FACE-OFF

HARMONISING DATA PROTECTION ACROSS THE ATLANTIC REMAINS CRITICAL

There is no denying that the agreement on data sharing arrangements between the EU and US has a troubled history. There is still much criticism that the deal in place still does not do enough to protect EU citizens from snooping by the US security services. Taking a closer look at how US President Donald Trump's administration will act in relation to both the Privacy Shield agreement and GDPR that are due to come in to force next year.

Jason Straight

BREXIT AND RESURGENT ISOLATIONIST POLICIES NOTWITHSTANDING, WE LIVE AN INCREASINGLY GLOBALISED WORLD – ESPECIALLY WHEN WE ARE TALKING ABOUT OUR DIGITAL ENVIRONMENTS. Cross-border data transfers have accelerated dramatically and show no signs of slowing. The result is that we have less and less control over its use and disposition as we continue to create more and more personal information.

Responding to rising concerns raised over data privacy resulting from the internationalisation of sensitive personal information, governments have been debating on how best to govern the international transfer of personal data. The introduction of both the EU-US Privacy Shield and the EU General Data Protection Directive (GDPR) are the most visible regulatory changes illustrating this trend. It's important to examine these new regulations and explore whether they can work harmoniously together or, as many critics have suggested, are likely to cause more friction and headaches within an already-complicated plethora of rules and regulations governing the international transfer of such data.

Let's begin by looking at the EU-US Privacy Shield and what it entails. Now nearly a year old, the Privacy Shield is a framework for transatlantic exchanges of personal data for commercial purposes between the European Union member countries and the United States. In September, the Privacy Shield will undergo its first annual review, which will be carried out by the European Commission and the US Department of Commerce (DOC).

No doubt a pivotal test for the success of the framework, the review will provide the first opportunity for officials to boost confidence in its durability, which many critics have deemed vulnerable to the same criticisms that doomed its predecessor agreement, Safe Harbor. Whether or not it passes the test, there is no doubt that the Privacy Shield will continue to face significant challenges and generate questions going forward: Is it here to stay? What components of the framework might be changed going forward to ensure that it endures? These are pertinent questions that organisations working in a transatlantic capacity should be addressing.

Now more than ever, it is imperative that organisations take stock of the legal challenges that they may face when transferring personal data. Considerations include: the costs and difficulties of implementing the Privacy Shield within the organisation; the life expectancy of the framework as it stands; and, perhaps more importantly, how likely it is to work in harmony with the General Data Protection Regulation (GDPR) that is to take effect within the EU in May 2018.

What is GDPR? After years of discussion, debate, lobbying and lamentation, GDPR will finally replace the EU's Directive 95/46/EC, which has provided data protection guidance in the EU since 1995 and was well in need of updating, especially considering how far the world has come over the last 20 years in terms of technology and the management of private data.

The ostensible purpose for enacting GDPR is to create regulatory consistency and certainty for companies operating in the EU with respect to their obligations to protect personal information for citizens of EU states. With a fining mechanism that allows penalties as high as 4% of global turnover (i.e., gross revenue), any company that has yet to take a hard look at its obligations under GDPR would be well-advised to do so before it's too late. Moreover, the sheer breadth of the regulation will create compliance headaches for nearly every organisation, large and small.

For foreign organisations undertaking business in the EU, the degree of emphasis placed on protecting personal information can be hard to grasp. But as GDPR explicitly states, protection of personal data is considered a 'fundamental right', in the EU and the regulation further clarifies that 'processing of personal data should be designed to serve mankind'.

Regardless of one's view regarding the sanctity of personal information, the reality is that in order to conduct any business in the EU or sell any goods or service to citizens of any EU state, organisations need to get up to speed to avoid the promised hefty fines.

However, with two distinct data protection frameworks governing the transfer of EU-US data, is it reasonable and actually feasible to expect organisations to comply efficiently and cost-effectively? In the lead-up to the Privacy Shield's review in September, a number of experts and policymakers have lifted their heads above the parapet to urge regulators to adjust the frameworks to enable them to work together more cohesively. Only time will tell whether or not the warnings have been sufficiently heeded.

A number of EU policymakers have expressed concern that the White House isn't backing the existing data transfer mechanism strongly enough. They have argued that amendments are necessary in order to strengthen privacy protections for EU citizens, and that in order to solidify the Privacy Shield, further restrictions on the sharing of personal data transferred out of the EU need to be implemented.

More than 2,100 US companies are participating in the Privacy Shield self-certification process (which is still in place on a voluntary basis today) to transfer data out of the EU more easily. Participating companies are obliged to certify to the DOC that their compliance with EU-approved privacy principles, including the limiting of US government access to data once it has been removed from the EU. This latter provision is a fundamental basis for the EU's approval of the system.

There is no doubt that the upcoming review of the Privacy Shield will provide an opportunity for improving the agreement, though it still remains unclear whether the Trump administration will stand by commitments the Obama administration made to limit government surveillance and acknowledge protections for EU citizens. Many have argued that despite European concerns, the legal mechanisms established by the US for EU citizens to file complaints alleging any US overreach in accessing data transferred to companies under the Privacy Shield appear to have robust support. There also appears to be strong backing for a EU-US law enforcement information-sharing agreement.

Without a crystal ball, it is difficult to forecast exactly how GDPR and the Privacy Shield will work together. What is clear, though, is that the review in September will be a good opportunity for policymakers on both sides of the Atlantic to come together and address some of the challenges and concerns faced by international organisations. Until then, global companies need to take the initiative to assess the risk posed by the new regulatory quilt and take appropriate action. ●

Jason Straight is senior vice president and chief privacy officer at Cyber Risk Solutions at UnitedLex, a legal outsourcing services provider headquartered in Kansas, US. Founded in 2006, the company provides legal services in the fields of litigation, electronic data discovery, document review, contract review and management, intellectual property, immigration and law firm support.