



The EU-US Privacy Shield: the new data protection deal

Service area / [Dispute Resolution and Litigation](#)

Location / [Group](#)

Date / [February 2016](#)

The (un)safe harbor and schrems

As explained in detail in our article from October 2015, the Court of Justice of the European Union declared in its judgment in the case of Schrems v Facebook that the EU-US Safe Harbor agreement (Safe Harbor) was invalid. This meant that data transfers between European Union Member States and the United States which were taking place under Safe Harbor, were no longer lawful.

The decision was primarily based on the ability of the US authorities to access personal data transferred from the Member States to the United States and process it in a way incompatible with the purposes for which it was transferred and beyond what was strictly necessary and proportionate for the protection of national security.

Notwithstanding this decision, the European Commission made it clear that there were alternative ways in which lawful transfers could be made – including the use of Binding Corporate Rules (BCRs), Standard Contractual Clauses (SCCs) or by consent. However, Safe Harbor could no longer be relied upon.

Since then, steps have been taken to agree a replacement for the Safe Harbor scheme.

The Article 29 Working Party's deadline of 31 January 2016

The EU's Article 29 Working Party (the Working Party), comprising the national data protection authorities of EU Member States, the European Data Protection Supervisor and the European Commission, set a deadline of 31 January 2016 for a new agreement to be reached to replace Safe Harbor, which had been in operation since 2000.

The Working Party stated that any new deal needed to address the issue of “massive and indiscriminate surveillance” that was taking place in the US. The deal should therefore include obligations in relation to the necessary oversight of access by public authorities, transparency, proportionality, redress mechanisms and clarify the data protection rights of individuals.

The new deal: the EU-US Privacy Shield

Although the original deadline of 31 January 2016 was not met, a new political deal in the form of the EU-US Privacy Shield (the Privacy Shield) was announced by the European Commission on 2 February 2016. Details of the new scheme have yet to be announced and there remains a high degree of uncertainty about its terms.

The Privacy Shield includes the following key elements:

- Stronger obligations on US companies to protect the personal data of EU citizens, including how personal data are processed and the individual rights of EU citizens being guaranteed. The US Department of Commerce will monitor US companies to ensure that they publish and adhere to these obligations. Any US company processing European human resources data must also comply with the decisions of European data protection agencies.
- Written assurances that US public authorities' access to data for law enforcement and national security purposes will be subject to clear limitations, safeguards and oversight mechanisms. These public authorities will only have exceptional, necessary and proportionate access to personal data, which will therefore not be subject to indiscriminate mass surveillance. The European Commission and US Department of Commerce will conduct an annual joint review of this arrangement to monitor its implementation.
- Effective protection of EU citizens' rights. This is achieved in several ways. US companies will have deadlines by which they must reply to complaints. European data protection authorities may refer complaints to the US Department of Commerce and the Federal Trade Commission to ensure that complaints are investigated and resolved. Free alternative dispute resolution will also be available. The US authorities are also in the process of creating an Ombudsman within the US State Department to whom EU citizens will be able to raise enquiries or complaints in relation to access to their data by US national intelligence authorities (on reference from a EU data protection authority).

It should also be noted that the US Judicial Redress Act was passed by the Senate Judiciary Committee on 28 January 2016. In the event that it comes into force, which is now likely as it nears the end of the legislative process, it would give EU citizens the right to start proceedings against specific government agencies in order to obtain redress for unlawful use of their data. The draft legislation preserves the right of companies to transfer personal data to the US for commercial purposes and requires EU member states to have personal data transfer policies that do not materially impede the national security interests of the US.

Further, President Obama signed an executive order on 9 February 2016 establishing a Federal Privacy Council, designed to serve as an interagency support structure to improve the privacy practices of government agencies through sharing best practice and structured training.

The response and next steps

The Working Party issued a press release on 3 February 2016 in which it welcomed the Privacy Shield, albeit reserving judgment on whether or not it deals with all of the issues raised in Schrems in relation to the international transfers of personal data. It referred to four essential guarantees for intelligence gathering in the context of European principles which it wished to see reflected in the Privacy Shield:

- Processing should be based on clear, precise and accessible rules;
- There must be necessity and proportionality;
- There needs to be an effective and impartial independent oversight mechanism; and
- Effective remedies must be available to the individual.

The Working Party remains concerned about the scope of processing and remedies available, meaning that there could be further negotiations in order to address these issues.

It is difficult to conceive of any government (let alone the US) giving a guarantee of independent oversight of its intelligence gathering activities. It remains to be seen as to whether any European nation state would be prepared to subject its own intelligence gathering to such oversight.

These negotiations have highlighted the inevitable tension between two competing (and both to some extent justified) concerns – those of privacy campaigners on the one hand and those of law enforcement authorities on the other. Striking a balance between the two would appear to be some way off.

The College of Commissioners is now preparing a draft adequacy decision in relation to the Privacy Shield (i.e. a decision that will state whether or not there will be adequate protection of the personal data of EU citizens that are transferred to the US under the new arrangement). This draft decision is expected to be produced within the next few weeks.

The Working Party has also requested that documentation relating to the Privacy Shield (in essence, the detailed terms which have yet to be made public) is produced to it by the end of February 2016, in order that they may analyse it at an extraordinary plenary meeting in March 2016. There remains significant uncertainty as to not only the precise terms being discussed, but also the extent to which the Working Party's concerns and guarantees have been addressed.

Notwithstanding the above, it has been suggested that the Privacy Shield could be implemented within the next three months, although objectively that seems optimistic.

Continued

Practical implications

The Working Party made it clear in their press release that transfers being effected under Safe Harbor are not valid and complaints arising from such transfers will be considered and determined in the usual way. However, Isabelle Falque-Pierrotin, Chair of the Working Party, has confirmed (9 February 2016) that the “moratorium” on enforcement would continue until April, in order to allow them time to scrutinise the Privacy Shield. Businesses effecting transfers under the auspices of Safe Harbor can expect enforcement action thereafter. However, the use of BCRs and SCCs remains legitimate, at least for now.

Businesses should therefore review their data flows and check (to the extent they have not done so already) that such are covered by one of the “approved” mechanisms, such as BCRs and SCCs.

The muted reaction of the Working Party and commentators would appear to suggest that there is considerable doubt as to whether the Privacy Shield will satisfy the concerns of the ECJ in Schrems – a state of uncertainty which is likely to last for a considerable time. It is also highly likely that any solution (including the Privacy Shield) is likely to be a short term one – the new General Data Protection Regulation is likely to have a significant impact, notwithstanding the assurances that the negotiators had one eye on the Regulation during their discussions.

We await the position that will be taken by the Channel Islands and other offshore Data Protection authorities in relation to local enforcement. In any event, it would be prudent to review what arrangements and contractual agreements are in place in relation to the international transfers of data (particularly to the US) and to obtain professional advice in order to safeguard the legitimacy of such transfers.



FIND US

Carey Olsen
Rodus Building PO Box 3093
Road Town Tortola VG1110
British Virgin Islands

T +1 284 394 4030
E bvi@careyolsen.com

Carey Olsen
PO Box 10008 Willow House
Cricket Square Grand Cayman
KY1-1001 Cayman Islands

T +1 345 749 2000
E cayman@careyolsen.com

Carey Olsen (Guernsey) LLP
PO Box 98 Carey House
Les Banques St Peter Port
Guernsey GY1 4BZ
Channel Islands

T +44 (0)1481 727272
E guernsey@careyolsen.com

Carey Olsen Jersey LLP
47 Esplanade St Helier
Jersey JE1 0BD Channel Islands

T +44 (0)1534 888900
E jerseyco@careyolsen.com



FOLLOW US

Visit our dispute resolution and litigation team at careyolsen.com



PLEASE NOTE

This briefing is only intended to provide a very general overview of the matters to which it relates. It is not intended as legal advice and should not be relied on as such. © Carey Olsen 2019