HERBERT SMITH FREEHILLS

SINKING THE SAFE HARBOUR: CJEU DECLARES US SAFE HARBOUR INVALID

07 October 2015 | London
Legal Briefings – By **Nick Pantlin** and **Miriam Everett**

On 6 October 2015, the Court of Justice of the European Union ("**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.

BUSINESS IMPACTS

Before the CJEU ruling, the US Safe Harbour was the means by which thousands of US-based organisations were able, in compliance with European data protection law, to receive and process personal data transferred from Europe into the United States (see "What is the US Safe Harbour?" below for further details).

- What does this mean today? – The CJEU ruling has effectively removed the Safe Harbour compliance route with immediate effect, meaning that "safe-harboured" organisations will now have to act quickly to find alternative ways to comply with the requirements of European data protection legislation. The CJEU did not provide any transitional period for compliance. Nor did it provide any guidance on how organisations should react in the immediate aftermath of the ruling, for example, by stopping transfers of personal data relying on the Safe Harbour mechanism until alternative arrangements are in place. However, the UK Information Commissioner has said that it recognises businesses will

need time to consider alternatives to the Safe Harbour, so it appears the message from the UK regulator at least is effectively "we're not going to come after you immediately". Organisations should therefore consider carefully the best steps to take before going ahead.

- What are the alternatives? – On a positive note, the US Safe Harbour is not the only way in which organisations are able to achieve data protection compliance. There are alternative methods provided for in the EU Data Protection Directive (the "**Directive**"). However, the number of alternatives is limited and some of them, such as individual consent, are extremely challenging from a business and commercial perspective. For example, how should an organisation go about collecting consents? What happens if some individuals do not give their consent? From a practical perspective, is it possible to only transfer some but not all data depending upon consent? Other more business-friendly alternatives, such as use of the so-called "Model Clauses" contracts or binding corporate rules, will take time to put into place, leaving organisations in a bit of a compliance no-man's land until they are able to get their house in order.

- What are the affected businesses? – Whilst a lot of the media attention from the case has focused on the impact it will have on large US tech organisations such as Facebook, Apple and Google, it is also worth noting that the judgment could have a significant practical effect on organisations which provide cloud or other online services hosted from the United States to customers in Europe. Providers who are able to offer EU-based hosting solutions may now find themselves at a competitive advantage (at least in the short-term). Other providers who have previously relied on the Safe Harbour to assure customers of their data protection compliance will need to put in place alternative compliance mechanisms. At the other end of the scale, some organisations, such as financial institutions, will be largely unaffected by the decision because they are unable to obtain the benefit of the Safe Harbour in any event (see "What is the US Safe Harbour?" below for further details).

- What should we expect next? – One of the next steps in the case will be for the Irish Data Protection Commissioner to act with respect to the original complaint against Facebook (see "Background to the Case" below for further details of the facts of the case). The outcome of that investigation may shed some light on how other regulators will approach the issue. It is also important to note that concerns about the Safe Harbour are not new. Negotiations have been taking place for more than two years between the European Commission and US authorities with a view to introducing a new, more privacy protective arrangement to replace the existing Safe Harbour. According to a statement issued by the UK Information Commissioner, those negotiations are well advanced. It is therefore possible that the CJEU ruling will provide a new impetus to those negotiations in order to produce an updated Safe Harbour fit for modern data protection and business purposes.

- What about the proposed data protection reforms? – Finally, the impact of this judgment is also likely to be taken into account in the current trilogue negotiations taking place between the European Commission, European Parliament and the Council with respect to the proposed new General Data Protection Regulation ("GDPR"). Although many aspects of the GDPR have been criticised for being overly bureaucratic, the proposed data transfer provisions appear to reflect a genuine attempt by the European institutions to

recognise the needs of a globalised economy. The proposed transfer provisions provide more scope for adequacy grounds to be established and make transfer restrictions easier to navigate. It is therefore possible that the GDPR could provide a silver lining for organisations looking to transfer data to the United States in the wake of the CJEU ruling.

BACKGROUND TO THE CASE

Maximillian Schrems, an Austrian law graduate and the plaintiff in the case, had been a Facebook user since 2008. As is the case with other subscribers residing in the EU, some or all of the data provided by Mr Schrems to Facebook was collected initially by Facebook's Irish subsidiary (Facebook Ireland) but then transferred to servers belonging to Facebook Inc and located in the United States, where it is processed and retained.

On 25 June 2013, Mr Schrems made a complaint to the Irish data protection authority (the "**Commissioner**") in which he asked the Commissioner to prohibit Facebook Ireland from transferring his personal data to the United States. He contended in his complaint that the law and practice in force in the United States did not ensure adequate protection of his personal data against the surveillance activities engaged in by the US public authorities. Mr Schrems referred in his complaint to the revelations made by Edward Snowden concerning the activities of the United States intelligence services.

The Irish data protection authority rejected the complaint on the grounds that the European Commission had found in the Safe Harbour Decision that the United States ensured an adequate level of protection.

The High Court of Ireland then referred the case to the CJEU to ascertain whether the Safe Harbour Decision has the effect of preventing a national supervisory data protection authority from investigating a complaint alleging that the United States does not ensure an adequate level of protection.

WHAT IS THE US SAFE HARBOUR?

The Directive provides that personal data may only be transferred outside of the EEA if the third country in question provides "adequate protection" for personal data.

In 2000, the European Commission issued the Safe Harbour Decision, in which it provided that the Safe Harbour Privacy Principles set out in the Annex to the Decision were considered to ensure an adequate level of protection for personal data being transferred to the United States.

Under the Safe Harbour, US organisations self-certify to the US Department of Commerce that they provide certain protections for personal data. Those protections are designed to ensure that organisations meet EU data protection requirements. Safe Harbour certifications are enforced by the Federal Trade Commission or the Department of Transportation in the United States as appropriate. However, the Safe Harbour is not available to some organisations, such as financial institutions, which are not subject to FTC jurisdiction.

The practical effect of the Safe Harbour is that personal data can be transferred from Europe to organisations in the Safe Harbour in compliance with the Directive and without additional measures being required.

As of 6 October 2015, the date of the CJEU ruling, there were 5475 organisations on the Safe Harbour list (although not all certifications were listed as "current").

THE JUDGMENT

The overall finding of the CJEU was that 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.

However, the CJEU also commented on the following other important and interesting aspects of the transfer of personal data pursuant to the Directive:

- Interaction of Commission Decisions with National Laws – The court confirmed that, until such time as a European Commission decision such as the Safe Harbour Decision is declared invalid, Member States and national supervisory authorities cannot adopt measures contrary to that decision.

- Scope of Powers of National Supervisory Authorities – The court confirmed that a European Commission decision such as the Safe Harbour Decision cannot eliminate or reduce the powers expressly accorded to national supervisory authorities by the Directive. Therefore, even if the European Commission has adopted a decision with respect to the adequate protection provided by a third country, the national supervisory authorities must be able to examine, with complete independence, any complaint regarding the transfer of personal data and whether such transfer complies with the requirements laid down by the Directive. If the national supervisory authorities were not able to do so, individuals whose personal data has been transferred would be denied their right to lodge with the national supervisory authorities a claim for the purpose of protecting their fundamental rights.

- On-going Validity of European Commission Decisions – The CJEU commented that it is incumbent upon the European Commission, after it has adopted a decision such as the Safe Harbour Decision, to check periodically whether the finding relating to the adequacy of the level of protection ensured by the third country in question is still factually and legally justified.

The CJEU further considered the Safe Harbour Decision itself and found it to be invalid. The judgment highlighted the following key flaws in the Safe Harbour Decision:

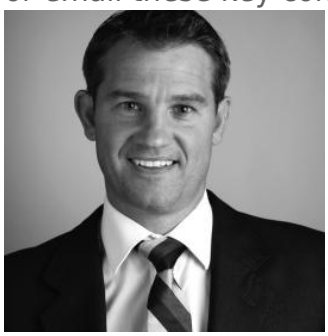
- Precedence – The Safe Harbour Decision provides that "national security, public interest, or law enforcement requirements" have primacy over the safe harbour principles. As a result, organisations receiving data under the Safe Harbour are required to disregard the safe harbour principles where they conflict with such requirements.

- Interference with Fundamental Rights – The issue of precedence highlighted above means that the Safe Harbour Decision enables interference, founded on national security and public interest requirements or on domestic legislation of the United States, with the fundamental rights of the persons whose personal data is or could be transferred from the European Union to the United States.

- Legal Remedies – The Safe Harbour Decision does not refer to the existence of effective legal remedies. The CJEU confirmed that legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection, as enshrined in the Charter of Fundamental Rights of the European Union. This has also been a key area of negotiation with respect to the recent EU-US Data Protection Umbrella Agreement.

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

LEGAL NOTICE

The contents of this publication are for reference purposes only and may not be current as at the date of accessing this publication. They do not constitute legal advice and should not be relied upon as such. Specific legal advice about your specific circumstances should always be sought separately before taking any action based on this publication.
