

## EU's highest court declares Safe Harbor invalid

### Regulatory News Alert

7 October 2015

The Court of Justice of the European Union (CJEU) has ruled on October 6, 2015 that the EU-US Safe Harbor Framework for transferring personal data from the EU to the US is invalid.

#### Background

The case was brought before the EU's highest court by Max Schrems, an Austrian Facebook user who lodged a complaint with the Irish Data Protection Authority (DPA) after the Snowden revelations had shown that his data and that of other EU citizens had been accessed by US intelligence services. Data from European Facebook users is transferred from its subsidiary in Ireland to servers located in the US, where it is processed. The Irish DPA first rejected the complaint on the grounds that, under the Safe Harbor scheme, the United States had been deemed by the European Commission to ensure an adequate level of protection of transferred personal data (i.e. protection equal to EU standards).

The High Court of Ireland, to which the case was then brought, asked the CJEU whether this reasoning holds, i.e. whether the existence of a decision from the European Commission (the EU's executive body) establishing that a third country ensures an adequate level of protection can eliminate or reduce the powers available to a national DPA to examine whether this is indeed the case. The CJEU clearly rejected this reasoning and argued that a national DPA must be able to examine, with complete independence, whether the transfer of a person's data to a non-EU country complies with the requirements laid down by the EU Data Protection Directive.

The CJEU further confirmed that it alone can declare a European Commission Decision invalid, and therefore went on to investigate the adequateness of the Safe Harbor framework. The Court of Justice of the European Union decided to declare the Safe Harbor Decision invalid for the following reasons:

- National security, public interest and law enforcement requirements of the United States prevail over the Safe Harbor scheme, so that United States undertakings are bound to disregard, without limitation, the protective rules laid down by the scheme where they conflict with such requirements;
- United States authorities were able to access the personal data transferred from the EU to the United States and process it in a way incompatible with the purposes for which it was transferred, beyond what was strictly necessary and proportionate to the protection of national security;
- The persons concerned had no administrative or judicial means of redress enabling, in particular, the data relating to them to be accessed and, as the case may be, rectified or erased.

The CJEU only declared it invalid. It did not foresee any grace period or transition period.

## Consequences: revising data transfer strategy

The direct consequence of this ruling is that the Irish DPA will now have to examine Max Schrems' complaint with due diligence, and at the conclusion of its investigation, is to decide whether, pursuant to the Directive, the transfer of the data of Facebook's European subscribers to the United States should be suspended on the ground that that country does not afford an adequate level of protection of personal data.

A much wider consequence of the CJEU ruling is that one of the most important and most used legal frameworks for transfers of personal data between the EU and the US has been declared invalid, forcing 4,400 US-based companies to revise their data transfer strategy in the short term.

The European Commission confirmed on a press conference later in the day that other mechanisms for organising data transfers to the US, such as EU model contracts, binding corporate rules (BCRs; for intra-group transfers) remain valid. In addition, it emphasised that the Data Protection Directive includes certain derogations that allow for international data transfers, i.e. when necessary for the performance of a contract (e.g. EU citizen booking a hotel in the US), on important public interest grounds (fight against fraud, etc.), to protect a vital interest of the data subject (emergency situations [alternatively: life or death situations e.g. emergency transfer of medical data?]), or based on the free and informed consent of the data subject.

## Next steps

The Commission will shortly issue guidance to national DPAs and businesses in order to ensure a uniform interpretation of the ruling across the EU, reinstate legal certainty for businesses and safeguard the transatlantic flow of data – calling it “the backbone of the European economy”. To this end, it will cooperate with the Article 29 Working Party, the EU's advisory body on data protection which brings together all 28 national DPAs. In addition, the Commission will act as a point of contact for queries from organisations.

In the meantime, the European Commission will continue the negotiations with the US on a new Safe Harbor Framework that started in October 2013. Commissioner Věra Jourová noted that the CJEU ruling acknowledges the concerns that were raised by the Commission in 2013, and that the negotiations will build on the ruling going forward. She could not state a deadline for the negotiations at this time, as the negotiations on national security aspects are taking more time than she had initially hoped.

As a side note, the Commissioners said that the negotiations on the reform of the EU data protection legislation, in the form of the General Data Protection Regulation, is still scheduled to end by the end of 2015.

We will keep our ears to the ground on the impact of the Safe Harbor CJEU decision and the reactions per country, on the ongoing negotiations between the EU and the USA for an updated 'safer' Safe Harbor agreement, and on the EU negotiations on the General Data Protection Regulation.

## Further information:

- The [official CJEU press release](#)
- The [official CJEU judgement](#)
- The European Commission press conference of 6 October 2015 (video):
  - <http://ec.europa.eu/avservices/video/player.cfm?ref=l109752>
  - <http://ec.europa.eu/avservices/video/player.cfm?ref=l109753>
  - <http://ec.europa.eu/avservices/video/player.cfm?ref=l109754>

## Forthcoming interesting events

### European Privacy Academy

The European Privacy Academy is a unique training, knowledge and networking centre focused on the actual day-to-day management of the privacy challenge. It provides both an on-campus data protection officer course and on-campus or in-house department-specific data protection trainings during which attendees learn to efficiently manage privacy and security in a risk based and integrated manner.

The next sessions of the European Privacy Academy are listed below:

- **DPO Course – October 2015:** 27 – 30 October 2015 & 22 January 2016
- **DPO Course – January 2016:** 18 – 21 January 2016 & 15 April 2016

In case of interest for this data protection training, please contact [Laurent de la Vaissière](#) or [Irina Hedeá](#).

# Your contacts

**Roland Bastin**

Partner | Information & Technology Risk  
Tel/Direct: +352 451 452 213  
rbastin@deloitte.lu

**Laurent de la Vaissière**

Director | Information & Technology Risk  
Tel/Direct: +352 451 452 010  
ldelavaissiere@deloitte.lu

**Irina Hedeá**

Director | Information & Technology Risk  
Tel/Direct: +352 451 452 944  
ighedeá@deloitte.lu

Deloitte Luxembourg  
560, rue de Neudorf  
L-2220 Luxembourg

Tel: +352 451 451  
Fax: +352 451 452 401  
www.deloitte.lu

Deloitte is a multidisciplinary service organisation which is subject to certain regulatory and professional restrictions on the types of services we can provide to our clients, particularly where an audit relationship exists, as independence issues and other conflicts of interest may arise. Any services we commit to deliver to you will comply fully with applicable restrictions.

Due to the constant changes and amendments to Luxembourg legislation, Deloitte cannot assume any liability for the content of this leaflet. It shall only serve as general information and shall not replace the need to consult your Deloitte advisor.

**About Deloitte Touche Tohmatsu Limited:**

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see [www.deloitte.com/lu/about](http://www.deloitte.com/lu/about) for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms.

Deloitte provides audit, tax, consulting and financial advisory services to public and private clients spanning multiple industries. With a globally connected network of member firms in more than 150 countries, Deloitte brings world-class capabilities and deep local expertise to help clients succeed wherever they operate. Deloitte has in the region of 200,000 professionals, all committed to becoming the standard of excellence.

© 2015 Deloitte General Services

Designed and produced by MarCom at Deloitte Luxembourg