CAREY OLSEN

Safe Harbour in a storm?

Service area / Cybersecurity and Data Protection
Location / Group
Date / October 2015

Europe's highest court, The Court of Justice of the European Union ("CJEU") has declared the EU-US Safe Harbour Agreement ("Safe Harbour") to be invalid as a mechanism to legitimise personal data transfers from the EU to the US.

The decision is unsurprising, given the recent release of Advocate General Bot's Opinion to that effect and the unrest at the Snowden revelations regarding government surveillance of personal data. However, it leaves businesses placing reliance on Safe Harbour in difficulties, as such data transfers are now unlawful. The decision affects all businesses moving employee, customer or other personal data between the EU and the US, placing reliance on Safe Harbour. This includes those using third party providers or group companies to host and process data for core HR, marketing, administration or compliance purposes. Even if the data is not stored in the US, if teams based there can access the data, then there may be an issue.

Background

Safe Harbour is a self-certification scheme created by the European Commission and the US Department of Commerce in order to allow US-based companies to overcome the restrictions placed on the export of data from the EU, in particular the EU requirement to ensure "adequate protection" for personal data being transferred from the EU to the US[1].

Those in the US wishing to import data from a variety of European countries could in turn benefit from applying a "blanket" standard to facilitate transfers from a variety of EU countries. Without Safe Harbour (or one of the other approved measures) being in place, the transfer would be banned, as the US is not deemed "adequate" for crossborder data transfers from an EU perspective.

There has been increased scrutiny of tech giants (such as Facebook) and their policies, following the Snowden revelations. The EU is also in the process of streamlining and updating its data protection rules and the negotiations have brought into focus the question as to whether Safe Harbour operates to protect personal data effectively. There has been a growing belief that US companies aren't meeting the standards that are being claimed, which hasn't been helped by criticisms from EU regulators and the prosecutions in the US of companies whose self-certification proved to be defective.

Schrems v Facebook

The case was brought by Maximilian Schrems, a Facebook user and privacy campaigner concerned by the outfall from the Snowden revelations, who argued that Safe Harbour didn't offer adequate protection against surveillance by the US authorities. As Facebook's EU headquarters are located in Ireland, the complaint was made to the Irish data protection authority ("Irish DPA").

1 Schrems –v- Facebook (Schrems C-362/14).

The Irish DPA rejected the complaint on the basis that the Commission decision of 26 July 2000 confirmed that under Safe Harbour, the US ensures an adequate level of protection of the personal data transferred and therefore it could not progress the complaint further. Schrems pursued the complaint to the Irish High Court, which referred two questions to the CJEU.

The questions were:

- Can a Data Protection Authority ("DPA") investigate on a Safe Harbour issue?
- Is Safe Harbour invalid?

Despite being legally bound by the Commission decision on the operation of Safe Harbour, the CJEU ruled that DPAs nevertheless retain power (and indeed have a duty) to investigate complaints independently. It is vital that DPAs are able to investigate and ban data exports where appropriate; the powers of the DPAs could not be fettered or eliminated by virtue of the Commission decision. The right to the protection of personal data was guaranteed by the Charter of Fundamental Rights and the DPAs were established to monitor the protection of those rights.

The Court also held that the Safe Harbour scheme is invalid. US law allows for the large scale collection of personal data without effective judicial control. Further, the public authorities in the US are not subject to Safe Harbour and US entities are bound to disregard the protective measures contained in Safe Harbour where they conflict with US law enforcement, national security or public interests.

Safe Harbour was considered by the Court to enable the interference by US authorities with the fundamental rights of individuals (including the right to respect for private life). Noting the derogations from privacy protection and the absence of methods of redress (in cases of misuse) in the US, the Court held that the Safe Harbour scheme doesn't meet the guarantees and safeguards contained in the EU legislation or the Charter of Fundamental Rights.

As a consequence, the case has been referred back to the Irish DPA to examine the complaint and to determine whether the transfer of data of Facebook's European subscribers should be suspended on the grounds that the US does not afford an adequate level of protection of personal data.

Whilst in some ways the decision is a sea change, many businesses are already utilising alternative methods to legitimise data transfers to the US. Alternative procedures should now be considered as a priority.

The Binding Corporate Rules ("BCR") scheme offers a safe zone to permit multiple transfers within group companies, utilising the mutual recognition system. It is also expressly recognised in the draft Regulation (due for possible implementation in the EU in 2016). Otherwise, the alternatives are to have contracts in place to cover the various transfers taking place, incorporating the EU "model clauses", or to try to seek approval from the local data protection authority for specific transfers. However, even model contracts do not prevent US authorities "overreaching", contrary to the EU concept of privacy.

Negotiations on the reform to Safe Harbour have been ongoing between the EU and the US for some time now and it is not clear how this ruling will impact on those negotiations. However, it is understood that the Commission will continue to renegotiate Safe Harbour and the issues outlined above will need urgent consideration. In the interim, the use of alternative methods should be investigated, or the transfers stopped. This approach is consistent with the guidance issued by the Office of the Data Protection Commissioner in Guernsey and the Office of the Information Commissioner in Jersey.

Whilst the case concerns an agreement between the EU and the US, the Guernsey and Jersey Data Protection legislation is based on the EU legislation and businesses looking to transfer data to the US are similarly obliged to consider the "adequacy" provisions and implement measures such as reliance on Safe Harbour, BCR or model contract clauses to satisfy themselves that the transfer can proceed. Guernsey and Jersey businesses therefore face similar considerations to those based in the EU in terms of their approach to this ruling.

At present neither the Cayman Islands nor the British Virgin Islands ("BVI") have equivalent data protection regimes to the EU, Guernsey or Jersey. Even so, this development may still be of relevance to businesses in Cayman or the BVI if they have a presence in one of the jurisdictions which is caught by the ruling or to which they transfer data.

Impact

- This is a big issue for international businesses transferring data on a cross-border basis and relying on Safe Harbour.
- Those transferring data from the EU to the US and relying on Safe Harbour will need to find replacement mechanisms as soon as possible.
- May lead to a fragmentation in approach within the EU, as individual DPAs adopt differing approaches to the question of "adequacy", leading to further uncertainty and increased cost at a time when the EU is looking to harmonise and standardise approaches across the EU and on a transatlantic basis.
- US-based businesses providing certification under Safe Harbour will now need to provide alternative guarantees for their European customers in order to engage their services lawfully.
- The initial response from the authorities suggests that they recognise that adjustments to comply with the decision will take a little time, so absent any data breaches, immediate enforcement action seems unlikely.

Continued

Next steps

- Assess which data transfers are affected and prioritise essential transfers, determining how best to legitimise them by the use of alternative mechanisms. These may include the use of express contractual provisions, BCR or authorisation from the Data Protection Commissioner.
- Review contractual documentation with service providers to check references to Safe Harbour and identify and implement alternative mechanisms as appropriate. This should be done not only on existing agreements, but be a consideration in relation to any new agreements.
- Remember that contractual clauses alone may not be enough – assess the service provider's ability to provide secure storage and transfer of data, alongside a more general assessment to check they have appropriate data processing procedures in place.
- Don't forget to consider and review any Privacy Policies that exist within your business to ensure appropriate cross-referencing to the alternative methods adopted is inserted.

FIND US

Rodus Building
PO Box 3093
Road Town
Tortola VG1110
British Virgin Islands

T +1 284 394 4030
F +1 284 494 4155
E bvi@careyolsen.com

PO Box 10008
Willow House
Cricket Square
Grand Cayman KY1-1001
Cayman Islands

T +1 345 749 2000
F +44 1481 739081
E cayman@careyolsen.com

PO Box 98
Carey House
Les Banques
St Peter Port
Guernsey GY1 4BZ
Channel Islands

T +44 (0)1481 727272
F +44 (0)1481 711052
E guernsey@careyolsen.com

47 Esplanade
St Helier
Jersey JE1 0BD
Channel Islands

T +44 (0)1534 888900
F +44 (0)1534 887744
E jersey@careyolsen.com

FOLLOW US

View our cybersecurity and data protection services at careyolsen.com