

September 8, 2016

Privacy Shield

By Alan S. Wernick, Esq.

A manufacturing client hired me to help his business with the legal issues involved in setting up their e-commerce enabled website. Shortly after the website went live, the client's CEO mentioned to me that he was now getting customer orders from places he had never received orders from before. The Internet is global. If your business has a website which obtains information on website visitors (some of whom may be from outside the U.S.), or if your business is presently engaged or planning to engage in doing business in Europe, then the Privacy Shield is critical to your business because data privacy violations can be expensive.

In addition to complying with U.S. data privacy laws, U.S. businesses (including both for profit and not-for-profit) that acquire customer data on customers from the European Union and other countries must comply with the countries' applicable data privacy laws. A failure to comply may result in substantial penalties. Since 2000 businesses could rely on the European Commission "Safe Harbor" decision as a cost-effective means for compliance; however that decision was declared invalid in October 2015. In July 2016, the Safe Harbor decision was replaced with the new "Privacy Shield Framework" (the "Privacy Shield") which imposes stronger obligations on U.S. companies to protect Europeans' personal data. A U.S. Department of Commerce overview of the EU-U.S. Privacy Shield is available at <http://goo.gl/es4kuS>. A European Commission fact sheet on the EU-U.S. Privacy Shield is available at <http://goo.gl/izkJbl>.

The Privacy Shield program, which is administered by the International Trade Administration ("ITA") within the U.S. Department of Commerce, enables U.S.-based organizations to join the Privacy Shield in order to benefit from the resulting presumption of having adequate compliance with EU privacy laws. To participate in the Privacy Shield Framework, a U.S.-based organization is required to self-certify to the Department of Commerce and publicly commit to comply with the Privacy Shield's requirements. While joining the Privacy Shield Framework is voluntary, once an eligible organization makes the public commitment to comply with the Framework's requirements, the commitment becomes enforceable under U.S. law. On August 1, 2016, ITA began accepting certification applications from businesses. A list of companies who have self-certified to the Privacy Shield is available at <https://www.privacyshield.gov/list>.

For U.S. based businesses, and their partners in the EU, the benefits of participation in the Privacy Shield include:

- All Member States of the European Union are bound by the European Commission's finding of "adequacy;"
- Participating organizations are deemed to provide "adequate" privacy protection, a requirement (subject to some limited exceptions) for the transfer of personal data outside of the European Union under the EU Data Protection Directive;
- EU Member State requirements for prior approval of data transfers either are waived or approval will be automatically granted; and
- Compliance requirements are clearly laid out and cost-effective – a benefit for small and medium-sized enterprises.

One key difference between the Safe Harbor decision and the Privacy Shield is in the requirement for accountability for data transferred by the business to third parties. The Privacy Shield participating business must, in addition to complying with the Privacy Shield notice and choice principles, have a contract with the third-party which contains certain provisions required of Privacy Shield participants.

The Privacy Shield is being enforced in the U.S. by the Federal Trade Commission ("FTC") and the Department of Transportation ("DOT"). Under the FTC Act, a business's failure to abide by commitments to implement the Privacy Shield principles may be challenged as deceptive by the FTC. The FTC has the power to prohibit such misrepresentations through administrative orders or by seeking court orders; violations of those administrative orders can lead to civil penalties of up to \$40,000 per violation or \$40,000 per day for continuing violations as of August 1, 2016. For businesses under the DOT's jurisdiction, failure by a U.S. or foreign air carrier, or a ticket agent that markets air transportation, to abide by its public commitment to implement the Privacy Shield could be actionable under 49 U.S.C. 41712, which prohibits U.S. and foreign air carriers and ticket agents from engaging in "an unfair or deceptive practice" in the sale of air transportation that results or is likely to result in consumer harm. Violations of section 41712 can result in the issuance of cease and desist orders and the imposition of civil penalties of up to \$32,140 for each violation as of August 1, 2016.

The bottom line for U.S. businesses participating in our robust and growing global economy is that privacy does matter and a failure to understand how it matters can impact the businesses' bottom line profitability. U.S. businesses that are stewards of personally identifiable information for customers and employees outside the U.S. may want to consider the Privacy Shield as a cost-effective means to comply with the data privacy laws of European countries participating in the Privacy Shield Framework.

About the Author

Alan S. Wernick – Lawyer, Arbitrator/Mediator, and Writer. Alan is a Martindale AV rated attorney and a Leading Lawyer in Computer and Technology Law, admitted to practice in IL, NY, OH, and DC. He has more than 36 years' experience and leadership roles including (1) in the private practice of law in Information Technology, Intellectual Property, & Privacy Law; (2) as in-house general counsel and as a partner in big law firms; (3) with the successful handling of numerous large complex transactions and M&A due diligence, (4) in strategic counseling of clients in the management of their technology and intellectual capital assets, and (5) in dispute resolution including litigation, arbitration, mediation, and appeals. Alan's multidisciplinary background in law, technology, and accounting helps clients meet their business objectives and manage their legal strategies and risks. For more information about Alan's practice, publications, and lectures, please visit WWW.WERNICK.COM or LinkedIn: www.linkedin.com/in/alanwernick/

