EU-US Privacy Shield gets Green Light

Authored by Philippa Donn, Editor of the Data Protection Network (www.dpnetwork.org.uk)

After nine long months of negotiations, the new EU-US Privacy Shield has been born. It replaces the *Safe Harbor Agreement* which was ruled invalid by the European Court of Justice in October last year, and certifications can be filed from 1st August 2016.

Its creators claim the Privacy Shield differs significantly from its predecessor: it contains more stringent privacy terms and safeguards, reflecting a broader range of legal protections in the US surrounding government surveillance. It also strengthens the rights of data subjects, includes robust complaint procedures and provides for enforcement mechanisms for organisations who fail to comply.

Launching the Privacy Shield, Andrus Ansip, Commission Vice-President for the Digital Single Market, said, *"it will protect the personal data of our people and provide clarity for businesses. We have worked hard with all our partners in Europe and in the US to get this deal right and to have it done as soon as possible. Data flows between our two continents are essential to our society and economy – we now have a robust framework ensuring these transfers take place in the best and safest conditions".*

Věra Jourová, Commissioner for Justice, Consumers and Gender Equality said, *"the EU-US Privacy Shield is a robust new system to protect the personal data of Europeans and ensure legal certainty for businesses. It brings stronger data protection standards that are better enforced, safeguards on government access, and easier redress for individuals in case of complaints. The new framework will restore the trust of consumers when their data is transferred across the Atlantic. We have worked together with the European data protection authorities, the European Parliament, the Member States and our US counterparts to put in place an arrangement with the highest standards to protect Europeans' personal data*".

The Privacy Shield, in a similar way to Safe Harbor, is based on a system of self-certification whereby organisations commit to *The Principles* of the agreement. *The Principles* apply to both data controllers and processors, with *"the specificity that processors must be contractually bound to act only on the instructions from the EU controller and assist the later in responding to individuals exercising their rights under the Principles."*

The 7 Principles are:

1. Notice
2. Choice
3. Data Integrity and Purpose Limitation
4. Access
5. Accountability for Onward Transfer
6. Security

7. Recourse, Enforcement and Liability

You can find more detail on *The Principles* from the European Commission here *(2.1 Privacy Principles)*

Under the *Choice Principle* it allows for data subjects to opt-out of their personal data being disclosed to a third party and includes a special rule generally allowing for the opt-out "at any time" from the use of personal data for direct marketing purposes.

It's worth noting that a US company processing personal data of EU/EEA data subjects whose activities fall under the scope of Article 3* of GDPR, must not assume that self-certification under the Privacy Shield will be sufficient to demonstrate compliance with all GDPR provisions.

Negotiators were keen to ensure heightened focus on transparency and oversight in the new agreement. As part of this drive, the US Department of Commerce will now be tasked with regularly monitoring organisations on the Privacy Shield list to ensure they are meeting their obligations. If found to be non-compliant with *The Principles,* organisations can be struck off the list and required to return or delete the personal data they have received under the agreement. The Department of Commerce will make both the Privacy Shield List and the re-certification submissions publicly available on a dedicated website.

In order to assuage concerns surrounding surveillance, the US Government has committed to create a new oversight mechanism for "national security interference," the *Privacy Shield Ombudsman*, who is to be independent from the Intelligence Community.

However, it's already being argued the Privacy Shield doesn't go far enough and still opens European citizens to mass US surveillance. Privacy campaigner Max Schrems, whose case against Facebook led to the demise of Safe Harbor, believes companies will be reluctant to sign up because in his words "it's going to fail like the one before." It is highly likely a legal challenge will be mounted, which could ultimately take the new framework to the European Court of Justice. The Commission will be hoping it can offer a more robust defence on the basis that the Privacy Shield is in their words, "fundamentally different from the old *Safe Harbor.*" A view Schrems, for one, doesn't share.

**Article 3 states that the Regulation applies to the processing of personal data of data subjects located in the EU, even if the relevant controller or processor is not established in the EU, provided that the processing relates to the offering of goods or services to the data subjects (whether or not payment is required), or the monitoring of data subjects' behaviour.*