Still a 'safe' Harbor? — implications of Schrems v DPC

Davinia Brennan, Associate in the Litigation and Dispute Resolution department at A&L Goodbody, discusses the future of Safe Harbor in light of ongoing scrutiny as Schrems v Data Protection Commissioner unfolds

The Safe Harbor regime is back in the spotlight following the Irish High Court decision in *Schrems v Data Protection Commissioner* ('DPC') [2014] IEHC 310 to refer to the Court of Justice of the European Union ('CJEU') questions concerning the extent to which national data protection authorities ('DPAs') are bound by the EU Commission's decision on the adequacy of Safe Harbor. The referral serves as a warning to organisations to be wary of relying solely on the Safe Harbor regime for transferring data from the EU to the US.

This article discusses the weaknesses of the Safe Harbor regime, the recommendations by the European Commission for strengthening the regime, and the findings of the Irish court in the *Schrems* case.

Safe Harbor — a recap

Over the past 14 years, Safe Harbor has served as an important mechanism for transferring data for commercial purposes from the EU to the US. As regular readers are aware, the Data Protection Directive (1995/46/EC) provides that personal data may only be transferred to countries outside of the European Economic Area ('EEA') which provide an adequate level of data protection.

The Commission Decision 2000/520/EC ('the Safe Harbor Decision') provides a legal basis for transfers of personal data from the EU to companies established in the US which adhere to the Safe Harbor privacy principles, and ensure an adequate level of data protection. US member companies must self-certify annually to the US Department of Commerce that they will comply with the seven Safe Harbor privacy principles (concerning notice; choice; onward transfer; access; security; data integrity and enforcement).

Why is Safe Harbor under scrutiny?

There has been increasing concern in Europe about the safety of data transferred to the US under the current Safe Harbor regime, particularly since the Edward Snowden revelations. (In June 2013, Edward Snowden leaked documents which revealed the existence of the PRISM surveillance programme, which allegedly allows the US National Security Agency ('NSA') to access personal data relating to EU citizens held by US-based internet companies.)

Whilst the Safe Harbor Decision contains an exemption to the data protection rules where necessary on the grounds of national security, the question has arisen as to whether the mass surveillance of personal data by US authorities is necessary to meet the interests of national security. The breadth of access of US authorities to EU citizens' data, combined with the fact that non-US persons do not have any legal right to redress in the US, has led to growing concern about the level of data protection afforded by Safe Harbor. In particular, criticisms have centred on the regime's reliance on self-certification and the lack of enforcement, which has resulted in a number of US companies failing to comply with the Safe Harbor principles.

Whilst DPAs may, under Article 3 of the Safe Harbor Decision, suspend data transfers to certified companies in specific circumstances (such as in cases where there is a substantial likelihood that the Safe Harbor principles are being violated) there do not appear to have been any suspensions to date. However, in response to the Snowden revelations, the German Data Protection Authorities have indicated they will examine whether data transfers on the basis of the Safe Harbor should be suspended.

The European Commission ('Commission') has warned that such suspensions, taken at national level, 'could create differences in coverage, which means that Safe Harbor would cease to be a core mechanism for the transfer of personal data between the EU and the US'.

Policing Safe Harbor — does the FTC lack muscle?

In an effort to assuage criticism concerning lack of enforcement, the US Federal Trade Commission

('FTC') recently took its largest-ever enforcement action against twelve companies that allegedly falsely represented that they were current certified members of Safe Harbor, when their certificates had in fact expired. Whilst it is encouraging that the FTC has stepped up its enforcement of the Safe Harbor regime, further policing of the principles is necessary in order to allay the concerns of EU citizens and DPAs.

The US Attorney General's recent announcement that the Obama administration will ask Congress to enact legislation granting EU citizens the right to bring claims in US courts under US privacy laws if they believe their personal data have been misused further demonstrates the efforts being taken by the US authorities to rebuild the EU's trust in data transfers to the US, and to preserve Safe Harbor.

Despite these efforts, it would be sensible for those companies relying solely on Safe Harbor to legitimise the transatlantic data exchanges, to actively check the US company importing the data is listed as a current member of the Safe Harbor regime, and to carry out due diligence to ensure it is complying with the Safe Harbor principles.

"Despite these efforts, it would be sensible for those companies relying solely on Safe Harbor to legitimise the transatlantic data exchanges, to actively check the US company importing the data is listed as a current member of the Safe Harbor regime, and to carry out due diligence to ensure it is complying with the Safe Harbor principles."

Improving the safety of Safe Harbor

The Commission has the responsibility for reviewing the Safe Harbor decision, and may maintain it, adapt it, suspend it or revoke it, in light of experience with its implementation.

The Commission has indicated that given the weaknesses in the current Safe Harbor regime, it cannot be maintained. However, as its revocation would adversely affect the interests of its 3,000 plus member companies, the Commission considers that the regime should be strengthened. On 27th November 2013, the Commission made thirteen recommendations which aim to make Safe Harbor safer and maintain the continuity of data flows between the EU and US.

The recommendations address issues such as improving transparency, redress, actively enforcing the Safe Harbor principles, and clarifying the scope of the national security exemption which allows US authorities to access EU personal data. Previous European Commission Vice-President, Viviane Reding, stated on 6th June 2014, that the US Department of Commerce has agreed to 12 of the 13 recommendations.

It seems that negotiators are currently stuck on the point that US authorities should only be allowed to access data covered by Safe Harbor to the extent that is strictly necessary or proportionate to the protection of national security. This is arguably the most important proposed revision of Safe Harbor in light of the Snowden revelations, as it effectively requires the US authorities to restrict their electronic data surveillance practices. Agreement on this point would undoubtedly help to reassure EU citizens and DPAs that their data will be safe from unnecessary disclosure, and would increase trust again in the flow of data from the EU to the US.

Alternatives to Safe Harbor

Safe Harbor is not the only means of ensuring that data are adequately protected when transferred out of the EEA. Alternative methods include the Model Contractual Clauses or Binding Corporate Rules ('BCRs'). Most international companies use the Model Contractual Clauses approved by the European Commission to transfer personal data outside of the EEA. For transfers within a corporate group, but outside of the EEA, BCRs can be used. The latter tend to be less popular on the basis that they need to be pre-approved by DPAs.

Irrespective of whether Safe Harbor, the Model Contractual Clauses or BCRs are used to transfer data from the EU to the US, under US laws, US authorities can force access to US companies' data stored in the EU, even though such disclosure is in breach of EU data protection laws. This was demonstrated recently by the US Court Order requiring Microsoft in the US, to produce email content stored on servers in Dublin.

The draft Data Protection Regulation — are sunset clauses a solution?

In January 2012, the European Commission published a draft Data Protection Regulation, which will repeal and replace the Data Protection Directive. The compromise text of the draft Regulation, adopted by the European Parliament on 12th March 2014, contains 'sunset' clauses (a measure that provides that the law shall cease to have effect after a specific date, unless further legislative action is taken to extend the law) and a requirement to review all current mechanisms that allow data transfers to the US. Such proposals are likely a response to the Snowden revelations.

The compromise text provides that adequacy decisions of the Commission (such as the Safe Harbor decision, and those approving the 'white list' of countries with adequate data protection laws) will remain in force for five years after the Regulation comes

(Continued on page 6)

(Continued from page 5)

into effect, unless they are amended, replaced, or repealed by the Commission (Article 41(8)).

It also provides that data transfers based on appropriate safeguards in a legally binding instrument (such as the Model Contractual Clauses or 'BCRs') should remain valid for two years after the entry into force of the Regulation, unless amended, replaced or repealed by the DPA (Article 42(5)).

The Council of the EU, comprised of national Ministers from each EU Member State, appears to be opposed to the inclusion of these sunset clauses. The draft Regulation requires the approval of the EU Council before it can become law, and thus it remains to be seen whether these proposals will be included in the final Regulation, which is expected to be passed in 2015 and brought into effect two years later, in 2017.

In its 'Opinion 04/2014 on Surveillance of electronic communications for intelligence and national security purposes', the Article 29 Working Party has welcomed the European Parliament's proposal for data controllers and processors to inform DPAs and data subjects about requests to disclose personal data to courts or regulatory authorities in countries outside of the EEA (Article 43a). The Working Party has stated that being transparent about these practices would greatly enhance trust.

Radical approach by CJEU to protection of personal data

In recent months, the CJEU has made some extreme decisions on data privacy issues that demonstrate the importance that the CJEU affords to the privacy rights of individuals, and which cast further doubt on the adequacy of the current Safe Harbor regime.

On 8th April 2014, in *Digital Rights Ireland Ltd and Seitlinger and others*, (Joined Cases C-293/12 and 594/12), the CJEU ruled that the Data Retention Directive (2006/24/EC) was invalid. The Directive required EU Member States to adopt laws obliging telcos and ISPs to retain certain user data for up to two years, and to provide such data to law enforcement authorities if requested.

The CJEU held that the Directive did not provide appropriate safeguards in respect of the accessing of data by national authorities, as required by the European Charter of Fundamental Rights ('EU Charter'). In addition, it failed to provide for the retention of data within the European Union with supervisions by an independent authority, in the manner required by Article 8(3) of the EU Charter.

In a separate and well covered case concerning the so called 'right to be forgotten', on 12th May 2014 in *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* (Case C-121/12), the CJEU held that data subjects have the right to request Google and other internet search engines operators to remove search results that include their name, where those results are inadequate, irrelevant or no longer relevant, or excessive in relation to the purpose for which they were processed.

Schrems v DPC (No. 1) — a landmark case

The CJEU's ruling in *Schrems v DPC* looks set to be another landmark one, with important practical implications for businesses transferring data to non-EU countries.

Background

On 18th June 2013, Max Schrems, an Austrian citizen, brought a judicial review challenge asking the Irish High Court to overturn a decision of the DPC refusing to investigate his complaint, on the grounds that it was frivolous and vexatious. He had complained that the Snowden revelations demonstrated that there is no effective data protection regime in the US, and that the DPC should exercise his statutory powers to direct that the transfer of personal data from Facebook Ireland to its parent company (Facebook Inc.) in the US should cease.

The DPC found that as Facebook Inc. had self-certified under the Safe Harbor regime, and the Safe Harbor Decision found that Safe Harbor provided an adequate level of data protection, there was nothing left for him to investigate.

The DPC refused to exercise his power to suspend the flow of data from Facebook Ireland to Facebook Inc., on the grounds that none of the specified conditions for doing so applied in this case. Furthermore the DPC contended that, in view of the fact that the Commission was already engaged in a review of Safe Harbor, it was perfectly lawful to take the view that the applicant's complaint should be addressed at EU level and not by him.

Decision

Judge Hogan concluded that Mr Schrems' objection was, in reality, to the terms of the Safe Harbor regime rather than to the manner in which the DPC had applied the regime. He noted that 'the Safe Harbor regime was… not only drafted before the Charter came into force, but its terms may also reflect a somewhat more innocent age in terms of data protection'.

The Irish High Court has asked the CJEU whether the DPC is absolutely bound by the EU Commission's Safe Harbor Decision in light of the subsequent entry into force of Articles 7 and 8 of the EU Charter, which protect the right to respect for private and family life and to protection of personal data, or alternatively, whether the DPC may conduct his own investigation of the matter in light of factual developments since the Safe Harbor Decision was first published.

It remains to be seen how widely these questions will be construed by the CJEU. The CJEU might answer the court's questions in a narrow way, focussing on the discretion of DPAs to look behind the EU Commission's Safe Harbor Decision, or it may go further and examine the issue of all adequacy-based transfers of data out of the EEA.

Judge Hogan highlighted that if the DPC cannot look beyond the Safe Harbor Decision, then it is clear that

Mr Schrems' complaint both before the DPC and in the judicial review proceedings must fail. The High Court proceedings have been adjourned pending the outcome of the reference to the CJEU.

Schrems v DPC (No.2)

On 16th July 2014, the Irish High Court granted an order joining Digital Rights Ireland ('DRI') as 'amicus curie' (a person with strong interest in, or views on, the subject matter of an action, but not a party to the action) to the CJEU proceedings in *Schrems*. The court held that DRI will likely be in a position to articulate its own distinctive views on the data protection questions arising, which may assist the CJEU in grappling with those difficult questions.

Risk minimisation

Due to the large-scale access by US authorities to EU data held by US based companies, before transferring personal data, all appropriate measures should be taken to minimise the risk of data being disclosed.

Data controllers should examine options such as anonymisation of data and also ensure that their privacy policies are clear and transparent, and easily accessible on their websites, so that customers are aware of the transfer of their data outside of the EEA, and that such data might be subject to disclosure to law enforcement agencies in third countries. For example, Nokia, which has operations in the US and is a Safe Harbor member, provides in its privacy policy: 'We may be obligated by mandatory law to disclose your personal data to certain authorities or other third parties, for example, to law enforcement agencies in the countries where we or third parties acting on our behalf operate.' Such measures should enhance trust and confidence by customers in how international companies handle their personal data.

Conclusion

Whilst the Safe Harbor regime currently remains a valid method for legitimising international data transfers, organisations should take caution and be aware of the risks involved with relying solely on the regime. EU companies should ensure that their contracts with US companies provide that in the event the US company ceases to be registered as Safe Harbor compliant, or in the event Safe Harbor is suspended or revoked, that the US company will be required to enter into an alternative data transfer arrangement, such as the Model Contracts or BCRs.

Whilst it seems unlikely that Safe Harbour will be revoked, the Commission has made it clear that the current regime must be revised in order to survive. It would be prudent for data controllers to consider the alternative data transfer methods available, in order to avoid being caught short, in the event that the current regime is suspended, pending reform.

The review by the CJEU, in the *Schrems* case, will undoubtedly put pressure on the Commission and the US government to reach agreement quickly on the reform of Safe Harbor, in line with the Commission's recommendations.

Davinia Brennan
A&L Goodbody
dbrennan@algoodbody.com