

# Data transfers under review: a new EU-US Privacy Shield

Following weeks of intense discussions between EU and US officials, it was announced, on 2 February 2016, that political agreement had been reached on a new framework for transAtlantic data flows. The announcement of the 'EU-US Privacy Shield' by the European Commission was the latest in a series of developments and reactions in the aftermath of the Court of Justice of the European Union's ('CJEU') judgement on 6 October 2015 in the *Schrems* case, rendering Commission Decision 2000/520 on Safe Harbor invalid. William Long and Francesca Blythe, Partner and Associate respectively at Sidley Austin LLP, provide their insights into what is currently known regarding the Privacy Shield.

## Introduction

This new framework still hangs in the balance, as the Article 29 Working Party ('WP29') confirmed in a statement on 3 February 2016 that it would not be in a position to support the framework until it had carried out a detailed review of the Privacy Shield in light of the CJEU judgement. Having said this, the WP29 did welcome the fact that the negotiations between EU and US officials had concluded.

According to the European Union's Commissioner for Justice, Consumers and Gender Equality, Věra Jourová, the new framework, which will take the form of an exchange of letters signed at the highest political level, will centre on three key issues broadly in line with the concerns expressed by the CJEU in its judgement in the *Schrems* case. These include:

1. New robust obligations on participating companies;
2. Transparency requirements and clear safeguards in respect of the US Government's access to personal data; and
3. Enhancement in the protections afforded to EU citizens.

As such, the European Commission and US authorities are confident that these legally binding commitments will ensure that safeguards are 'essentially equivalent' to those in the EU and will, therefore be sufficient to withstand the inevitable legal challenges.

## What do we know?

Although all the details of the new framework have not been disclosed, there are a number of elements which have been confirmed, including:

- Participating US companies will have to commit to new 'robust obligations' in respect of the processing of personal data and the safeguarding of individuals' rights, including, for example, new

contractual requirements for onward transfers. Companies will be monitored by the US Department of Commerce with the Federal Trade Commission taking the lead on enforcement.

- In respect of surveillance, written assurances will be given by the US that for data transferred pursuant to the Privacy Shield:

1. Public authorities' access to personal data will be subject to clear limitations, safeguards and oversight mechanisms;
2. Indiscriminate mass surveillance will not be permitted except in limited circumstances;
3. Safeguards will apply equally to non-US citizens; and
4. An Annual Joint Review Committee will be established with reviews undertaken by the European Commission and the US Department of Commerce, with input from the US security and intelligence agencies and European data protection authorities. There is also a push from certain stakeholders for industry to be involved in the annual reviews.

- In terms of individual redress, there will be a new multi-layered complaints mechanism where should a US-participating company not be able to resolve an individual complaint, then the individual will have recourse to an alternative dispute resolution procedure, as well as enforcement action by the Federal Trade Commission and, as a last resort, a binding arbitration panel. All of these are intended to be available at no cost to individuals, although it has not yet been confirmed who will cover this cost. In addition, in the context of surveillance and access by national intelligence authorities to individuals' data an independent ombudsman will be appointed.

## The practicalities

Participating US companies in the

Privacy Shield will have to meet more stringent obligations regarding the processing of personal data than under the now invalid Safe Harbor Framework. We understand that these obligations will be in line with the EU General Data Protection Regulation, which is due to be adopted in the coming months. In practical terms, this is likely to mean that US companies will need to implement a data protection programme that meets EU privacy standards, document international data flows, review and amend existing notices, consents and privacy policies, impose onward transfer agreements on subcontractors or other third party recipients, and develop complaints procedures. However, it is still unclear how Safe Harbor self-certified companies will transition to the new framework and how companies new to the framework will certify to the Privacy Shield, although, we understand that the European Commission will be working on a number of guidelines to assist companies in implementing the Privacy Shield.

#### **Where does this leave us in terms of next steps?**

The European Commission is to prepare a draft 'adequacy decision' in the coming weeks, which marks the start of the comitology procedure in the EU. This so-called comitology procedure involves review of the Privacy Shield by the WP29 and the Article 31 Committee, which consists of representatives from EU Member States. The European Parliament will also be consulted and may require a resolution to be passed.

The WP29 has imposed a deadline of the end of February 2016 for it to receive the documents on the Privacy Shield from the European Commission. In its statement published on 3

**Although the significant efforts by US and EU authorities to achieve a political agreement on are very much welcomed, there will continue to be uncertainty until the WP29 has concluded its review, not only of the Privacy Shield but also of the other data transfer mechanisms**

February 2016, the WP29 indicated that its review would be undertaken in line with the 'four essential guarantees for intelligence activities' established pursuant to EU case law:

1. Processing should be based on clear, precise and accessible rules;
2. Necessity and proportionality should be demonstrated;
3. An independent oversight mechanism should exist; and
4. Effective remedies should be available for individuals.

#### **Conclusion**

Although the significant efforts by US and EU authorities to achieve a political agreement on the Privacy Shield are very much welcomed by businesses operating transAtlantic data flows, there will continue to be uncertainty until the WP29 has concluded its review, not only of the Privacy Shield but also of the other data transfer mechanisms (i.e. EU Standard Contractual Clauses and Binding Corporate Rules).

During this period of ambiguity companies will need to closely monitor the fast-moving developments to determine the best strategy for dealing with international transfers.

---

**William Long** Partner  
**Francesca Blythe** Associate  
 Sidley Austin LLP, London  
 wlong@sidley.com  
 fblythe@sidley.com

---