Milbank

9 October 2015

CONTACT

Joel Harrison
Partner
+44-20-7615-3051
jharrison@milbank.com

Sean Keaton
Partner
+44-20-7615-3078
skeaton@milbank.com

Laurence Jacobs
Partner
+44-20-7615-3096
ljacobs@milbank.com

Nicholas Smith
Partner
+1-212-530-5275
nsmith@milbank.com

Data Privacy and Information Security Group Client Alert: Safe Harbor Briefing Note

This note sets out:

- information about the effects of the CJEU judgment invalidating the Safe Harbor;
- alternatives to the Safe Harbor that may be available; and
- recommended next steps.

1. WHAT ARE THE EFFECTS OF THE CJEU JUDGMENT?

On 6 October 2015, the CJEU found the EU/US Safe Harbor agreement to be invalid in the case of *Schrems v Data Protection Commissioner*. This means that the Safe Harbor can no longer be relied upon by companies in the EU that need to transfer personal data to the US (whether to other group companies, service providers or other third parties).

Whilst it is unlikely that EU data protection authorities (DPAs) will start taking enforcement action immediately against companies that have been relying on the Safe Harbor (given the large number of EU companies that have been doing so, and that until the CJEU's judgment the Safe Harbor was formally recognised as a valid basis for transferring data to the US), it will be important to show the DPAs that prompt action is being taken to implement alternative measures to enable transfers to the US to continue in compliance with EU law. We would not rule out the possibility that the DPAs will start taking enforcement action against companies that continue to transfer data to the US without implementing alternative measures once they have had an opportunity to put these measures in place.

2. WHAT ARE THE ALTERNATIVES TO THE SAFE HARBOR?

There are several alternatives to the Safe Harbor, which are regularly used for transfers from the EU to other non-EU countries. The principal alternative mechanisms are:

- Using standard contracts approved by the European Commission (known as 'standard contractual clauses' or 'model clauses'). These can be used for transfers to US-based service providers (such as outsourcing and cloud computing providers), as well as for transfers to US companies that use the data for their own purposes. There are two forms of standard contractual clauses – controller-to-processor (C2P), for transfers to service providers, and controller-to-controller (C2C), for transfers to US companies that use the data for their own purposes. It is important for companies implementing the standard contractual clauses to note that they contain real obligations that must be complied with in practice; they cannot simply be signed and 'put in a drawer', as often happens.

- Obtaining consent from data subjects to their data being transferred to the US. This will not, however, be appropriate in all circumstances, and should be considered only if other options are not available.

- Putting in place Binding Corporate Rules (formal arrangements for intra-group transfers). This is appropriate only for transfers to other group companies, and cannot be used for transfers to third parties.

Which of these is the most appropriate will depend on the type of data transfer, and not all of them may be available in all cases. In most cases, companies relying on the Safe Harbor for data transfers to the US fall into one of the following five categories:

- **Companies in the EU transferring data to US-based service providers (such as cloud computing providers) under the Safe Harbor**. In most cases, the Safe Harbor can be replaced with standard contractual clauses (usually using the C2P form). It is important to note that a number of major US cloud providers, such as Microsoft, Google and Amazon, *already* use standard contractual clauses despite also being members of the Safe Harbor, meaning that there is already an alternative mechanism in place to allow the transfers to continue. For service providers that have been relying *solely* on the Safe Harbor, standard contractual clauses can be put in place.

- **Companies transferring data intra-group from the EU to the US under the Safe Harbor**. For intra-group transfers to US companies, standard contractual clauses will generally be the most appropriate short-term measure. The standard contractual clauses will follow either the C2C form,

where data is shared with group companies in the US for their own purposes, or the C2P form, where a group company in the US acts as service provider on behalf of group companies in the EU. Companies should also evaluate the possibility of implementing Binding Corporate Rules (BCRs), which offer a more flexible solution for intra-group transfers (to the US and elsewhere); however, it is important to note that implementation of BCRs is a substantial undertaking, with most BCR projects taking at least 18 months to complete.

- **Companies in the EU that share personal data with third parties in the US under the Safe Harbor**. These transfers can generally be covered by standard contractual clauses (usually the C2C form).

- **Companies in the US that receive personal data from third parties in the EU under the Safe Harbor**. These transfers can generally be covered by standard contractual clauses (C2C or C2P, as appropriate).

- **Companies in the US that collect data directly from EU data subjects under the Safe Harbor**. These companies have a few options available:

    - One is to put in place standard contractual clauses (usually using the C2C form) with an EU group company. However, that may not be appropriate in all cases, and it may require broader changes to the way in which the company operates (i.e. the data would have to be genuinely collected by the EU group company so that the contract reflects how data flows actually operate). We would expect DPAs to scrutinise carefully arrangements under which a US company has simply incorporated an EU subsidiary solely for purposes of having an EU-based counterparty to enter into the standard contractual clauses.

    - Another option is to rely on data subjects' consent to their data being transferred to the US. This is a valid option provided that the consent is freely given and the wording of the consent is sufficiently clear, but there are some data subjects (such as employees) for whom it will not be appropriate. Another important point is that consent can be withdrawn subsequently, so there would need to be a back-up plan for those individuals who withdraw consent. (In the case of online companies, for example, users who subsequently withdraw consent may simply have their accounts deleted.)

    - In some cases companies may be able to rely on the transfer being necessary for performance of a contract with the data subject. This will require consideration on a case-by-case basis.

3. WHAT ARE THE NEXT STEPS?

The steps that each company will need to take depend on how the Safe Harbor is being used by that company, and in particular whether the company has been transferring data or receiving data (or both) in reliance on the Safe Harbor. Companies will need to conduct some initial data gathering in order to assess what their alternative options are.

We suggest assessing this both from the perspective of (a) companies in the US that are currently members of the Safe Harbor and (b) companies in the EU that transfer data to companies in the US under the Safe Harbor.

(a) Identify group companies which are existing Safe Harbor members

- Corporate groups will need to identify which group companies are Safe Harbor members. If the group doesn't have an internal record of its Safe Harbor members, it can check the online Safe Harbor list (available at https://safeharbor.export.gov/list.aspx) to determine which group companies are members of the Safe Harbor.
- For each company identified as a Safe Harbor member, the following needs to be identified:
    - Which personal data does it receive from the EU?
    - Who are the data subjects?
    - How does it receive that data – directly from data subjects or from other companies? If from other companies, who are they?
    - For what purposes does the company receive the data? In particular, does it use the data for its own purposes or is it merely a service provider on behalf of other companies?
    - Does the company transfer the data to any other companies? If so, to whom and where are those companies located?

(b) Identify transfers from EU group companies to the US

(i) Transfers to Service providers

- EU companies should identify which of their service providers rely on the Safe Harbor. This can be checked against the Safe Harbor list. However, it is important to note that the fact that a provider appears on the Safe Harbor list does not necessarily mean that remedial action is required. For example, the

provider may also use other mechanisms for transfers to the US (such as standard contractual clauses), rather than relying solely on the Safe Harbor. Similarly, some providers are Safe Harbor members but service some or all of their EU customers from facilities in the EU.

- Once a company has identified which of its service providers was relying solely on the Safe Harbor to provide services to the company, the company will need to ascertain the types of data processed by each provider, the categories of data subject and the nature of the services provided.

- These providers should then be contacted and informed that standard contractual clauses should be put in place as a priority. A number of those service providers may already have prepared completed sets of clauses reflecting the data that they process as standard, in which case those should be reviewed; in other cases, the company can either request the provider to prepare a set of clauses or prepare its own.

- We expect that a number of US providers will act proactively and contact their customers in the EU to address their concerns.

(ii) Transfers to other US companies

Some companies in the EU may also be sharing data with other third parties in the US (such as collaboration partners) under the Safe Harbor. This type of data sharing may be more difficult to identify and the full range of group activities and business collaborations should be considered carefully to identify the range of third party data sharing arrangements.

DATA PRIVACY AND INFORMATION SECURITY GROUP

Please feel free to discuss any aspects of this Client Alert with your regular Milbank contacts or any of the members of our Data Privacy and Information Security Group.

If you would like copies of our other Client Alerts, please visit our website at www.milbank.com and choose “Client Alerts” under “News.”

LONDON
10 Gresham Street London EC2V 7JD

Joel Harrison	jharrison@milbank.com	+44-20-7615-3051
Sean Keaton	skeaton@milbank.com	+44-20-7615-3078
Laurence Jacobs	ljacobs@milbank.com	+44-20-7615-3096

NEW YORK
28 Liberty Street, New York, NY 10005

Nicholas Smith	nsmith@milbank.com	+1-212-530-5275