FINANCIER WORLDWIDE corporatefinanceintelligence

Transatlantic compliance: understanding today's picture and best practice next steps

By Jayne Rothman, Epiq Systems
May 2016

A complicated picture just got more complex. The transatlantic transfer of personal data between the European Union and the US is now governed by new data privacy compliance obligations following an October 2015 ruling that invalidated the previous Safe Harbour privacy accord. For businesses, this means a new set of rules to learn and a new set of standards to adhere to.

The background of this latest development can be traced back to 1995 and the establishment of the EU Data Protection Directive. The Directive was enacted to balance the protections for individuals' privacy with the free movement of personal data within the EU. The Directive established limits regarding the collection and use of personal data and required that each Member State establish an independent national body to supervise activities associated with the processing of personal data.

Among other things, the Directive stipulates that personal data may only be transferred from a Member State to a "third country" (e.g., those outside the EU) if that country provides an adequate level of protection, subject to certain exceptions. The Article 29 Data Protection Working Party (the Article 29 Working Party), established pursuant to the Directive, negotiated with US representatives regarding the protection of personal data transferred between the EU and US and, as a result, the Safe Harbour Principles were issued by the US Department of Commerce in July 2000.

Turbulence under Safe Harbour

In the years after its inception, Safe Harbour became subject to criticism. The criticism focused on the ability of US companies to 'self-certify' under the programme, and the fact that the Federal Trade Commission (FTC) which policed Safe Harbour was not suitably stringent. Indeed, controversy over Safe Harbour had been brewing for years, not least following Edward Snowden's whistleblowing revelations which caused the European Commission to call for a review of the programme. Then, a landmark ruling in October 2015 impacted the entire compliance landscape. In the case of *Schrems vs. Data Protection Commissioner*, the European Court of Justice invalidated the Safe Harbour framework. This effectively meant that personal data transferred from Members States in Europe to the US pursuant to Safe Harbour was no longer deemed to be adequately protected, a decision that left the nearly 4500 companies that self-certified under Safe Harbour in a state of flux.

In fact, efforts to update and replace Safe Harbour with a '2.0 version' had been underway for some time, but the *Schrems* ruling demanded an urgent response. EU data protection authorities (gathered together as the Article 29 Working Party) set a 31 January 2016 deadline to replace the invalidated mechanism and for the EU and the US Department of Commerce to develop a new solution.

The introduction of the EU-US Privacy Shield

On 2 February 2016, the European Commission and the US Department of Commerce reached a deal on a new transatlantic personal data transfer pact, the resulting EU-US Privacy Shield. The European Commission has proposed that the new Privacy Shield framework be deemed adequate to enable transfers of personal data between EU Member States (and presumably the three European Economic Area members, i.e., Norway, Liechtenstein and Iceland) and the US.

The Privacy Shield framework is described by the US Department of Commerce as embodying "a renewed commitment to privacy by the U.S. and the EU, and to ensure it remains a living framework subject to active supervision, the Department of Commerce, the FTC and EU DPAs (Data Protection Authorities) will hold annual review meetings to discuss the functioning of and compliance with the Privacy Shield".

The stated aim is to strengthen cooperation between the FTC and EU DPAs, providing independent, vigorous enforcement of the data protection requirements set forth in the Privacy Shield framework. EU individuals will have access to multiple avenues to resolve concerns – at no cost to the individual – and will have an option to work with their local (national) DPA to resolve complaints. Additionally, the Privacy Shield framework includes certain safeguards and transparency obligations relative to US governmental access to personal data. For the first time, the US government has provided the EU with written commitments, including an assurance from the Office of the Director of National Intelligence that public authority access to personal data for national security purposes will be subject to clear limitations, safeguards and oversight mechanisms.

The Privacy Shield framework includes significant advancements to improve transparency regarding personal data use, strengthen the protections provided by participants and deliver a comprehensive education about the rights EU individuals have under the programme. But it is not without its critics. There are concerns about unfettered access to consumer data by intelligence and law enforcement officials. And the fact that the programme is subject to annual reviews has led to questions over whether the law could change on a regular basis, or as happened last autumn, get struck down altogether.

Before the EU-US Privacy Shield can become binding, among other things, the framework will be reviewed by the Article 29 Working Party – which will provide a non-binding opinion – and then will need to be adopted formally by the EU Commission. Further, it's possible that the Privacy Shield will be subjected to legal challenges before the European Court of Justice, assuming the EU Commission formally deems it adequate.

Best practice guidelines

Clearly, businesses cannot afford to simply wait for decisions on legality. Despite the somewhat precarious current situation, organisations conducting data transfers involving personal data from the EU are tasked with identifying and implementing a robust plan with built-in contingency if the horizon should suddenly change. In the interim, the Article 29 Working Party has confirmed that the use of model contracts or binding corporate rules can still be used for transfers of personal data from the EU to the US. Companies involved in the transfer of personal data from the EU to the US

should review their policies and procedures in light of these interim measures with an eye to further changes in the EU, especially as the new General Data Protection Regulation is formalised, as it will impact not only companies that operate in the EU, but those that do business with EU consumers.

Jayne Rothman is Senior Vice President, General Counsel and Secretary of Epiq Systems. She joined the company in 2005, and has served as Epiq's senior legal advisor since 2006. She manages general matters, including mergers & acquisitions, corporate governance, commercial transactions, litigation, dispute resolution, settlements, employment, real property, data privacy, governance, risk and compliance (GRC), enterprise risk management, insurance, intellectual property and management of inside and outside counsel. Ms. Rothman holds a J.D. from New York Law School and a bachelor's degree in humanities from the University of New Hampshire. She is admitted to practice in New York, California, S.D.N.Y. and E.D.N.Y Courts. Ms. Rothman is a frequent speaker, writer and presenter on a variety of legal topics.