Montgomery & Hansen LLP

Client Alert July 15, 2016

EU Approves Privacy Shield as Basis for Transferring European Personal Data to the USA.

By Daniel Appelman

Companies in the United States are prohibited by European law from transferring to this country any personal data of Europeans unless the use of that data is adequately protected as determined by the European Commission and the European national data protection authorities, or unless the data subject has consented. This includes, for example, website and mobile application user registration data, employment data, consumer purchasing data and medical data.

The basis for legal protection of personal data in Europe is Directive 95/46/EC of the European Parliament and of the Council (the "EU Data Protection Directive"). United States federal and state laws do not ensure protection for personal information that is equivalent to the protection required by the EU Data Protection Directive. Consequently, until last year many U.S. companies relied on complying with a set of privacy principles negotiated by the EU and the U.S. Department of Commerce called the EU-U.S. Safe Harbor. However, last October, the European Court of Justice invalidated the Safe Harbor after finding that it failed to ensure adequate protection of personal data. Consequently, thousands of U.S. companies that collect, store and process the personal data of Europeans in reliance on the Safe Harbor were suddenly engaging in illegal activities under European law.

EU data protection regulators threatened to begin enforcement actions against those companies unless negotiators quickly developed a substitute for the Safe Harbor. The need for such a substitute was evident, given the enormous volume of personal data flowing between Europe and the U.S.

Last Tuesday, July 11, 2016, the European Commission formally approved a new set of rules, called the EU-U.S. Privacy Shield, as an adequate legal basis for transferring personal data from EU member countries to the U.S. Those rules became effective immediately.

Like the prior Safe Harbor, the new Privacy Shield allows U.S. companies to self-certify their compliance with a set of negotiated privacy principles that the European Commission determined would provide a level of protection for personal data equivalent to that required by the EU's Data Protection Directive. For many, this will be a quicker, cheaper and less resource-intensive process compared with the two other major options for legally transferring personal data from the EU to the U.S., i.e., adopting binding corporate rules or model contract clauses that have been pre-approved by the European Commission. However, the Privacy Shield contains new obligations that may prove to be more burdensome than those under the invalidated Safe Harbor.

We briefly summarized the features of the Privacy Shield in an earlier Client Alert here when the new rules were first proposed. In somewhat greater detail, those features include the following:

- The Privacy Shield requires compliance and certification by both data controllers and data processors. A data controller is a person or organization which alone or jointly with others determines the purposes and means of processing personal data. A data processor is a person or organization which processes personal data on behalf of the controller. Companies that collect personal data from Europeans, including through website and mobile app account registrations, and companies that store or process such personal data on behalf of those companies, are "data controllers" and "data processors" respectively. Both must either comply with the Privacy Shield or transfer personal data from Europe to the U.S. through other means that have

For more information on privacy law, please contact Daniel Appelman at 650.331.7014 or dappelman@mh-llp.com

been approved by the European Commission or the relevant European national data protection authorities.

- The protection afforded by the Privacy Shield applies to any EU data subject whose personal data have been transferred from the EU to companies in the U.S. that have become Privacy Shield participating organizations. Organizations become Privacy Shield participants by certifying their adherence to the privacy principles in annual registrations with the U.S. Department of Commerce. The Department of Commerce has committed to maintain a public list of those registered organizations, to update the list and to make public a record of organizations that have been removed from the list and the reasons for their removal.

- Organizations participating in the Privacy Shield framework are required to provide information to data subjects about the type of personal data they collect, the purpose of its processing and the rights of data subjects to access that personal data and to opt out of its collection. Each Privacy Shield participating organization must also give its data subjects links to the Department of Commerce's website where they can find the list of participating organizations and information about their rights and available resources in the event of a dispute or non-compliance. Privacy Shield participating organizations must also provide each data subject with a link to the website of appropriate alternative dispute settlement providers.

- Participating organizations must limit the personal data they collect from EU data subjects to that which is relevant for the purpose of the processing.

- Whenever the purpose of the processing changes or whenever that purpose includes direct marketing to data subjects, they must be given the right to opt out.

- Participating organizations may not collect or process "sensitive data" at all unless the data subject opts in. Sensitive data includes data that reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health or sex life.

- Data subjects have the right, upon request to organizations participating in the Privacy Shield framework, to know which of those organizations are processing their personal data and to correct, amend or delete personal information where it is inaccurate or has been processed in violation of the principles.

- Participating organizations must annually re-certify their participation with the Department of Commerce and must document their compliance either through a system of self-assessment or by means of outside compliance reviews, such as third party auditing.

- The Privacy Shield framework includes special rules for U.S. data controllers and data processors that transfer personal data of EU data subjects to third party controllers or processors (called "onward transfers"). This is to ensure that the protection guaranteed by the Privacy Shield will be respected by those third parties.

- The Department of Commerce will administer the Privacy Shield system, including conducting regular updates and reviews of participating organizations; and the Federal Trade Commission and the Department of Transportation (where applicable) will assist in enforcement.

- The Privacy Shield framework includes enhanced recourse for EU data subjects who are affected by non-complying participating organizations. Data subjects may bring complaints regarding non-compliance directly to the participating organization, to an independent dispute resolution body designated by the participating organization, to national EU data protection authorities or to the Federal Trade Commission. Referrals to the Federal Trade Commission may result in enforcement actions for unfair or deceptive trade practices.

The Safe Harbor was invalidated by the European Court of Justice mainly because of concerns about intrusive U.S. government surveillance as revealed by former NSA contractor, Edward Snowden. Almost half of the European Commission's 44 page decision implementing the Privacy Shield addresses new limitations on the ability of U.S. intelligence agencies to conduct such surveillance using personal data belonging to EU data subjects.

Despite the European Commission's formal approval of the Privacy Shield, there is considerable uncertainty about its fate. Many observers expect the Privacy Shield to be challenged by Europe's data protection authorities, non-governmental organizations and EU data subjects as failing to ensure a level of protection that is essentially equivalent to that guaranteed by the EU Data Protection Directive. Nevertheless, several U.S.

companies, including Microsoft and Google, have already indicated that they will become participating Privacy Shield organizations.

The Privacy Shield will be an option for businesses transferring European personal data to the United States as well as for those companies processing, using or storing such data, unless and until the European Court of Justice invalidates it as they did the Safe Harbor. Companies that previously relied on the Safe Harbor should become familiar with the new compliance requirements of the Privacy Shield and determine whether participation is appropriate for them.