Jisc – Safe Harbour

A note for institutions 12 October 2015

NOTE ON THE COURT OF JUSTICE OF THE EUROPEAN UNION'S JUDGMENT ON 'SAFE HARBOUR' ARRANGEMENTS FOR THE TRANSFER OF PERSONAL DATA FROM THE EEA TO THE USA

KEY POINTS

- Safe Harbour Agreement no longer a valid basis for EEA to US transfers of personal data
- Organisations considering the use of other mechanisms, such as Model Clauses and BCRs
- Possible that such alternative mechanisms will be undermined by the same concerns regarding the activities of US intelligence agencies as influenced the decision of the court on the Safe Harbour Agreement
- Institutions need to review their arrangements with US service providers including for cloud services
- Jisc will review arrangements with Jisc cloud partners - Microsoft, Google and AWS
- Guidance expected from the ICO and European data protection authorities in the near future with ICO stating that it understands that institutions will need time to transition to new arrangements

INTRODUCTION

On 6 October 2015 the Court of Justice of the European Union (**CJEU)** ruled that the 'Safe Harbour' Agreement, which facilitates the flow of personal data from the European Economic Area to the United States of America, is invalid.[1] Jisc has prepared this note to help UK education and research institutions (**Institutions**) to understand the judgment and its potential impact.

This note does not constitute legal advice. It provides a summary of some of the main data protection issues which arise from the CJEU's judgment. Institutions should seek their own legal advice regarding their compliance with any applicable data protection legislation including as regards the transfer of personal data controlled by them to the United States of America.

[1] Available at: http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=81685

RELEVANT LEGAL OBLIGATIONS

A key principle of the EU's Data Protection Directive (which was implemented in the UK by the Data Protection Act 1998) places limits on the ability of Institutions to transfer personal data outside of the EEA. Such transfers are only permitted where "adequate protections" are in place, or where the destination country has been pre-approved by the European Commission (**Commission**) as having adequate data protection laws.

Although the US has not been designated as meeting these 'adequacy' requirements, the Commission and the US agreed the Safe Harbour Agreement in 2000. The Safe Harbour Agreement facilitates the transfer of personal data from the EU to the US. Under it, US organisations self-certified compliance with the requirements of the Safe Harbour Agreement, which enabled them to meet the 'adequacy' standards outlined in the Directive.

THE CJEU'S JUDGMENT

The CJEU's judgment came in a case referred to it from the High Court of Ireland in connection with a complaint raised by a privacy group, 'Europe v Facebook' about the way Ireland's data protection authority handled concerns it had raised with regard to Facebook's data transfer arrangements.

The Irish data protection authority argued that it was bound by the Commission's decision that the Safe Harbour Agreement adhered to EU data protection laws. On that basis it had declined to investigate the complaint.

The CJEU has now ruled that:

- the Safe Harbour Agreement does not provide adequate protection of personal data, as required by the Directive. In particular, it said that there are insufficient restrictions on how the US authorities can use personal data transferred from the US to the EU, and on that basis the Safe Harbour Agreement did not respect privacy in the way required by the Directive. The CJEU's concerns over the ability of US authorities to access personal data is of particular note. Such concerns might be considered equally relevant in any challenge over transfers of personal data to the US under other legal constructs, such as binding corporate rules or the EU Model Clauses;

- national data protection authorities (such as the Irish data protection authority, and the UK Information Commissioner's Office ("**ICO**")) are not bound by the Safe Harbour Agreement; and

- national data protection authorities are free to investigate complaints about data transfers when new issues come to light (but the CJEU will still have the final say on whether decisions taken by the Commission in relation to data transfers are valid or not).

EU MODEL CLAUSES AND BCRs

The judgment means that many organisations which currently rely on the Safe Harbour Agreement to transfer personal data to the US will need to find other legal mechanisms to do so. The two most commonly used other mechanisms are:

The EU Model Clauses

Organisations have been able to use the EU Model Clauses since the EU Commission created them in 2001. The Clauses were created by the Commission in 2001 and can be used to govern the transfers of personal data outside of the EEA and to meet the 'adequacy' standards outlined in the Directive.

Sometimes organisations make changes to the Model Clauses. This may have an adverse impact on compliance. The Article 29 Working Party (the advisory body comprising representatives from each of the 28 EU data protection authorities) has previously stated that amendments of this nature may be acceptable in principle. However, the ICO

has indicated that any amendments or inconsistent provisions might in certain circumstances render the model clauses non-compliant.

Binding Corporate Rules (BCRs)

Companies can implement binding corporate rules for data transfers to other members of their company group who are based in non-EEA countries. BCRs involve organisations committing to a code of conduct for handling and protecting personal data within their group in a way that complies with EU data protection law. This mechanism only applies to intra-group transfers. It has limited applicability as it cannot be used to enable 'customer > IT service provider' transfers of personal data.

KEY QUESTIONS ABOUT THE JUDGMENT

What is the ICO's view?

The ICO has stated that, "*the judgment means that businesses that use Safe Harbor will need to review how they ensure that data transferred to the US is transferred in line with the law. We recognise that it will take them some time for them to do this. It is important to bear in mind that the Safe Harbor is not the only basis on which transfers of personal data to the US can be made. Many transfers already take place based on different provisions.*"

Institutions should note, in particular, that:

- the ICO will be issuing guidance for organisations over the coming weeks, after consulting with other EU data protection authorities; and
- the ICO has made clear that it wants data controllers to have time to transition to other mechanisms of transferring personal data to the US.

Any ICO guidance will help Institutions to develop their approach to dealing with this issue. In the meantime, Institutions should bear in mind that, whilst the judgment is limited to the Safe Harbour Agreement, mechanisms such as the EU Model Clauses and BCRs could come in for scrutiny for similar reasons, i.e. concerns regarding the access the US authorities may have to personal data that is transferred to the US.

What action should Institutions take if they have service providers which use Safe Harbour?

Institutions should review arrangements with US service providers. If service providers or business partners are relying on the Safe Harbour Agreement to validate the transfer of personal data to the US, Institutions should ask for an update from them on how they will ensure compliance with EU data protection laws on the transfer of data outside of the EEA. Institutions should consider whether the measures are sufficient to ensure such transfers are lawful. This will not be an easy assessment to make given the concerns expressed by the CJEU on the surveillance activities undertaken by the US authorities.

What additional guidance can Institutions expect on the ruling in the coming days/weeks?

The Article 29 Working Party will meet in the near future to discuss the implications of the judgment[2]. It is hoped that they will provide guidance on the practical application of the judgment as soon as possible.

The ICO will issue its own guidance in the coming weeks. Institutions should monitor ICO press releases for announcements and guidance.

Will there be a new version of 'Safe Harbour' in the future?

Institutions should note that, following the Edward Snowden revelations on the surveillance activities of US intelligence agencies, the EU Commission has been in negotiations with the US over a new 'Safe Harbour'-style regime. The pace of progress on this regime is dependent on how effectively some of the issues identified in this CJEU decisions can be addressed by the US authorities. It is not expected that negotiations will conclude any time soon.

How has the technology sector responded to the ruling?

Trade body the **Internet Association** (which has members such as Google, Amazon, Facebook and Uber) stated that the judgment could present "significant challenges" for small businesses and consumers.[3]

Microsoft has moved to reassure its cloud customers about the impact of the ruling.[4] Its President and chief legal officer Brad Smith stated that "some customers may ask if this means that they will no longer be able to transfer their customer data from the European Union to the United States. For Microsoft's enterprise cloud customers, we believe the clear answer is that yes they can continue to transfer data by relying on additional steps and legal safeguards we have put in place." Jisc assumes this to be a reference to Microsoft's use of the EU Model Clauses.

What mechanisms do Microsoft, Google and Amazon use for data transfers outside of the EEA?

Jisc appreciates that Institutions who use cloud computing solutions will be particularly keen to understand how the judgment affects arrangements they may already have in place with cloud providers.

Jisc is engaging directly with the cloud providers with whom it deals to understand how they propose to address any concerns raised by the decision of the CJEU. Jisc will report the outcomes of such discussions to Institutions in due course. In the meantime, the table below sets out the approaches commonly adopted by Microsoft, Google and Amazon in connection with their cloud offerings. Please note that we have prepared this table in the context of terms/agreements reviewed previously by Jisc in procuring cloud services (as indicated next to the cloud provider) and does not necessarily represent the position across *all* terms/agreements of those cloud providers across *all* their different product suites:

[2]Available at: http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151006_wp29_press_release_on_safe_harbor.pdf
[3] Available at: http://internetassociation.org/100615safeharbor/.
[4] Available at http://blogs.microsoft.com/on-the-issues/2015/10/06/a-message-to-our-customers-about-eu-us-safe-harbor/.

Service Provider	Safe Harbour?	EU Model Clauses?	Have the EU Model Clauses been modified?
Microsoft (*Online Services Terms*)	Microsoft's Online Services Terms commit to abide by the Safe Harbour Agreement. In addition, for the Online Services which are subject to Microsoft's 'Data Processing Terms' (note this does not cover *all* Online Services) Microsoft states that all transfers of personal data will be covered by the EU Model Clauses.		Yes
Google (*Google Apps for Education*)	No	Yes	Yes
Amazon Web Services (*various AWS terms*)	Amazon Web Services has previously relied on both Safe Harbour and the EU Model Clauses, depending on the particular transaction. Institutions should check the particular terms of their own contracts with Amazon Web Services in that regard.		N/A (case by case basis)