Is there life after [Safe Harbor's] death?

By Cecilia Álvarez Rigaudias[*] and Natascha Gerlach[**]

October 15, 2015

On October 6, 2015, only two weeks after the Advocate General's opinion in *Schrems v. Data Protection Commissioner (Ireland)*[1], the Court of Justice of the European Union (CJEU) published its long-awaited judgment [2], creating a storm of controversy and uncertainty.

The CJEU ruled in simple terms that "Decision 2000/520 is invalid," thus swiftly and without any grace period disabling the European Commission's 15-year-old decision on the adequacy of the protection provided to personal data transferred to the United States under the Safe Harbor privacy principles (the "Safe Harbor Decision"). More than 4,400 entities that had been self-certified under Safe Harbor are now left wondering how to move forward.

The judgment, which overall confirms the Advocate General's opinion, first responds to the primary question laid before it by the Irish High Court by ruling that an adequacy decision by the European Commission (EC) in accordance with Art. 25 of EU Directive 95/46 does not curtail the power of national Data Protection Agencies (DPAs) to oversee personal data transfers. DPAs should be able "to examine with complete independence" whether a transfer of personal data respects the requirements of the Data Protection Directive. The CJEU does

---

[*] Cecilia Álvarez Rigaudias is the European Privacy Officer Lead of the pharma multinational Pfizer. Cecilia is Vice-president of APEP (Spanish Privacy Professional Association), Spanish member of CEDPO (Confederation of European Data Protection Organisations) and member of the Steering Committee of The Sedona Conference Working Group 6.

[**] Natascha Gerlach is a Senior Attorney with Cleary Gottlieb Steen & Hamilton, currently based in their Brussels office. She oversees Cleary's European Practice Support Department, which supports the eDiscovery needs of all European offices. Natascha specializes in Data Protection issues in connection with cross-border discovery and advises on data security issues. She is a member of The Sedona Conference Working Group 6.

[1] See Cecilia Álvarez Rigaudias and Natascha Gerlach, *"Reports of my death have been greatly exaggerated": The Advocate General's opinion in the Max Schrems v. Facebook case*, Oct. 1, 2015, https://thesedonaconference.org/wgs/wg6 (log-in required).

[2] The full text of the CJEU's judgment may be found at http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=117353.

emphasize, however, that only the CJEU has the authority to invalidate an adequacy decision made by the EC.

On the Safe Harbor decision itself, the CJEU based its invalidation on several arguments. While the CJEU acknowledged that an "adequate" level of protection does not mean an identical level, the wide derogations for national security, public interest, and law enforcement provided in Safe Harbor, and the potential for blanket access by U.S. authorities to personal data transferred from the EU, failed to provide even an adequate level of protection as mandated by the Directive and Articles 7 and 8 of the EU Charter of Fundamental Rights. The CJEU held that "legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life." The Safe Harbor principles only bind U.S. firms but not U.S. authorities, and "where U.S. law imposes conflicting obligations, U.S. organisations […] must comply with U.S. law" to the potential detriment of the Safe Harbor Principles they certified under. In light of this, and without reference to any limitations or access to effective legal redress, the Safe Harbor decision, according to the CJEU, does not fulfill the requirements of Art. 25 (6) of the Directive and is thus invalid.

After the Ruling: First Step – We Mustn't Panic!

Immediately after the CJEU judgment was issued, various national DPAs hurried to issue press statements with reassuring messages that they would not rush into enforcement actions and instead work on further guidance for those impacted by the judgment. [3]

The Article 29 Working Party itself acknowledged "that this decision, taken in the context of the negotiation on the European Regulation and the discussions on the Safe Harbour between the European Commission and the US authorities, has

[3] *See, e.g.*, Information Commissioner's Office (UK), *ICO response to ECJ ruling on personal data to US Safe Harbor*, Oct. 6, 2015, 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/; Agencia Española de Protección de Datos (Spain), *El TJUE declara inválida la Decisión de la Comisión que declara el nivel adecuado de protección del Puerto Seguro*, Oct. 6, 2015, http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2015/notas_prensa/news/2015_10_06-ides-idphp.php; Garante per la protezione dei dati personali (Italy), *Facebook: dichiarazione di Antonello Soro sulla sentenza della Corte di Giustizia Europea*, Oct. 6, 2015, http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/4308245.

major consequences on all stakeholders" and announced immediate expert meetings.[4]

From these proclamations, it is hoped that DPAs grant a reasonable grace period and leave those companies having safe harbor certificates time to work out next steps.

Step Two – Was I Hit?

The obvious impact of the CJEU's judgment is on those organisations that relied exclusively on Safe Harbor for transferring personal data from the EU to the U.S. Those entities will need to jump to action to implement alternative mechanisms for the transfer of that data before the DPAs begin enforcement proceedings. As Commissioner Vera Jourová, at a press conference following the CJEU judgment, put it, "transatlantic data flows between companies can continue using other mechanisms for international transfers of personal data available under EU data protection law"[5], pointing to standard contractual clauses and binding corporate rules as viable alternatives.

Binding Corporate Rules (BCRs) are designed to legitimize data transfers of personal information only within a corporation, allowing for personal data to be moved between corporate entities with the same protection throughout. BCRs approved by the DPA in one EU Member State are accepted in most, but not in all, other EU Member States.[6] However, BCR implementation is complex, expensive (both financially and in terms of time commitment), and can be onerous, due to the DPA approval process they must undergo.[7] The current drafts of the General Data

---

4 Article 29 Data Protection Working Party, *The Court of Justice of the European Union invalidates the EU Commission Safe Harbor Decision*, Oct. 6, 2015, http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151006_wp29_press_release_on_safe_harbor.pdf.

5 European Commission, *First Vice-President Timmermans and Commissioner Jourová's press conference on Safe Harbour following the Court ruling in case C-362/14 (Schrems)*, Oct. 6, 2015, http://europa.eu/rapid/press-release_STATEMENT-15-5782_en.htm.

6 21 countries are currently part of a mutual recognition procedure. *See* European Commission, *What is mutual recognition?* http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/mutual_recognition/index_en.htm.

7 Member State procedures differ greatly with respect to BCRs, and the Art. 29 Working Party, recognizing this, has developed a coordinated procedure, with the application made to a lead DPA which then enters into the negotiations with other potentially involved DPAs. For a comprehensive description, *see* CHRISTOPHER KUNER, EUROPEAN DATA PROTECTION LAW (2ND ED. 2009), ¶4.127).

Protection Regulation (GDPR) contemplate BCRs but it is still unclear whether they will survive in their current form and effect.

The Commission's decisions on Standard Contractual Clauses (SCCs), in accordance with Art. 26(2) and 26 (4) of the Directive, provide—in theory at least—the means to use one set of clauses for transfer from each of the EU Member States. In some Member States, however, SCCs require prior notification to the DPA or even DPA approval, which can be time consuming and formalistic.[8] Binding different entities can also mean a large number of individual contracts to keep track of, versus the relative simplicity of Safe Harbor, at least in controller-to-controller transfers.[9]

The DPAs' powers to review whether an international transfer meets the applicable data protection standard would also apply to the transfers based on SCC and BCRs. A 2010 EC decision stated that "supervisory authorities should have the power to prohibit or suspend a data transfer or a set of transfers based on the standard contractual clauses in those exceptional cases where it is established that a transfer on contractual basis is likely to have a substantial adverse effect on the warranties and obligations providing adequate protection for the data subject."[10] For example, Article 4. 1. (a) of that decision expressly allows for the member state DPAs to exercise their powers to prohibit or suspend data flows where "the law to which the data importer or a sub-processor is subject imposes upon him requirements to derogate from the applicable data protection law which go beyond the restrictions necessary in a democratic society as provided for in Article 13 of Directive 95/46/EC where those requirements are likely to have a substantial adverse effect on the guarantees provided by the applicable data protection law and the standard contractual clauses. . ."

---

8 Commission Decision of 5 February 2010 on Standard Contractual Clauses, 2010/87/EU, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32010D0087, Recital 5, states "[t]his Decision should be without prejudice to national authorisations Member States may grant in accordance with national provisions implementing Article 26(2) of Directive 95/46/EC. This Decision should only have the effect of requiring the Member States not to refuse to recognise, as providing adequate safeguards, the standard contractual clauses set out in it and should not therefore have any effect on other contractual clauses." There may be formal requirements, such as notarization and filing, inherent in the Member State's law for such contracts. A comprehensive list can be found at Kuner, *supra* note 7, at Appendix 12.

9 Other derogations (exceptions that permit transfer of personal data outside of the EU), such as consent of the data subject, are typically construed narrowly and not intended to facilitate bulk transfers, but are intended to apply to the transfer of specific data for a single purpose.

10 Commission Decision of 5 February 2010 on Standard Contractual Clauses, 2010/87/EU, *supra* note 8.

Moreover, if Safe Harbor is untenable because of the CJEU's concern that U.S. federal agencies will have unfettered access to EU personal information, that very same concern applies to any personal information transferred to the U.S. under any transfer vehicle, be it BCRs, SCCs, or even consent of the data subject. It may be argued that no transfer of personal information from the EU to the U.S. should be permitted, as the rationale cited by the CJEU to defeat Safe Harbor certification would equally condemn BCRS and SCCs.

Already the French Commission Nationale de l'Informatique et des Libertés (CNIL) has specifically addressed this "elephant in the room" in their press release of October 7, stating that the invalidation of the adequacy decision raises the question of the level of protection of data transferred to the Unites States, and that data protection authorities will need to take into account that the American situation is not 'adequate', when examining the validity of the transfers that are submitted to them for approval.[11] As we write this paper, we are receiving reports that the DPA in the German state of Schleswig-Holstein has issued a position paper recommending that companies using SCCs and consent mechanisms cancel those arrangements with their U.S. partners and do a complete review of all data transfers in consultation with the authority, and that the European Parliament is holding a plenary session "to ask the Commission to clarify the legal situation following the (Safe Harbor) ruling and demand immediate action to ensure effective data protection for EU citizens."[12]

Step 3: We know, that we know nothing.

While concerns about the blanket access that U.S. (and other national) surveillance agencies may have to personal data, which led to the CJEU judgment, are certainly reason for concern, the judgment did not concern itself with the political or practical consequences of the outcome.[13]

---

[11] Commission Nationale de l'Informatique et des Libertés, *Invalidation du « safe harbor » par la Cour de Justice de l'Union européenne : une décision clé pour la protection des données*, Oct. 7, 2015, http://www.cnil.fr/linstitution/actualite/article/article/invalidation-du-safe-harbor-par-la-cour-de-justice-de-lunion-europeenne-une-decision-cl/.

[12] Sam Pfeifle, *Safe Harbor Fallout: Commission, Council Debate Parliament; German DPA Takes Next Step*, THE PRIVACY ADVISOR, Oct. 14, 2015, https://iapp.org/news/a/safe-harbor-fallout-commission-council-debate-parliament-german-dpa-takes-next-step/.

[13] *See* Christopher Kuner, *The Sinking of the Safe Harbor*, VERFASSUNGSBLOG, Oct. 8, 2015, http://www.verfassungsblog.de/en/the-sinking-of-the-safe-harbor/#.VhqGBvmqqko.

The EC and U.S. Department of Commerce have been in negotiations for a new Safe Harbor framework since the 2013 EC Communication[14], which raised, among other concerns, those that the CJEU cited to invalidate the current Safe Harbor. It is generally understood that these negotiations are approaching conclusion, however, the CJEU judgment may force the parties to remain at the table longer. With the suggested independence of the DPAs to review transfers made under binding adequacy decisions, a new Safe Harbor may not bring back the previous relative harmony.[15]

The CJEU judgment may also have an impact on the ongoing trialogue negotiation for the GDPR, which is expected to finish by the end of this year. Among the questions are whether the international transfers chapter will be re-opened with respect to the derogations, and the fate of controversial provision regarding governmental and judicial law enforcement requests issued by third countries (the so-called "anti-FISA" clause).[16] We may see indirect fallout from the ruling in the final version of the "anti-FISA" clause in the GDPR, with whatever further restrictions it may bring.

On the practical side, particularly with respect to onward transfers in the context of litigation or investigations, the effect of the CJEU judgment is not immediately certain. Sophisticated litigation support providers and their clients have often relied on Safe Harbor certifications for review purposes, and will now have to look for alternative means. However, the onward transfer of data to requesting parties in the U.S. has generally been outside the Safe Harbor framework, and onward transfer restrictions will still have to be carefully reviewed on a case-by-case basis. The advice issued by the Article 29 Working Party as well as The Sedona

---

14 European Commission, *Communication from the Commission to the European Parliament and the Council on the Funbctioning of the Safe Harbour*, COM(2013) 847, Nov. 27, 2013, http://ec.europa.eu/justice/data-protection/files/com_2013_847_en.pdf.

15 The recent "Umbrella Agreement" for the exchange of information for law enforcement purposes may address some of the concerns raised in the CJEU judgment, but it is on hold until H.R. 1428, the Judicial Redress Act of 2015, is passed into law, which will extend provisions of the U.S. Privacy Act to EU citizens. *See also* Drinker Diddle & Reath LLP, *CJEU declares Safe Harbor Framework invalid*, Oct. 6, 2015, http://www.lexology.com/library/detail.aspx?g=0c3eb36a-82c4-4204-9935-bd36fb139400.

16 This clause was included in the first leaked version of the GDPR proposed by the EC, removed from the official version of the EC, and re-included by the European Parliament. If kept as currently proposed by the European Parliament, it would require EU data exporters to obtain the prior DPA authorization in order to disclose data requested by a third country's authority, including documents required in litigation by U.S. court rules or a U.S. court order.

Conference Working Group 6[17] continue to be important guidance on navigating these issues. With regard to day-to-day data transfers, privacy law expert Dr. Christopher Kuner observes that "[s]etting an unrealistic standard for adequacy and inciting individuals to have adequacy decisions reviewed by the CJEU (see paras. 61-65) makes a system that is already slow and cumbersome, with only 12 decisions issued in 17 years (11 minus the Safe Harbor), even more glacial."[18]

The EC and the national DPAs are aware of the fact that the CJEU judgment has major consequences for any EU organisations exchanging data with the U.S. on the basis of the Safe Harbor (e.g., with U.S. parent companies, U.S. vendors, or otherwise). The Schleswig-Holstein DPA is only one of 16 in Germany and does not speak for their general conference, which also includes the Federal Data Protection Authority. It is obvious though, that clear, uniform guidance and time are needed in order to both analyze the impact of the CJEU judgment and implement realistic alternative mechanisms—outside of moving the data back to the EU.

---

[17] THE SEDONA CONFERENCE INTERNATIONAL PRINCIPLES ON DISCOVERY, DISCLOSURE & DATA PROTECTION, Dec. 2011, https://thesedonaconference.org/download-pub/495.

[18] *Supra* note 13.