Last week, the Court of Justice of the European Union (CJEU) gave an important ruling which any business transferring personal data between the EU and the United States should know about — in particular those that make use of the “Safe Harbor” scheme for data transfer.

What is Safe Harbor?

Data protection standards vary across the world, and historically US law has not provided the same level of protection for personal data as exists in the EU. As a result, European data protection laws have typically required parties transferring data from the EU to the United States to obtain informed consent to the transfer of data and/or take purposive steps to safeguard it to European standards.

The Safe Harbor scheme was one way in which data could be lawfully transferred to the United States. It was set up in 2000 by a European Commission (Commission) finding that adequate protection for personal data would be provided by US undertakings that self-certified their adherence to a set of rules known as the Safe Harbor principles.

What’s happened?
However, in the Irish case of *Schrems v Data Protection Commissioner*, the CJEU has now decided that Safe Harbor is not, in fact, safe enough. In particular, the CJEU found that the Commission’s decision establishing the Safe Harbor scheme was flawed, and is therefore invalid.

More generally, the CJEU also confirmed that a Commission decision that a third country ensures an adequate level of protection for an individual’s personal data and related rights does not stop either (i) an individual bringing a claim in relation to the transfer of his personal data to that country; or (ii) a national data protection authority from investigating his complaint.

**Why does this matter?**

The judgment has wide ramifications for organisations based in or dealing with the United States which have previously relied on Safe Harbor as a basis for transferring personal data to the United States from the EU. Effectively, the CJEU’s ruling means that it will no longer be possible to rely on Safe Harbor to do this.

More specifically, Mr. Schrems will be able to proceed with his complaint about the transfer of his personal data by Facebook from its Irish subsidiary to servers in the United States (where it is allegedly subject to large-scale, indiscriminate surveillance by US authorities that does not comply with EU data protection standards). It will be interesting to see how the Irish authorities deal with this.

**Is this a surprise?**

Yes and no. There has been notable discontent with Safe Harbor in recent years, particularly around its reliance on self-certification rather than external enforcement of the required standards. Indeed, representatives of the EU and US governments are currently holding talks about a potential replacement scheme.

However, this issue has been called into sharp focus by the decision in Schrems. The CJEU quite deliberately goes beyond the case at hand to address wider concerns around Safe Harbor in a way that could potentially leave businesses with a US connection exposed.

**So what does it mean for my business?**

Don’t panic. The relevant authorities appreciate that the position has changed relatively quickly, and we do not expect to see overnight enforcement action against businesses that have previously relied on Safe Harbor. In the United Kingdom, the Information Commissioner’s Office has indicated that it is preparing guidance on the available options for EU-US data transfer, and we expect other European data protection authorities to follow suit.

Similarly, your business may not actually rely on Safe Harbor that much — or at all. There are other ways in which you can record your intention to safeguard personal data transferred to the United States which, as matters currently stand, satisfy the relevant European authorities. For example, Binding Corporate Rules (BCRs) can be put in place to signify a business-wide endeavour to safeguard data, contracting
parties can sign up to pre-approved “model clauses” confirming that data will be processed in line with EU standards, and informed data subject consent to the transfer of their personal data to the United States provides a further line of defence.

As a first step, we therefore recommend that you carry out a risk assessment, to:

- Identify what sort of personal data, if any, you transfer from the EU to the United States. For example, does the data relate to customers or employees? How sensitive is it? What is the purpose of the transfer, and who is it being transferred to?

- Analyse where, and how far, you rely on Safe Harbor to lawfully effect any such data transfers (whether to your other group companies, or external service providers).

- Consider whether your Safe Harbor transfers are already covered by another lawful avenue for data transfer (for example, with the express consent of the data subject).

This should help you establish how much of an issue the loss of Safe Harbor poses to your business, if any. If it is necessary to put alternative measures in place, you can then consider which other lawful avenue(s) for transferring personal data from the EU to the United States might be appropriate.

The route you choose will depend very much on the nature of your business and the data transfers you need to make. For example, an organisation that primarily transfers data between group companies, and has previously operated in compliance with Safe Harbor standards, might well be able to migrate to having BCRs fairly smoothly (although in all likelihood a “multi-tiered” combination of approaches will be appropriate).

Are any other changes likely to occur?

At a high level, it is hoped that the ongoing governmental talks might lead to a replacement for the Safe Harbor scheme sooner rather than later. In the meantime, as mentioned above, other avenues for lawful EU-US data transfer are available (and even though some of these, like BCRs and model clauses, potentially suffer from similar concerns around US government surveillance, they are yet to be scrutinised in the same way as Safe Harbor, and so currently remain valid options).

The key step now is to engage with this issue, and assess the level of risk (if any) it poses to your business, and how you might react.

© 2019 McDermott Will & Emery