New ‘EU-US Privacy Shield’ to replace Safe Harbour

February 2, 2016

On February 2, 2016, in a meeting conducted in Brussels, the European Commission and the United States agreed on a new framework for transatlantic data flows. With all the negative connotations surrounding it, the name “Safe Harbour” has been dropped, and the new agreement will be called the “EU-US Privacy Shield.”

This new framework will return legal certainty to companies that were thrown into confusion after the European Court of Justice discredited the Safe Harbor Framework in its decision in the case of Max Schrems on October 6, 2015.

The Article 29 Working Party, the meeting of the data protection Authorities from across the European Union, continues in Brussels and will provide its feedback on this new scheme in the next 24 hours. It was that body that promised to start enforcement action against the approximately 4000 U.S. companies that signed up to Safe Harbour if a replacement was not agreed upon by January 31, 2016. The passing of that deadline and the strong words exchanged between attendees during the talks over the weekend made an agreement look beyond hope. However, today’s announcement should bring relief to those who rely on the transfer of data to run their business operations in Europe.

The new arrangement will impose more stringent obligations on companies in the United States to protect the personal data of Europeans, in addition to imposing stronger monitoring and enforcement obligations on the U.S. Department of Commerce and Federal Trade Commission (FTC), including through increased cooperation with European data protection authorities.

The new scheme offers the following greater protections to EU citizens’ data:

- U.S. companies wishing to import personal data from Europe will need to commit to even more robust obligations on how personal data is processed and how rights are guaranteed.
- The U.S. Department of Commerce will monitor companies to ensure that they publish their commitments, thereby making their commitments enforceable by the FTC under U.S. law.
- Any company handling human resources data from Europe is required to commit to complying with decisions of the European data protection authorities.
- The United States has given the European Union written assurances that the access of public authorities for law enforcement and national security will be
subject to clear limitations, safeguards, and oversight. Exceptions must be used only to the extent necessary and proportionate.

1. The United States has ruled out the possibility that personal data transferred to the United States under the new arrangement will be subject to indiscriminate mass surveillance.

2. Under the new scheme, U.S. companies have deadlines to reply to complaints.

3. European data protection authorities can refer complaints to the Department of Commerce and the FTC.

4. A new Ombudsman position will be created to handle complaints that national intelligence authorities have accessed data.

In addition to these protections, the Safe Harbour scheme calls for an annual joint review to regularly monitor the functioning of the arrangement. The review will also cover the issue of national security access. The European Commission and the U.S. Department of Commerce will conduct the review and invite national intelligence experts from the United States and European data protection authorities to contribute to the review.

Next Steps

The European Commission will prepare a draft “adequacy decision” in the coming weeks, which could then be adopted by the College of Commissioners at the European Union. In the meantime, the United States will make the necessary preparations to put in place the new framework, monitoring mechanisms, and Ombudsman.

EU Vice-President for the Single Digital Market Andrus Ansip said:

We have agreed on a new strong framework on data flows with the US. Our people can be sure that their personal data is fully protected. Our businesses, especially the smallest ones, have the legal certainty they need to develop their activities across the Atlantic. We have a duty to check and we will closely monitor the new arrangement to make sure it keeps delivering. Today’s decision helps us build a Digital Single Market in the EU, a trusted and dynamic online environment; it further strengthens our close partnership with the US. We will work now to put it in place as soon as possible.

The Article 29 Working Party has yet to make any comment but it would seem they should be content now that an agreement has been reached—better late than never!

The Ogletree Deakins Data Privacy Practice Group will continue to monitor the progress of the new EU-US Privacy Shield and will provide further updates and present a webinar on practical steps businesses should take to comply with the new requirements.