HERBERT SMITH FREEHILLS

SHOCKWAVES AFTER SCHREMS: SAFE HARBOR FALLOUT CONTINUES

02 November 2015 | London
Legal Briefings – By **Nick Pantlin**, **Miriam Everett** and **Duc Tran**

Following the recent judgment finding the US Safe Harbor invalid for the transfer of personal data from Europe, data protection observers have witnessed a ripple effect across EU Member States and beyond, as regulators grapple with the consequences of the ruling.

On 6 October 2015, the Court of Justice of the European Union (the "**CJEU**") issued its long-awaited ruling in the case of Maximillian Schrems v Data Protection Commissioner (Case C-362/14). The CJEU found that the existence of the European Commission Decision 2000/520 in relation to the so-called US Safe Harbour (the "**Safe Harbour Decision**") did not prevent a national data protection authority from investigating individual complaints relating to the transfer of personal data to the United States. The CJEU further considered the Safe Harbour Decision itself and found it to be invalid.

ARTICLE 29 WORKING PARTY STATEMENT

In its eagerly awaited statement released on 16 October 2015, the Article 29 Working Party (the "**Working Party**"), the body of representatives which includes representatives the European Member States' data protection authorities, as well as representatives from the European Commission and the European Data Protection Supervisor, clarified a number of consequences of the decision in the Schrems case:

- Safe Harbor transfers – the Working Party has reiterated that transfers taking place pursuant to the Safe Harbor Decision and following the CJEU judgment are unlawful.
- Binding Corporate Rules and Model Clauses – the Working Party has said that it will take some time to analyse the impact of the CJEU judgment on other transfer mechanisms

under the Data Protection Directive. In the meantime, it has confirmed that Model Clauses and Binding Corporate Rules ("BCRs") are still valid mechanisms for the transfer of personal data to the US. However, the use of such mechanisms will not prevent data protection authorities from investigating particular cases, for example, if there has been a complaint.

- A new Safe Harbor? – the Working Party has called upon the Member States, European institutions, and the US authorities to urgently enter into negotiations to find solutions which will enable the transfer of data to the US. The current Safe Harbor negotiations could be a solution but the Working Party also suggests the negotiation of an intergovernmental agreement providing stronger guarantees to EU data subjects. It also confirms that any new agreement must include obligations on the necessary oversight of access by public authorities, transparency, proportionality and redress.

- Timetable – the Working Party states that if no alternative solution is found by the end of January 2016, the EU data protection authorities are committed to take all necessary and appropriate actions, which may include coordinated enforcement actions, presumably to enforce the CJEU judgment and potentially suspend data flows.

The Working Party seems to therefore be trying to inject a level of urgency into negotiations to find a new data transfer solution by setting a deadline and hinting that even Model Clauses and BCRs will be subject to additional scrutiny going forward. To view a copy of the Working Party statement, please click here.

SELECTED REGULATOR RESPONSES

From a practical perspective, in the aftermath of the CJEU judgment, some global organisations are reported to be in the process of establishing, or have already established, data centres in Europe to avoid transferring data to the US altogether. We have also seen movement from a regulatory perspective, with the following selected reactions from regulators in EU Member States and further afield:

UK – in his statement on the case dated 6 October 2015, the UK Information Commissioner stated that: "The judgment means that businesses that use Safe Harbor will need to review how they ensure that data transferred to the US is transferred in line with the law. We recognise that it will take them some time for them to do this." It appears therefore that the message from the UK regulator is that he will not immediately start taking enforcement action but that organisations should consider carefully the best steps to take before going ahead.

Israel – in the first example of the global ramifications of the CJEU judgment, on 19 October the Israeli Law, Information and Technology Authority ("**ILITA**") revoked its own decision giving prior authorisation for the transfer of data from Israel to US companies signed-up to the Safe Harbor. From a European data protection perspective, Israel is currently a so-called "white list" country, having been found by the European Commission to provide an adequate level of protection for personal data, including restricting data transfers to third countries that are not part of the EU or receive data from the EU under a valid legal arrangement. The European Commission's decision with respect to Israel means that personal data may currently be transferred from the EU to Israel without additional compliance measures (such as Model Clauses or consent) being required. The decision by ILIITA may be a pre-emptory one to try and ensure that Israel's own status as a white list country does not get called into question, but it will have a significant impact on Israel's burgeoning technology sector, which has historically often relied on the Safe Harbor to send data from Israel to the US.

Ireland – in Ireland, the Schrems case returned to the Irish High Court on 20 October 2015 following its referral to the CJEU. The presiding Judge in the Irish High Court held that the Irish Data Protection Commissioner (the "**DPC**") had an independent duty to investigate, and EU/US political developments that may or may not happen were irrelevant. The DPC will now investigate Facebook's EU to US data transfers to see whether or not they meet Irish and EU data privacy requirements.

USA – the CJEU judgment has also had an effect in the US. In the aftermath of the ruling, the House of Representatives passed the Judicial Redress Bill on 20 October 2015, moving the Bill one step closer to law. The Judicial Redress Bill was proposed as part of the EU-US Umbrella Agreement announced in September (for further details, see our eBulletin available here). As part of that announcement, the EU had confirmed that, although the Umbrella Agreement had been finalised, it would not be signed until the Judicial Redress Bill was passed. Passing through the House of Representatives is the first step in moving this legislation forward – it must now be passed by the Senate (at present, the legislation is under review by the US Senate Judiciary Committee). However, the legislation is not just important for the Umbrella Agreement. Judicial redress was also mentioned by the Working Party in its statement as a vital component of any future agreement between the EU and the US with respect to the transfer of personal data to the US. The proposed Judicial Redress Bill would "designate foreign countries or regional economic integration organisations whose natural citizens may bring civil actions under the Privacy Act of 1974 against certain US government agencies for purposes of accessing, amending or redressing unlawful disclosures of records maintained by an agency." In theory, EU Member States could therefore be designated, giving European citizens legal redress with respect to privacy breaches. In an interview, European Data Protection Supervisor Giovanni Buttarelli identified the Bill specifically as something that would allow the US to move toward becoming "essentially equivalent" to the EU, which would address some of the concerns of the CJEU in the Schrems case. As a result, US tech companies with operations in the EU have a particular interest in the passage of the Judicial Redress Bill into law, and are continuing to re-evaluate their data transfer policies in the wake of the CJEU judgment.

Germany – most recently, the German data protection authorities have expressed a restrictive view with respect to the consequences of the CJEU judgment in their position paper dated 26 October 2015 (the "**German Position Paper**"). In the German Position Paper, the German data protection authorities confirmed that a data transfer solely based on Safe Harbour is unlawful, but also went further to state that:

- BCRs and "**Export Agreements**" (being data transfer agreements which deviate from the Model Clauses in some way) being used as the basis of a data transfer into the US will not be approved by the German data protection authorities going forward (although the German Position Paper does not confirm whether or not existing BCRs and Export Agreements may continue to be used as a transfer compliance mechanism); and

- any data transfer into the US on the basis of the consent of the data subject will only be permitted under very restrictive conditions (i.e. in general, consent of the data subject will not justify repeated mass transfers of personal data).

Prior to the German Position Paper, the German data protection authorities had published different views on the impacts of the CJEU judgment. The view of the competent data protection authority for Schleswig-Holstein was that Model Clauses and consent (as well as the Safe Harbor) are invalid ways of transferring data to the US. The authority in Schleswig-Holstein even recommended that German companies terminate their Model Clauses, perform a complete review of data transfers, and consult with the authority regarding data transfers to the US.

While the joint German Position Paper certainly has helped clarify the position in Germany, companies seeking to lawfully transfer data to the US are still left with considerable uncertainty as to what their future compliance mechanism will be:

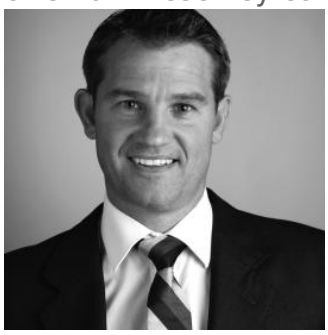
- Companies previously relying on the US Safe Harbor have few options. Since obtaining data subject consents will not be feasible in the majority of cases, the most efficient way (except for companies located in Schleswig-Holstein) is likely to be to implement Model Clauses. In Germany, these do not require the prior approval of the German data protection authorities.

- Companies (except for those located in Schleswig-Holstein) with BCRs and Model Clauses already in place can continue to use these mechanisms for the time being.

In any event, it is recommended that companies closely monitor further developments and seek individual legal advice. It is not beyond the realms of possibility that the German data protection authorities will eventually share the view of the authority in Schleswig-Holstein in finding transfers to the US on the basis of Model Clauses to also be unlawful. However, for the time being, companies should bear in mind that any unlawful transfers are punishable by the German data protection authorities with a fine of up to EUR 300,000 per individual case.

KEY CONTACTS

If you have any questions, or would like to know how this might affect your business, phone, or email these key contacts.



NICK PANTLIN
PARTNER, HEAD OF TMT & DIGITAL UK & EUROPE, LONDON
+44 20 7466 2570
Nick.Pantlin@hsf.com

MIRIAM EVERETT
PARTNER, LONDON
+44 20 7466 2378
Miriam.Everett@hsf.com

DUC TRAN
OF COUNSEL, LONDON
+44 20 7466 2954
Duc.Tran@hsf.com

LEGAL NOTICE