Torkin Manes
Barristers & Solicitors

Torkin Manes LegalPoint

TECHNOLOGY, PRIVACY & DATA MANAGEMENT

APRIL 2016

Welcome to the new EU-US Privacy Shield

After two years of negotiations, the European Commission and United States of America (the "**U.S.**") have unveiled the replacement to the U.S.-EU Safe Harbor Framework (the "**Safe Harbor**"), known as the EU-U.S. Privacy Shield (the "**Privacy Shield**").

When U.S. companies engage in trade and commerce with the European Union (the "**EU**"), the personal information of EU citizens is often transferred to the U.S. Prior to October 2015, U.S. companies protected the data of EU citizens by complying with the requirements of the Safe Harbor. However, on October 6, 2015, the Court of Justice of the European Union declared that the Safe Habor was invalid. After this decision, the U.S. and EU began negotiations to develop a new framework for transatlantic data transfers, which the European Commission revealed on February 2, 2016 as the Privacy Shield. The intention of the Privacy Shield is to ensure that when the personal information of EU citizens is transferred to U.S. companies under the Privacy Shield, such personal information will receive equivalent data protection standards to those standards that exist in the EU. On February 29, 2016, the European Commission released a draft adequacy decision and the legal texts that will form the Privacy Shield, including written assurance by the U.S. government to enforce the agreement and the Privacy Shield Principles, that is, the principles that participating U.S. companies will be required to follow (the "**Privacy Shield Principles**")[1].

The decision to enter the Privacy Shield is voluntary. U.S. companies that wish to rely on the Privacy Shield are required to self-certify, publicly declare their adherence to the Privacy Shield Principles and demonstrate full compliance. The U.S. Department of Commerce (the "**Department of Commerce**") will keep an updated and publicly available list of the companies that have entered the Privacy Shield (the "**List**") and will remove from such List any companies that have voluntarily withdrawn or been removed due to non-compliance. U.S. companies that have entered the Privacy Shield must apply the Privacy Shield Principles to personal information transferred under the Privacy Shield. Additionally, companies that were

Lisa R. Lifshitz
Chair, Technology, Privacy & Data Management

PHONE
416 775 8821

EMAIL
llifshitz@torkinmanes.com

Dianne Hajdasz
Associate, Technology, Privacy & Data Management

PHONE
416 777 5429

EMAIL
dhajdasz@torkinmanes.com

removed from the List, but still retain personal information that was received while they participated in the Privacy Shield, must continue to apply the Privacy Shield Principles to such personal information.

The Privacy Shield Principles are broken down into seven areas: (1) **Notice** (i.e. companies must inform individuals about specifically listed information); (2) **Choice** (i.e. individuals must be given the opportunity to choose whether their information can be disclosed to a third party or used for a purpose other than the original purpose for which the information was collected); (3) **Accountability for Onward Transfer** (i.e. companies must enter into contracts with third party controllers that will process the personal information); (4) **Security** (i.e. companies must protect the personal information from loss, unauthorized access, disclosure, modification and destruction); (5) **Data Integrity and Purpose Limitation** (i.e. the personal information must be limited to that which is necessary and it cannot be processed in ways that are incompatible with the purposes for which the information was collected or authorized; (6) **Access** (i.e. individuals must have access to their personal information and can correct, amend or delete any inaccuracies); (7) **Recourse, Enforcement and Liability** (i.e. there must be "robust mechanisms" to ensure participating companies comply with the Privacy Shield Principles, consequences for those that do not comply, and recourse for individuals affected by such non-compliance such as dispute resolution services and arbitration). In addition to these seven principles, there are supplemental principles that provide additional information regarding various topics including, but not limited to, the role of EU Data Protection Authorities (the "**DPAs**"), the self-certification process, human resources data, mandatory contracts for onward transfers of personal information, requests by an individual to access his/her personal information, pharmaceutical and medical products and publicly available information.

The U.S. will administer and monitor the Privacy Shield in varying ways, some of which are discussed below. The U.S. will implement an Ombudsperson Mechanism through which the Ombudsperson will handle complaints of EU individuals regarding access of their personal information by national intelligence authorities. The Department of Commerce will make available to the public the List and a record of those companies that were removed from the List. The Department of Commerce will also verify that any companies that are self-certifying (or annually re-certifying) have satisfied specific requirements, such as having the company's privacy policy on its public website or at a location where it can be viewed by the public. The Department of Commerce will follow up with companies that are no longer on the List, and it will review the privacy policies of companies that used to participate under the Privacy Shield for any false claims of current participation under the Privacy Shield. In addition, the Department of Commerce will increase its cooperation with the DPAs by dedicating a specific contact at the Department of Commerce to communicate with the DPAs. The European Commission and Department of Commerce will conduct annual joint reviews, involving U.S. national security authorities and the DPAs, to monitor the functioning of the Privacy Shield, including access to personal information by U.S. national security authorities. The U.S. has also provided the EU with written assurances that the access of personal information of EU citizens by public authorities for the purposes of law enforcement and national security will be based on "clear limitations, safeguards and oversight mechanism, preventing generalised access to personal data"[2].

The Privacy Shield is not yet in force. Before the College of Commissioners can make a final decision, there will be consultations with representatives of the EU member states and the Article 29 Working Party. In the meantime, the U.S. will begin preparing for this new framework.

Canadian companies should take note that U.S. companies will have new and distinct compliance requirements under the Privacy Shield, including amended privacy policies, in the near future.

1 The full text of the EU-U.S. Privacy Shield Framework is available on the U.S. Department of Commerce website at the following link: <https://www.commerce.gov/privacyshield>

2 European Commission, R*estoring trust in transatlantic data flows through strong safeguards: European Commission presents EU-U.S. Privacy Shield*, Press Release, 29 February 2016, available online at: European Commission <http://europa.eu/rapid/press-release_IP-16-433_en.htm>.

3 *Ibid.*