweden. In this presentation, Ms. Witt provided insights on how companies can navigate these difficult issues by providing an explanation of US surveillance laws, recommendations on how to craft supplementary measures and a discussion of risk mitigation strategies. She also discussed the recently proposed EU – US Data Transfer Framework and whether such a mechanism will be a viable alternative to solving the transatlantic data transfer conundrum.

In the presentation sponsored by JP Infonet, Ms. Witt provided five key insights on the following:

1

The GDPR-Induced Evolution of American Privacy Programs: The enactment of GDPR represented a watershed moment for global companies generally. The comprehensive nature of the law and the significant potential fines required complex and time-consuming preparation efforts that included extensive data mapping to understand the full scope of personal data processing, the preparation and negotiation of data processing agreements with processors and other business partners, implementation of data subject access request and data protection impact assessment policies and procedures, improved security measures, updates to privacy notices and the implementation of data transfer mechanisms, among other tasks. Some US companies who previously did not have a dedicated privacy professional or counsel on staff before the enactment of GDPR steadily expanded their privacy teams to have at least one and often more than five or so privacy professionals or attorneys fully dedicated to privacy within the organization. Given the enactment of comprehensive privacy laws in the United States (i.e., California, Virginia, Colorado, Utah and Connecticut) and GDPR-like laws adopted internationally (e.g., Brazil's LGPD), companies continue to invest significantly in the development of their privacy programs. According to the **2021 IAPP-EY Annual Privacy Governance Report** from the International Association of Privacy Professionals, companies with 25,000-74,900 employees on average have 13 full-time privacy professionals on staff and 33 part-time privacy professionals. Companies within that range are typically spending on average USD $873,000 annually on privacy-related compliance activities, which is an increase of $200,000 since 2020. Many companies are planning to hire between one and five additional privacy staff members at the director level or higher.

2

Transatlantic Data Transfer Challenges: Since the invalidation of the Privacy Shield by the CJEU in Schrems II in July 2020, companies have spent over two years grappling with the implications of the decision. Such challenges have only increased since then as further discussed below. To address the Schrems II decision and generally update the prior Standard Contractual Clauses ("SCCs") for GDPR, the European Commission adopted updated SCCs on June 4, 2021. The updated SCCs offered a welcomed, modular approach that more appropriately reflected the various types of data transfers. Companies must update the prior SCCs by December 27, 2022 and, due to Schrems II, companies must also evaluate whether supplementary measures are required and perform complex transfer impact analyses to confirm that personal data can be transferred in a compliant manner with such SCCs. Due to Brexit, the United Kingdom ("UK") has its own form of International Data Transfer Agreement and Addendum and requires the update of prior SCCs by March 21, 2024, as well as its own version of a transfer impact assessment.

3

US National Security Laws: An especially thorny issue addressed in Schrems II by the CJEU was the type and degree of U.S. government access, via national security surveillance activities, to the personal data being transferred from the EU. The CJEU determined that the potential for government access resulted in a failure to afford EU data subjects the privacy rights provided by the GDPR. The CJEU focused on two sources of authority for surveillance: the Foreign Intelligence Surveillance Act (FISA) Section 702 and Executive Order 12333, which the Court viewed as implicating bulk collection of personal data, without adequate oversight or right to individual redress. Unfortunately, the broad definitions of "electronic communications service provider" and "remote computing service" subject many U.S. companies and their subcontractors to FISA and the risk of access by the intelligence community. According to U.S. Department of Justice guidance, U.S. companies providing internal communications platforms (e.g., email to employees) may be subject to FISA 702 as an "electronic communications service provider".

4

GDPR Enforcement Trends: American companies (particularly technology companies) have been the subject of a number of the largest and most notable GDPR-related enforcements in the EU. The largest fine thus far was issued by the Luxembourg supervisory authority against an American online marketplace. A number of other American technology companies have been fined by regulators in France, Ireland and the United Kingdom. Some of the more recent enforcement actions in Austria, France, Italy and Denmark have determined that certain US-based website analytics tools engage in unlawful transfers based on the potential access by US intelligence agencies due to inadequate supplementary measures. If additional European regulators follow these decisions (which they are likely to), the ability of U.S. companies to rely on Standard Contractual Clauses ("SCCs") to transfer personal data from Europe to the United States appears to be fraught with the risk of such transfers being declared unlawful. To complicate matters further, regulators have offered little in the way of practical solutions or alternatives, and the guidance has been relatively uncompromising.

5

The Newly-Proposed Data Transfer Framework – a Possible Solution to Data Transfer Headaches?: Given the current regulatory enforcement trends in Europe, the only workable solution would appear to be changes to how U.S. intelligence agencies collect and process signals intelligence, a prospect that many believed to be a non-starter. Fortunately, a compromise may be on the horizon. Following a joint E.U. – U.S. announcement earlier in 2022 on an agreement in principle for a new data transfer framework to replace the invalidated Privacy Shield and as mentioned earlier this year in a prior alert the White House published its long-awaited **executive order** ("EO") on transatlantic data transfers to replace the invalidated Privacy Shield on October 7, 2022. In addition, the U.S. Department of Justice ("DOJ") followed this announcement by issuing related **regulations** setting forth new redress mechanisms including the creation of a Data Protection Review Court ("DPRC"). The EO is crafted to address many of the criticism raised by the CJEU in Schrems II. The EO requires U.S. intelligence authorities to limit U.S. signals intelligence activities to what is necessary and proportionate. The EO kicks off a ratification process by the European Commission, which is expected to take as long as six months. There are hopes that the new framework will be available for use by March 2023 or shortly thereafter, although the specter of a new challenge to the framework remains a possibility. It should be noted, however, that the EO and DOJ regulations have the force of law as of the date they were issued, so companies can rely on the "necessity" and "proportionality" principles when conducting their transfer impact analyses and can rely on the redress mechanism once the DOJ has determined that the EU is a "qualifying state". As many practitioners in this field know, there is never a dull moment in Transatlantic Data Transfers! Stay tuned for more…

For more information, please contact:
Amanda Witt, awitt@kilpatricktownsend.com
www.kilpatricktownsend.com