At a glance

October 2015

The CJEU's *Schrems* ruling on the Safe Harbour Decision

On 6 October 2015, the Court of Justice of the EU (CJEU) declared invalid the European Commission's decision on the adequacy of the US data protection system (*Safe Harbour* Decision). In this judgment, regarding the transfer of personal data from the EU to the USA, the Court also clarified that national supervisory authorities are always allowed to investigate the lawfulness of data transfers and, if necessary, to suspend them. The case underlines the requirement for ensuring high-level protection when EU citizens' data are transferred to third countries. The implications for businesses, governments and EU institutions, as well as for EU-US relations, remain to be clarified.

Background

The 1995 Data Protection Directive (Directive 95/46 – hereafter the DP Directive) aims to encourage coherent free movement of personal data while protecting individual rights. A *high level* of protection is ensured, to the extent that data transfer outside the EU/EEA is allowed only if the third country can ensure an *adequate* level of protection. Such *adequacy* shall *be assessed* under Article 25 *in light of all the circumstances* surrounding a data transfer operation and *the rules of law* in force in the third country in question. The European Commission may find, by adopting a decision, that a third country ensures an adequate level of protection. On that basis, the Commission issued Adequacy Decision 2000/520 (hereafter the Adequacy Decision), stating that the 'Safe Harbour' system, enacted by the US Department of Commerce, was 'adequate' and allowed data transfers to US firms complying with the Safe Harbour principles (see box below). On 6 October 2015, following a complaint against Facebook by an Austrian citizen, Max Schrems, the CJEU declared the adequacy decision **invalid,** thus making the Safe Harbour principles insufficient to allow transatlantic transfers. Over 4 000 companies relied on this adequacy decision for their transatlantic data transfers.

The **Safe Harbour principles** were not compulsory; firms joined them voluntarily. To do so they had to issue an annual statement self-certifying that they complied with the principles. The validity of self-certifications was normally verified by the US Department of Commerce which also maintained a list of firms with valid certifications. The monitoring of compliance was normally under the jurisdiction of the Federal Trade Commission. Indeed, the Safe Harbour principles functioned like promises (usually enclosed in firms' 'privacy policies') to customers; failure to comply with such promises triggers a case of **unfair and deceptive practices** pursuant to Section 5 of the Free Trade Commission Act. The firm could disregard the application of the Safe Harbour principles for a number of derogations, included one for law enforcement purposes.

The *Schrems* judgment

Schrems had lodged a complaint with the Irish Data Protection Authority, asking it to investigate whether his Facebook data were transferred from Facebook's European headquarters (based in Ireland) to servers in the USA. Indeed, he argued that, in light of the Snowden revelations about the NSA's data collection programme (PRISM), US law and practice did not offer the *adequate* protection to EU citizens required by EU law. The Irish Data Protection Authority (DPA) rejected the complaint on the ground that the EU-US transfer of data relies on the Commission's binding 'Safe Harbour' Adequacy Decision. The case, first brought to the High Court of Ireland and then referred to the CJEU for a preliminary ruling, called into question the lawfulness of data transfer to the USA under the Safe Harbour framework in light of EU Law. The CJEU, following the Advocate General's Opinion, has:

EPRS | European Parliamentary Research Service
Authors: Shara Monteleone and Laura Puccio, **Members' Research Service**
PE 569.050

- confirmed that national DPAs' powers to examine a person's claim (as enshrined by Directive 95/46 and by the EU Charter of Fundamental Rights) are not reduced by the existence of an adequacy decision,
- considered that the 'Safe Harbour' voluntary scheme is insufficient to ensure protection for EU citizens;
- declared – as the only party entitled to do so – the related Commission Adequacy Decision invalid.

High level of protection of fundamental rights

By declaring the adequacy decision invalid, the CJEU stressed the need to interpret the requirement of *adequate protection* under the DP Directive in the meaning of *essentially equivalent* to that guaranteed in the EU, in line with the Directive's objective of ensuring a *high level of protection* that extends to personal data transferred outside the EU. Furthermore, according to the Court, this requirement should be read in accordance with the Charter of Fundamental Rights, which protects the rights to privacy, to data protection and to effective judicial remedy, and which entrusts national DPAs with supervisory powers. This also implies a continuous assessment of the rules and practices of third countries in terms of safeguards, as conditions for the transfer of data. The CJEU held that the Adequacy Decision did not contain such findings. The Decision did not ensure that application of derogations under the Safe Harbour framework, in particular derogations for law enforcement purposes, would be complemented by sufficient safeguards for EU citizens against the risk of abuse and unlawful access and use of that data. Therefore the Adequacy Decision did not verify that interferences with fundamental rights would be limited to those strictly necessary.

This judgment forms part of a growing and consistent jurisprudence of the CJEU, stressing the significance of high-level protection of personal data (e.g. the *Google Spain* and *Digital Rights Ireland* cases). Some national DPAs have issued their own positions on the case, such as the DPA of Germany's Schleswig-Holstein and the Italian Garante, stressing the fact that the ruling requires Member States and EU bodies to ensure real and concrete respect for the Charter.

Legal consequences of the CJEU ruling

The invalidity of Adequacy Decision 2000/520 has raised several issues for transatlantic firms. Some guidance was given by the Article 29 Working Party (Art. 29 WP), bringing together the EU DPAs, which issued a common position on the implementation of the judgment.

The **first issue** concerned the retroactivity of the CJEU judgment, i.e. the impact on data transfers performed under Safe Harbour prior to the CJEU ruling. The Art. 29 WP affirmed that transfers still taking place under the Safe Harbour Decision *after* the CJEU judgment are unlawful. The **second issue** concerns the instruments still available to firms for transferring data. Here the Art. 29 WP considered existing transfer tools still applicable, such as the Binding Corporate Rules or Standard Contractual Clauses (SCC), issued by the Commission under the DP Directive. A second option could be to rely on unambiguous consent of the data subject. However, in light of the *Schrems* judgment, the Schleswig Holstein DPA considered a data transfer on the basis of SCC to the USA no longer to be permitted, and found the reliance on data-subject consent extremely problematic. The **third issue** concerned the establishment of a transitional period for firms to adjust. The Art. 29 WP gave three months' leeway, stating that coordinated enforcement actions would be taken by the end of January 2016 if no appropriate solution is found with the US authorities.

The Commission announced that future guidance will be issued jointly with the DPAs in order to ensure robust safeguards for citizens and legal certainty for businesses. In particular, it points out the need to avoid a patchwork of potentially contradictory decisions by the national data protection authorities.

The Commission and the USA, worried about current uncertainty, are continuing negotiations on Safe Harbour 2.0, to comply with the *Schrems* judgment. The Art. 29 WP stressed that this should include obligations on oversight mechanisms, transparency, proportionality and means of redress. The Umbrella Agreement on Data Privacy and Protection, finalised in September 2015, could also help fill the gap establishing a framework for data protection in EU-US law enforcement policies. The bill for a US Judicial Redress Act, passed by the House of Representatives and awaiting the Senate's vote, would contribute, extending the benefits (including redress rights) of the US Privacy Act to citizens of major US allies.

The role of the European Parliament

The case has recently been debated in the EP, and Civil Liberties (LIBE) Committee Chair, Claude Moraes (S&D, UK), urged the Commission to suspend 'Safe Harbour' immediately and initiate a new data protection framework. Parliament has repetitively called for the suspension of Safe Harbour privacy principles, in particular in its 2014 resolution on the electronic mass surveillance programmes run in the USA and some EU countries. An EP resolution on the follow-up to that 2014 resolution, based on a motion from the LIBE Committee, is due to be voted in plenary on 29 October.