# How safe is the U.S-EU safe harbour?

**Sep 09 2013** Bridget Treacy

Following widespread concern about the U.S. government's surveillance programmes, European Commission vice president Viviane Reding announced in July 2013 that the Commission would conduct an assessment of the U.S.-EU Safe Harbour agreement. The Safe Harbour is an important mechanism for enabling the transfer of personal data from the EU to the U.S., in accordance with European data protection laws, and it is used by a significant number of companies across a wide range of sectors. Reding has raised doubts about Safe Harbour, suggesting that it "may not be so safe after all" and noting that it "could be a loophole for data transfers because it allows data transfers from EU to U.S. companies, although U.S. data protection standards are lower than our European ones". European data protection authorities (DPAs) have also expressed doubts about Safe Harbour, all of which has led to concern about the future of Safe Harbour.

**Origin of Safe Harbour**

The U.S.-EU Safe Harbour framework was established in 2000 as a means of enabling European data controllers to transfer personal data to the U.S. while ensuring adequate compliance with EU data protection law. Since then, more than 3,000 U.S. companies (processors as well as controllers) have voluntarily signed up to the Safe Harbour framework. Despite submitting to U.S. law, and to oversight by the Federal Trade Commission (FTC), and notwithstanding the fact that the FTC has brought a number of enforcement actions for breaches of Safe Harbour commitments, some European DPAs continue to have reservations about the effectiveness of the Safe Harbour as a means of ensuring adequate data protection.

**Safe Harbour criticisms**

German regulators have been expressing concern about Safe Harbour for some time. In 2010, the Dusseldorfer Kreis (a working group comprising the 16 German state DPAs responsible for data protection in the private sector) issued a resolution requiring additional diligence from German exporters who relied on a data importer's Safe Harbour certification. By requiring additional diligence, the resolution appeared to question the European Commission's decision that Safe Harbour certification was sufficient to demonstrate an adequate level of data protection.

The Dusseldorfer Kreis concluded that German data exporters should not rely exclusively on the U.S. Department of Commerce's list of entities that had certified to the Safe Harbour when determining whether a U.S. data importer ensured an adequate level of protection for personal data under German law. Instead, German data exporters must also verify whether a self-certified importer complied with certain minimum Safe Harbour requirements by:

- checking when the entity first certified to the Safe Harbour;
- ensuring the importer provides notice of the data processing to relevant individuals as required by the notice principle under Safe Harbour; and
- documenting its assessment and making it available on request to a German DPA.

If, after further diligence, the exporter still had doubts about the importer's Safe Harbour compliance, the Dusseldorfer Kreis recommended using the European Commission's standard contractual clauses to ensure adequate protection.

These concerns were echoed in the Article 29 Working Party's Opinion on Cloud Computing, issued in July 2012, in which it suggested that EU data exporters could not rely on cloud providers' self-certification to Safe Harbour alone to legitimise data transfers. By contrast, in April 2013, the U.S. Department of Commerce's International Trade Administration confirmed Safe Harbour as a legitimate data transfer mechanism for cloud vendors, on the basis that cloud computing did not present any unique issues for Safe Harbour.

The European Commission endorsed the Safe Harbour framework in its draft Data Protection Regulation, published in January 2012. The Draft Regulation has proposed that adequacy decisions made under the existing directive would remain in effect unless amended, repealed or replaced by the Commission. That view has not been shared by all those involved in the review of Europe's data

protection laws. The lead Parliamentary Committee (Civil Liberties, Justice and Home Affairs (LIBE)) has proposed amending the draft Regulation so that adequacy decisions (including Safe Harbour) would only remain in force for two years after the Regulation came into effect. None of the other Parliamentary Committees has tabled a similar proposal, so it is unclear how this issue will be resolved.

**Impact of PRISM**

Following recent reports of U.S. and EU authorities intercepting and accessing the electronic communications of EU citizens on a substantial scale, the Safe Harbour has come under still further scrutiny. The European Parliament called on the Commission to review Safe Harbour, claiming that the PRISM surveillance programme constituted a "serious violation" of the Safe Harbour agreement.

In response to the PRISM revelations, German DPAs have decided to take further action, and to stop issuing approvals for data transfers until the German government demonstrates that unlimited access to German citizens' personal data by foreign national intelligence services complies with the fundamental principles of data protection law (i.e., necessity, proportionality and purpose limitation), and to review whether to suspend transfers carried out on the basis of Safe Harbour and standard contractual clauses.

Meanwhile, the Article 29 Working Party has written to Reding setting out the main issues of concern, relating to PRISM, to be raised with the U.S. The issues include determining what data are actually collected through the intelligence programme (i.e., whether the data includes content as well as metadata); from where the data are collected; in what circumstances the data may be accessed; the role of the Foreign Intelligence Surveillance Court and the criteria the court applies to allow surveillance orders against non-U.S. persons; and the relationship between intelligence programmes and compliance with conditions for third-country data transfers.

**Consequences for business**

There is growing concern within the business community that uncertainty over the status and future of Safe Harbour may damage confidence. A group of organisations representing the technology industry recently wrote to the U.S. Administration and Congress urging engagement with EU officials to ensure that the Safe Harbour continued as a mechanism to facilitate international data transfers. Given the widespread use of Safe Harbour, and the importance of ensuring adequate transfers to the U.S., it seems unlikely that Safe Harbour will be abandoned.

Despite Reding's comments, and the response of the German DPAs, the Commission's decision on the adequacy of Safe Harbour remains in force, until specifically repealed or changed. Further, although national DPAs may suspend data flows to Safe Harbour certified entities in exceptional circumstances, such a decision by a national regulator would be a serious decision, and not one to be taken lightly.

Discussions about the adequacy of Safe Harbour will continue, both before and after publication of the Commission's review. It is possible that the findings of that review may be reflected in revised text in the Draft Regulation. In any event, irrespective of the outcome of the Commission's review, some EU DPAs are likely to continue to hold reservations about whether the Safe Harbour framework is sufficiently rigorous, and will point to a lack of enforcement actions as evidence that bears out this concern. There may perhaps be further FTC enforcement action on the basis of Safe Harbour failings. Meanwhile, anecdotally, companies appear to have shown more interest in Binding Corporate Rules as a data transfer mechanism.

HUNTON& WILLIAMS

***Bridget Treacy*** *is a partner at Hunton & Williams and leads the UK privacy and information management practice. Her practice focuses on privacy, data protection, information governance and e-commerce issues for multinational companies across a broad range of industry sectors. Bridget can be reached on +44 (0) 20 7220 5731.*