From “Safe Harbor” to “Privacy Shield”: laying the groundwork for a new agreement on transatlantic data transfer with the United States

February 11, 2016

Authors

Loïc Berdnikoff

Chief Privacy Officer and Chief, Legal Operations and Conformity and and Lawyer

Raymond Doray

Partner, Lawyer

Guillaume Laberge

Partner, Lawyer

The United States and the European Union recently concluded a new agreement aimed at allowing U.S. companies to continue to collect, use and disclose personal information concerning European citizens, while still preserving their fundamental rights.

To properly understand the importance of this new agreement, one must be aware that the Court of Justice of the European Union, in a decision rendered on October 6, 2015, had declared invalid the previous data sharing framework, known as "Safe Harbour", which governed the holding of personal information regarding European nationals by numerous American companies, including Web giants such as Facebook and Google. This transnational agreement provided for a self-certification mechanism for U.S. companies by which they undertook to abide by a certain number of guiding principles applicable in the European Economic Area (EEA), pursuant to which these companies could obtain the authorization to collect and store personal information originating from the European Union. Such an agreement was necessary to allow U.S. companies to hold personal information about European citizens because the legislative framework applicable in the United States does not offer "an adequate level of protection" for personal information as compared with that required by European authorities.

However, in the wake of the revelations by Edward Snowden regarding the mass surveillance by U.S. authorities of the computer data of several large corporations, an Austrian citizen, Maximillian Schrems, sought and obtained the invalidation by the Court of Justice of the European Union of the Safe Harbour Agreement.[1] The Court held that the “legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life”. While this decision was, in principle, supposed to apply immediately, the Data Protection Working Party (known as the “WP29”) — an independent European advisory board on data protection and privacy — urged the European institutions and the U.S. government to act by January 31, 2016 to agree to an alternative solution.

It was in this context that the European Commission made the highly anticipated announcement, on February 2, 2016, of a new agreement in principle with the United States, dubbed the "Privacy Shield". The details of this agreement have not yet been disclosed, but we already know that this new mechanism will entail stricter obligations and tighter control of U.S. companies that deal with information of a personal nature originating from the European Union. Furthermore, access by U.S. authorities to this information is expected to be more closely regulated and more transparent.

While, in theory, this agreement does not directly affect Canadian companies that collect, use or disclose personal information regarding European citizens, any such companies having an American subsidiary or a place of business in the United States and which collect personal information from Europe, as well as Canadian companies mandating third parties located in the United States with tasks that require the communication of personal information on European nationals, e.g. for hosting purposes, would be well advised to ensure they comply with the conditions of this new agreement when it takes effect. Stay tuned for more updates.

---

1. *Schrems* v. *Data Protection Commissioner*, 2000/520/CE, Court of Justice of the European Union, 6 Octobre 2015.