
ESTABLISHED 1987

INTERNATIONAL REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

# Safe Harbor invalid: What to expect after the ruling?

**Sarah Cadiot** and **Laura De Boel** explain what businesses can do to enable transfers to the US.

On 6 October 2015, the Court of Justice of the European Union (CJEU) issued a landmark judgment[1] invalidating the European Commission's Decision of 2000[2] which recognised the adequacy of the EU-U.S Safe Harbor framework (Safe Harbor). In addition to the invalidation of this adequacy decision, the CJEU upheld the power of national Data Protection Authorities (DPAs) to independently investigate international data

*Continued on p.3*

# ECJ clarifies meaning of territorial scope in DP Directive

Hungarian data protection law applies to a company's activities in Hungary, although registered in Slovakia. **Andrea Klára Soós** reports.

On 1 October 2015, the European Court of Justice (ECJ) published its decision in case No. C-230/2014[1]. In this decision the ECJ followed the argumentation of Advocate General Pedro Cruz Villalón[2] and came to the conclusion that the principle of establishment should be applied by the authorities of other EU Member States. Consequently, a data controller could be investigated

*Continued on p.5*



Issue 137 **October 2015**

*Safe Harbor... from p.1*

transfers based on adequacy decisions. This may lead to a fragmented approach to international data transfers in the European Union (EU).

The "Schrems case" is a new milestone in EU data protection law. This article analyses the judgment and describes the implications for businesses.

## Facts of the Schrems case

Maximillian Schrems, an Austrian Facebook user, opposed the transfer of his personal data to Facebook's servers located in the US under Facebook's Safe Harbor certification. Schrems referred to the media revelations that the US National Security Agency (NSA) and other US authorities accessed personal data from EU citizens collected by Safe Harbor certified companies. Schrems claimed that Safe Harbor therefore did not adequately protect his personal data.

In 2013, Schrems requested the Irish DPA to investigate Facebook's practices and suspend data transfers to its servers in the US (Facebook's EU headquarters are located in Ireland). However, the Irish DPA rejected Schrems' claim because it considered itself bound by the adequacy decision concerning Safe Harbor (the "Safe Harbor Decision") adopted by the European Commission (the "Commission"). Schrems appealed the DPA's decision to the Irish High Court, which turned to the CJEU to clarify whether or not a national DPA is bound by the Safe Harbor Decision.

## I. The judgment

In response to the High Court's preliminary question, the CJEU declares that, regardless of an adequacy decision from the Commission, DPAs must be able to independently examine the lawfulness of data transfers to third countries. However, only the CJEU can declare an EU act, such as an adequacy decision, invalid.

The CJEU then goes beyond the preliminary question by examining the validity of Safe Harbor, and declaring it invalid. We analyse the key findings of the judgment below.

### Safe Harbor is invalid

The CJEU invalidates the Safe Harbor Decision. Thus, Safe Harbor is no longer available as a legal transfer mechanism for transferring personal data from the EU to the US.

In its fifteen years of existence, Safe Harbor was criticised in Europe and considered by some as inefficient for the protection of personal data of EU individuals. After the Snowden revelations, the Commission itself issued critical opinions on Safe Harbor. The CJEU refers to these communications[3] from the Commission to demonstrate that Safe Harbor does not sufficiently protect personal data transferred from the EU to the US. In particular, the CJEU considers that the broad national security exception in the Safe Harbor Decision allowed for disproportionate interference with the fundamental rights provided both under the EU Data Protection Directive 95/46/EC and the EU Charter of Fundamental Rights.

The CJEU refers to its judgment in Digital Rights Ireland and Others[4] to stress that derogations to the protection of personal data should only apply in so far as is strictly necessary. The alleged mass surveillance by US authorities goes beyond what is strictly necessary according to the CJEU.

The CJEU also criticises the lack of effective judicial remedies available to EU individuals whose personal data are accessed by US authorities. The CJEU considers that the procedures before the US Federal Trade Commission and dispute resolution mechanisms foreseen under Safe Harbor do not enable EU individuals to obtain access, rectification or erasure of their personal data, or administrative or judicial redress with regard to the collection and further processing of their personal data under US surveillance programmes.

### Oversight by national DPAs

The CJEU declares that national DPAs are competent for investigating claims related to international data transfers, even if these transfers occur on the basis of an adequacy decision, such as the Safe Harbor Decision. According to the CJEU, the existence of an adequacy decision from the Commission cannot reduce or eliminate the independence and powers granted to the national DPAs by the EU Data Protection Directive.

However, the CJEU declares that a DPA cannot by itself invalidate adequacy decisions, including the Safe Harbor Decision. The CJEU alone has jurisdiction to declare that an EU act is invalid, but DPAs can use their powers to independently investigate companies' data transfer practices. This entails a major risk of fragmentation of the EU internal market. DPAs in different EU countries may have divergent approaches to international data transfers in the absence of clear guidance from the Commission or the Article 29 DP Working Party.

This is especially relevant considering recent CJEU case law on the application of national data protection law and the competence of national DPAs – e.g Costeja[5], and more recently Weltimmo[6] [see article on p.1 in this issue]. The CJEU considers that an EU Member State's national data protection law applies, and its national DPA is competent, as soon as a company's establishment in that Member State is involved in operations connected to data processing (e.g sales), without actually carrying out data processing activities. There is a risk that different DPAs declare themselves competent to investigate a company's data transfer practices, with conflicting decisions as a result. The One-Stop Shop and consistency mechanisms foreseen under the draft General Data Protection Regulation (GDPR) will hopefully mitigate this risk.

## II. Practical implications of the judgment

### Companies should look into alternative data transfer mechanisms

There is no one-size-fits-all alternative solution to Safe Harbor which can be recommended to all companies. Each company should look at its data processing activities, corporate structure, and the nature and frequency of its international data flows to determine which solution fits. The following different solutions are available:

- Data transfer agreements (based on the EU Model Clauses or ad hoc agreements)
- Binding Corporate Rules (BCRs)
- The derogations provided under the

EU Data Protection Directive 95/46/EC (e.g consent).

Some authors question whether the EU Model Clauses and BCRs are equally at risk because of this judgment. However, this seems unlikely since EU Model Clauses and BCRs do provide some protection for individuals in case non-EU data importers are faced with data disclosure requests from foreign authorities (e.g third-party beneficiary rights for individuals). Also, the political context around these legal instruments is very different from the Safe Harbor context.

Some companies have already announced that they will rely predominantly on EU Model Clauses as an interim and/or long-term solution. EU Model Clauses are often a good alternative solution, but they presume that there is a data exporter established in the EU (e.g affiliate of the importer, third party exporter) that the non-EU data importer can contract with. For non-EU companies that offer online services directly to individuals in the EU, a model contract may not be a practical solution.

The use of the "Processor-to-Processor" EU Model Clauses, which have not yet been formally approved by the Commission, may become more popular since they allow service providers to regulate their international data transfers, although these clauses have some shortcomings (e.g require DPAs' prior approval).

Another alternative solution would be to obtain individuals' consent to data transfers to the US (e.g via a tick box on a registration page). DPAs previously did not see consent as a viable data transfer solution for repetitive and structural data transfers. However, in light of the judgment, consent could be the most realistic option in certain circumstances. Moreover, during their press conference following the judgment, First Vice-President of the Commission Frans Timmermans and Commissioner Vera Jourová stressed that businesses can rely on consent if no other ground for data transfers is available[7]. However, the use of consent may raise practical difficulties, since individuals may refuse to consent to the transfer, or later on withdraw their consent.

In the long term, BCRs are seen as the best alternative to Safe Harbor, since they represent a single solution for international data transfers. However, implementing BCRs requires cooperation and approval from DPAs and the process takes time. Until their BCRs are approved, companies may still need to find an interim solution (e.g EU Model Clauses).

Many companies are now in the dark regarding the solutions they should implement in the short and long term. On the day of the judgment, the UK DPA stated 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", adding "we recognise that it will take them some time for them to do this".[8]

**Safe Harbor 2.0?**

On 27 November 2013, the Commission issued 13 recommendations to enhance the Safe Harbor[9] which led to negotiations between the EU and the US for a new Safe Harbor. These 13 recommendations include a series of imperative enhancements to make to the current Safe Harbor, including stronger safeguards regarding the derogations granted to US authorities for national security requirements.

The criticism of the CJEU is in line with the demands of the Commission. However, so far, no agreement on an updated Safe Harbor has been reached. In her press statement[10] right after the judgment was issued, Commissioner Vera Jourová indicated that an agreement is still not in sight, and that the national security derogation remains a stumbling block in the negotiations. Even if updates to the Safe Harbor are agreed upon, it remains to be seen what the level of trust in such Safe Harbor 2.0 will be. There would be a risk that Safe Harbor 2.0 would again be challenged in courts, and that the CJEU would consider that the updates are not sufficient to correct the problems identified in the Schrems judgment. Moreover, it seems unlikely that companies would return to using Safe Harbor, even in its new version, if they have implemented other data transfer mechanisms in the meantime.

**Guidance, please**

During their press conference, First Vice-President Timmermans and Commissioner Jourová stated that the Commission had started discussions with the national DPAs to issue guidance on how to deal with EU data transfer restrictions in light of the CJEU's judgment. At the moment of writing, the Article 29 DP Working Party is meeting to discuss the content of this guidance. The aim is to ensure a coordinated response by all national DPAs and avoid contradictory decisions. Hopefully, clear and practical guidance will be issued soon.

**Impact on the GDPR**

Chapter V of the GDPR provides rules on international data transfers that are similar to the requirements under the current EU Data Protection Directive. Due to the secrecy surrounding the Trilogue negotiations on the GDPR, it is difficult to assess the impact of the judgment on the final text. Sources involved in the Trilogues indicate that Chapter V has generally been agreed on, but the judgment may lead the EU institutions to re-open negotiations. For instance, the discussion on whether adequacy decisions should be adopted by way of delegated acts or implementing acts could be brought up again.

## III. Conclusion

This landmark judgment has important implications for transfers of personal data from the EU to the US. In light of the CJEU judgment, Safe Harbor certified companies should assess alternative options for data transfers. This process takes time and will require a careful review of the company's business and corporate structure. DPAs will hopefully stay pragmatic and engage in dialogues with companies when needed. What is certain is that this is another key judgment in a series of cases in which the CJEU demonstrates a very strict interpretation of EU data protection law.

 

**AUTHORS**

Sarah Cadiot, Associate and Laura De Boel, Senior Associate, Wilson Sonsini Goodrich & Rosati, LLP, Belgium.
Emails: scadiot@wsgr.com and ldeboel@wsgr.com
The authors are grateful to Anna Ciesielska, legal intern in WSGR's Brussels office, for her excellent research assistance.

**REFERENCES**

1 Case C-362/14 Maximillian Schrems v Data Protection Commissioner [2015], available at: http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=139721
2 Decision 2000/520/EC of July 26, 2000, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000D0520:EN:HTML
3 Communication from the Commission to the European Parliament and the Council entitled 'Rebuilding Trust in EU-US Data Flows' (COM(2013) 846 final, November 27, 2013) and Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU (COM(2013) 847 final, November 27 2013).
4 C-293/12 and C-594/12 Digital Rights Ireland and Others [2014], available at http://curia.europa.eu/juris/document/document.jsf?text=&docid=153045&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=109775
5 Case C-131/12, Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González [2014], available at http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&docid=152065
6 Case C-230/14, Weltimmo s. r. o. v. Nemzeti Adatvédelmi és Információszabadság Hatóság [2015], available at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62014CJ0230
7 European Commission's press statement following the Schrems judgment, 6 October 2015, available at http://europa.eu/rapid/press-release_STATEMENT-15-5782_en.htm
8 Information Commissioner Office's press release "ICO response to ECJ ruling on personal data to US Safe Harbor", 6 October 2015, available at https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2015/10/ico-response-to-ecj-ruling-on-personal-data-to-us-safe-harbor/
9 European Commission's Memo "Restoring Trust in EU-US data flows - Frequently Asked Questions", 27 November 2013, available at http://europa.eu/rapid/press-release_MEMO-13-1059_en.htm
10 Ibid 8.

# Join the Privacy Laws & Business community

## Six issues published annually

### PL&B's International Report will help you to:

**Stay informed of data protection legislative developments in 100+ countries.**

**Learn from others' experience through case studies and analysis.**

**Incorporate compliance solutions into your business strategy.**

**Find out about future regulatory plans.**

**Understand laws, regulations, court and tribunal decisions and what they will mean to you.**

**Be alert to future privacy and data protection law issues that will affect your organisation's compliance.**

## Included in your subscription:

**1. Online search functionality**
Search for the most relevant content from all *PL&B* publications and events. You can then click straight through from the search results into the PDF documents.

**2. Electronic Access**
You will be sent the PDF version of the new issue on the day of publication. You will also be able to access the issue via the website. You may choose to receive one printed copy of each Report.

**3. E-Mail Updates**
E-mail updates help to keep you regularly informed of the latest developments in data protection and privacy issues worldwide.

**4. Back Issues**
Access all the *PL&B International Report* back issues since 1987.

**5. Special Reports**
Access *PL&B* special reports on Data Privacy Laws in 100+ countries and a book on Data Privacy Laws in the Asia-Pacific region.

**6. Events Documentation**
Access International and/or UK events documentation such as Roundtables with Data Protection Commissioners and *PL&B Annual International Conferences*, in July, in Cambridge, UK.

**7. Helpline Enquiry Service**
Contact the *PL&B* team with questions such as the current status of privacy legislation worldwide, and sources for specific issues and texts. This service does not offer legal advice or provide consultancy.

## To Subscribe: www.privacylaws.com/subscribe

"*PL&B's International Report* is a powerhouse of information that provides relevant insight across a variety of jurisdictions in a timely manner. **Mark Keddie, Chief Privacy Officer, BT Retail, UK**"

## Subscription Fees

**Single User Access**

*International* Edition **£500 + VAT***

*UK* Edition **£400 + VAT***

*UK & International* Combined Edition **£800 + VAT***

* VAT only applies to UK based subscribers

**Multi User Access**

Discounts for 2-4 or 5-25 users – see website for details.

**Subscription Discounts**

Special charity and academic rate:
50% discount on all prices. Use HPSUB when subscribing.

Number of years:
2 (10% discount) or 3 (15% discount) year subscriptions.

**International Postage (outside UK):**

Individual International or UK Edition
Rest of Europe = £22, Outside Europe = £30

Combined International and UK Editions
Rest of Europe = £44, Outside Europe = £60

## Satisfaction Guarantee

If you are dissatisfied with the *Report* in any way, the unexpired portion of your subscription will be repaid.

*Privacy Laws & Business* also publishes the United Kingdom Report.
**www.privacylaws.com/UK**