

To Our Clients and Friends

Memorandum



friedfrank.com

Schrems v Data Protection Commissioner: No “Safe Harbor” from the Oncoming Storm?

On 6 October 2015, the Court of Justice of the European Union (“CJEU”) handed down its decision in *Schrems v Data Protection Commissioner* in which Max Schrems challenged the legality of a decision by the Irish Data Protection Commissioner (“Irish DPC”) not to investigate his claims relating to the adequacy of the US-EU Safe Harbor scheme in light of the revelations made in 2013 by Edward Snowden. This memorandum sets out the background to the *Schrems* case, summarises the Advocate General’s Opinion and CJEU’s judgment, and analyses the potential wider implications for the “adequacy” standard for international data transfers under the European Data Protection Directive 95/46.

Schrems v Data Protection Commissioner: Background

Mr. Schrems was an Austrian law student and a privacy activist. Following the disclosure of the existence of the US PRISM program to the public, Mr. Schrems filed a complaint with the Irish Data Protection Commissioner objecting to the transfer by Facebook Ireland of his personal data to Facebook Inc. in the US. Facebook’s US data transfers were based on its membership of Safe Harbor, a self-regulatory scheme that is enforced by the US Federal Trade Commission. The basis of Mr. Schrems’s objection was that the Snowden revelations showed that the US could not ensure the adequate protection of his personal data.

The Irish DPC rejected Mr. Schrems’s complaint summarily on the basis of an earlier Commission Decision 2000/520 (the “Decision”), where the Commission considered that, under the Safe Harbor scheme, the US ensures an adequate level of protection of the personal data transferred from the EU. Mr. Schrems took the Irish DPC decision to the Irish High Court which, in turn, referred two questions to the CJEU. In summary, these asked whether national data protection authorities (“DPAs”) are absolutely bound by the Decision with regard to data transfers to the US, or whether they may conduct their own investigations into the adequacy of data protection in light of Articles 7, 8 and 47 of the EU Charter of Fundamental Rights.

The Advocate General’s Opinion

Advocate General Bott’s opinion on the questions referred by the Irish High Court was that the national DPAs, in this case the Irish DPC, were not bound by the Decision to dismiss Safe Harbor complaints summarily. Instead, national DPAs were required to undertake their own investigations and, if necessary, suspend transfers where the protections provided by the third country were deemed to be insufficient.

The Advocate General, however, raised *sua sponte* the issue of whether the Decision was valid under EU law at all. The Advocate General went on to conclude that the Decision was not valid under EU law,

principally, for two reasons: (i) that the limits to the Safe Harbor scheme on grounds of national security, public interest or law enforcement requirements were too widely drawn; and (ii) that the Safe Harbor scheme provided no means of independent review of apparent violations of data privacy rights. This resulted in a system which failed to ensure an adequate level of protection of the personal data transferred from the EU to the US, and likely violated EU citizens' human rights.

The CJEU's Judgment

The CJEU has, largely, adopted the approach of Advocate General Bott by holding that: (i) the existence of a Commission decision finding that a third country ensures an adequate level of protection of the personal data transferred cannot eliminate or even reduce the powers available to the national DPAs to exercise independent scrutiny; and (ii) that the Decision, in any event, was invalid.

In respect of the second point, the CJEU was critical of the fact that at no point had the Commission investigated whether the US provided an adequate level of protection of fundamental rights or of the rights under EU data protection law equivalent to those found within the EU, instead having restricted itself to an analysis of the Safe Harbor scheme. Without formally deciding whether Safe Harbor ensured an adequate level of protection, the CJEU observed that US public authorities are not subject to Safe Harbor, and that undertakings are bound to disregard, without limitation, the protective rules laid down by the Safe Harbor scheme where they conflict with certain national and public interests.

Commentary

As a preliminary point, it is important to highlight the limits of the CJEU's judgment. The judgment does not have the effect of invalidating the Safe Harbor scheme. Rather, the judgment holds that the Decision, which recognised Safe Harbor (and, therefore, the US) as providing an adequate level of protection for third country transfers is invalid with the knock-on effect that each national DPA must consider the level of adequacy of transfers to the US based upon the evidence presented. This could, potentially, have a wide-ranging impact on corporations and other entities, such as Facebook, who routinely transfer data from the EU to the US. But the effect of the judgment is not to prevent the transfer of personal data to the US altogether.

As the national DPAs are now required to decide, in effect individually, whether the US or, indeed, any other certified third country, has adopted a data protection regime which is EU-compliant, there is the possibility of a divergence of views on this point, with the result that Member States perceived as adopting a "weaker" approach to data protection could be seen as more favourable places for overseas corporations to base their operations. Alternatively, this may ultimately spell the end of the existing Safe Harbor scheme by a thousand cuts.

While Mr. Schrems may have performed a valuable exercise in bringing to the fore some important concerns, the jeopardising of Safe Harbor risks undermining the growing awareness and acceptance of EU data standards within the US. It is wistful to expect that EU data protection laws can be used as an effective tool to impose checks and balances on overseas states, and the decision of the CJEU risks creating uncertainty about the status of data transfer mechanisms, which are crucial organs of commerce.

The EU has established two other formal schemes for enabling data transfers outside of the EU (in addition to the obtaining of an individual data subject's consent), which may, following the CJEU's judgment, gain further traction amongst international corporations: Model Contract Clauses ("MCCs") and Binding Corporate Rules ("BCRs"). MCCs are standard contractual clauses recognised by the Commission as offering adequate safeguards so as to permit third country transfers. Currently, the Commission has authorised four such clauses. BCRs are rules applied by the company to third country transfers.

In conclusion, the CJEU's decision does not signify the "end" of Safe Harbor. Rather, it acts to redistribute the "balance of powers" within the EU from the Commission to national DPAs. Whether this will ultimately lead to national fragmentation or to the rebirth of a more robust Safe Harbor remains to be seen.

* * *

Authors:

James Kitching

Simon Camilleri

This memorandum is not intended to provide legal advice, and no legal or business decision should be based on its contents. If you have any questions about the contents of this memorandum, please call your regular Fried Frank contact or the attorney listed below:

Contact:

London

James Kitching

+44.20.7972.6295

james.kitching@friedfrank.com

