THE ADR PROVISIONS OF EU PRIVACY LAWS

By Kimberly Taylor, Esq.

Companies doing business globally have a variety of complex issues to deal with, not the least of which is concern about the security of personal data collected from their customers.

In 1995, the European Union issued Directive 95/46/EC, the *Data Protection Directive*, concerning the protection of individuals with regard to the processing and transfer of personal data. Thereafter, the U.S. Department of Commerce (DOC), in consultation with the EU, developed the U.S.-EU Safe Harbor Framework. This, along with the U.S.-Swiss Safe Harbor Framework, is a streamlined process for American companies to comply with the Data Protection Directive. The Framework enables U.S. organizations to transfer personal data from the EU to the U.S. provided the American company certifies with the DOC that it adheres to the Safe Harbor privacy principles. As of December 2013, more than 4,000 companies had certified compliance with the Safe Harbor program.

Despite the Safe Harbor Framework, concerns were raised recently within the EU about data privacy amidst revelations of surveillance of EU citizens' data by the American government. The European Commission (EC) undertook a review of the EU-U.S. Safe Harbor scheme to ensure that it adequately served the purpose of preserving EU citizens' data protection right when that data was transmitted to the United States. Late last year, the EC issued a report concerning the operation of Safe Harbor and offered a number of recommendations to strengthen it.

The EC recommended that companies using the Safe Harbor process to self-certify compliance with the Data Privacy Directive be required to publicly disclose their privacy policies and include a link on their websites to the DOC list of currently certified members of the Safe Harbor. The company must also require its subcontractors to publish the privacy conditions of the terms of those subcontracting agreements. Those privacy policies should set out the extent to which U.S. law permits authorities to collect data under the Safe Harbor. Recognizing that arbitration and mediation are effective means of resolving disputes between consumer and companies, the EC also suggested changes to the already-existing requirement that companies must create a readily available and affordable mechanism for dealing with individual complaints, including a system of alternative dispute resolution (ADR) by an independent third party.

Safe Harbor certified companies' privacy policies are required to include links to the relevant ADR processes. ADR must be made "readily available and affordable" to complainants, under the Enforcement Principle of the U.S.-EU Safe Harbor Framework. The DOC must systematically review the transparency, accessibility and procedures of the ADR providers, including how they follow up on complaints by consumers. The EC recommended that any breaches of the Safe Harbor Framework be published and that a percentage of certified companies should be periodically investigated to ensure privacy policy compliance. Doubts about companies' compliance and evidence of breach of the

This article was originally published by LAW.COM and is reprinted with their permission.

policy protections should be reported by the DOC to competent EU data protection authorities. And the national security exception should be exercised sparingly only in those instances where it is strictly necessary or proportionate.

There are a variety of companies that serve as a Safe Harbor ADR provider, including the EU Data Protection Panel, the Better Business Bureau, TRUSTe, and traditional ADR providers such as AAA and JAMS. Processes and charges for this service vary, with some companies requiring an annual fee on a sliding scale basis depending on annual sales and others charging a fee per case. Because of concerns by the EC that the cost of utilizing an ADR process not be prohibitive, most ADR providers assess those costs against the companies rather than the individuals bringing privacy complaints. Residents of the EU can initiate an ADR claim if the company has self-certified its compliance with the Safe Harbor Framework so long as they include credible documentation to support the allegations and establish that they have made a good faith effort to resolve the complaint with the company.

European privacy regulation has represented the leading edge in improved security for consumer data. Regulation regarding the privacy of consumer data worldwide will continue to expand as a growing number of countries consider both how consumer data is collected and used by companies. Companies would be well advised to ensure that their data use and control policies not only comply with minimum regulated standards, but exceed them to meet the expectations of their customers and to avoid the potential legal and business consequences of improperly handling consumer data. Protecting the privacy of personal data is a serious concern for all companies, but those doing business in the EU and Switzerland must ensure that their privacy policies comply with the Safe Harbor Framework. ■

Kimberly Taylor, Esq. *is Senior Vice President and Chief Operating Officer of JAMS. She oversees JAMS operations in the United States and abroad and works directly with the President and CEO. She leads a team that spans 25 resolution centers across North America and is responsible for the company's day-to-day operating activities. She can be reached at ktaylor@jamsadr.com.*