Westlaw Journal
COMPUTER & INTERNET
Litigation News and Analysis • Legislation • Regulation • Expert Commentary
VOLUME 33, ISSUE 11 / NOVEMBER 6, 2015

EXPERT ANALYSIS

European Court of Justice Rules U.S.–EU 'Safe Harbor Program' Invalid

By Kenneth N. Rashbaum, Esq.
Barton LLP

The Court of Justice of the European Union ruled Oct. 6 that the U.S.–EU "safe harbor program," under which multinational organizations transferred digital information from the European Union to the United States, is invalid. Previously, organizations that had registered with the program, administered by the U.S. Department of Commerce, self-certified that they would safeguard personal data they transferred from the EU to the United States in accordance with certain data protection principles (described below). Data trans-ferred under these circumstances met the European Commission's standard for adequate protection of EU citizens' personal data.[1]

You may have read articles or blog posts about this decision that imply that all data already in the United States under the safe-harbor program are at immediate risk, or that all transfers of personal information from EU countries will immediately grind to a halt. Neither is the case at the moment, but planning for alternative means for transferring data should begin now.

The decision, distilled to its essence, holds that individual EU countries are now free to decide whether to suspend transfers of personal data under the auspices of the safe-harbor program.

The court ruled that European Commission decision 2000/520/EC authorizing transfers under the safe-harbor program[2] is invalid because it deprived member states of the right to pursue their own determinations of whether the program provides an adequate level of protection in the face of changed circumstances following the disclosures of Edward Snowden regarding National Security Agency's "mass and undifferentiated accessing of personal data" in the United States.[3]

The case was brought by Max Schrems, an Austrian student and Facebook user. When Schrems opened his Facebook account, he agreed that Facebook Ireland would host his data which, would be sent to Facebook U.S. for processing, as is the case with all EU Facebook users. The data had been sent to the U.S. under the auspices of the safe-harbor program.

In 2000, the European Commission authorized personal data transfers to the United States under this program, which comprises seven principles of data protection consistent with EU law:

- Notice: Information provided to individuals about the purposes for which it collects and uses information about them, the types of third parties to whom the organization provides that information and what choices and methods are offered to individuals to limit information uses and disclosures.

- Choice: The opportunity for the individual to opt out where their personal information is to be disclosed to a third party or used in a manner incompatible for the purpose for which it was collected.

- Onward transfer: A restriction on transfer of an individual's information to a third party without consent, or unless that organization subscribed to the "Safe Harbor Principles."

Previously, organizations self-certified that they would safeguard personal data they transferred from the EU to the United States in accordance with certain data protection principles.

- Security: Reasonable precautions to protect information from loss, misuse or unauthorized disclosure.
- Data integrity: A restriction on processing data in a manner inconsistent with the rationale for its collection, and reasonable steps to insure that the data is accurate, complete and current.
- Access: an individual must have access to the information about themselves held by the organization, and be provided with the opportunity to correct, amend or have it deleted, subject to certain limitations.
- Enforcement: Provision of access to mechanisms for recourse for aggrieved individuals. This takes the form of a requirement that registered organizations designate a private dispute resolution forum (there is, at present, no redress in U.S. courts for EU citizens aggrieved by unauthorized disclosures that take place in the United States).[4]

Schrems filed a complaint with the Data Protection Authority in Ireland, alleging that his Facebook data was not adequately protected due to NSA access to all data within the United States, as revealed by Snowden.

One of the more salient aspects of the European Commission 2000 decision, 2000/520 EC, is that it was binding on all EU member states; that is, no member state could challenge the finding that transfers to the United States under the safe-harbor program offered an adequate level of privacy protection — until now.

The European high court reasoned that it had the authority to revisit the 2000 decision on safe harbor because the "level of protection by a third country is liable to change ... so it is incumbent on the commission to check periodically whether the finding relating to the adequacy of the level of protection ensured by the third country in question is still factually and legally justified. Such a check is required, in any event, when evidence gives rise to a doubt in that regard."[5]

Accordingly, the court ruled the 2000 decision formerly binding on all EU member states is invalid so that data protection authorities, or DPAs, of individual countries may now make their own determinations of whether data transfers pursuant to safe harbor offer an adequate level of data protection. If the relevant DPA finds that the program no longer offers an adequate level of protection, it may order transfers of personal data under the program suspended.

On Oct. 16 the German DPA did just that. It suspended all transfers from Germany to the United States pursuant to the safe-harbor program.[6] And the fallout may not be limited to the EU.

Israel has also suspended transfers pur-suant to the program. Israel, a country the EU has deemed to have data protection commensurate with its own, had previously approved data transfers to companies registered with the program. Many American technology companies, such as Google, Intel, Microsoft and HP, have a significant presence in Israel. On Oct. 19, the Israeli Law, Information and Technology Authority, the country's data protection authority, known as ILITA, also announced that "it is no longer permissible to rely on the safe harbor as a basis for transfers of personal data from Israel to the [United States]."[7]

Other DPAs may make their decisions based on EU standards or their own culture and privacy laws, but there is no way to know the criteria for such decisions at this time. It is not at all clear, though, that other DPAs will follow suit.

Yet, on the same day, the Article 29 Working Party on Data Protection issued a statement in which it stated that "transfers that are still taking place under the safe-harbor decision after the CJEU decision are unlawful," but also implied a grace period until the end of January. *After that time*, "EU data protection authorities are committed to take all necessary and appropriate action, which may include coordinated enforcement actions," the statement said.[8]

Deputy Commissioner David Smith from the Information Commissioner's Office in the United Kingdom offered similar comments in response to the *Schrems* decision.

"The judgment means that businesses that use safe harbor will need to review how they ensure that data transferred to the U.S. is transferred in line with the law," he said, adding that his office recognizes it will take some time for them to do this.[9]

CONSIDER THE OPTIONS

The European Court of Justice's decision leaves the question of suspension of transfers to individual, state DPAs. The court remanded the case to the High Court of Ireland, which had certified the question of local DPA jurisdiction. Now, the High Court of Ireland will conduct its own protection adequacy investigation and make its own findings.

As stated above, individual DPAs may not act for some time, but some may act within weeks, some longer and others may not act at all. Further, the decision is phrased prospectively, in that it does not speak to data that is already in the United States pursuant to safe harbor. There is no mandate to do anything with data already here under the program.

It is nonetheless strongly advisable to begin consideration of options and alternatives.

First consider the EU countries from which the organization would obtain personal data and evaluate how quickly their DPAs are likely to move on this.

While some DPAs may not have the resources to consider the question of suspension right away, others may jump on this quickly, as Germany has. The suspension of data flows from Europe for such organizations could have serious business consequences.

If the local DPA suspends safe-harbor transfers, another instrument for data transfer will be required quickly so your data transfers may continue.

Personal data may be transferred to the United States with a data transfer agreement using model contract clauses. These clauses have been approved by all member states, and do not require approval by DPAs (though a data transfer agreement itself must be submitted to the relevant DPA).

Another approved method for data transfer is a set of binding corporate rules, a "code of conduct" that defines global policy with regard to internal transfers between entities of multinational organizations. Binding corporate rules can function as a global data protection code of conduct, but in the European Union they require approval by the pertinent DPA.[10]

There are advantages and disadvantages to each of these solutions, but if the local DPA in the country from which your organization would be receiving data suspends transfers that had been made under the safe-harbor program, adoption of one of these methods will be required within a very short period of time.

But there is another consideration, with a potentially sunnier side: does the organization fit within recognized exceptions "derogations" to the transfer of personal data? Article 26 of the Directive comprises a number of derogations that may apply and, if they do, no instrument may be required for data transfers. These include:

- Consent of the data subject (which must be informed and freely given).
- Data transferred "for the establishment, exercise or defense of legal claims."
- The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party.[11]

Consent, it has been said, cures a variety of sins if it is provided voluntarily and is "unambiguous."[12] Many multinational organizations have employees sign agreements that state the employee consents to his or her email and other information to be transferred beyond the European Economic Area (comprising the EU member states, Norway, Iceland and Liechtenstein). In those countries where consent obtained by an employer is not considered involuntarily given, this could suffice.

Individual EU countries are now free to decide whether to suspend transfers of personal data under the auspices of the safe-harbor program.

Binding corporate rules can function as a global data protection code of conduct, but in the European Union they require approval by the pertinent data protection authority.

More and more organizations may try, in the wake of the *Schrems* decision, to go the consent route by use of "click boxes" for online agreements, which can produce its own set of concerns for overuse of the consent derogation.[13]

The derogation for transfers in connection with defense or establishment of a legal claim may be of considerable use for digital consultants such as e-discovery vendors.

The Article 29 Working Party on Data Protection, in 2009, issued Working Document WP158 that stated that transfers to common-law countries outside the European Union may take place for purposes of litigation if the personal data set were reduced by culling and filtering for sensitive and irrelevant data, so as to mitigate, to a degree, the potential privacy intrusion on the EU data subject.[14]

Indeed, one can make a compelling argument that the safe-harbor program was never an appropriate transfer method for these organizations, since litigation data collection is performed with the purpose of ultimate disclosure to a court and/or adversary, and a core safe-harbor principle was that data transferred pursuant to program would not be subject to onward transfer, including production of these data to courts or adversary counsel.

A third useful derogation is a contract that requires data transfer for the performance of a contract, which is in the data subject's interest. Transfers of health data between a treating hospital in, say, France and a consulting physician in the United States or, arguably, certain transfers of financial information of the data subject from her bank in Belgium to her investment advisor in New York, may fit within this derogation.

CONCLUSION

Perhaps the best practical counsel one can provide is breathe, keep calm and consider all the alternatives. Safe harbor still exists in the United States, and as of this writing no data protection authority has ordered transfers under safe harbor suspended.

But that day is likely coming soon, so planning should rise to the top of a multinational organization's "urgent" pile.

Analysis should begin with the question of whether the organizations' transfers qualify for derogation under Article 26, in which case it is possible that no alternative transfer instrument may be needed at all.

If the transfers do not so qualify, the next step in the analysis should include the type of information transferred, the volume of data transfers, and the feasibility of alternative methods of transfer of protected data given the nature of the organization's business and culture.

NOTES

[1] U.S.-EU Safe Harbor Overview, U.S. Dep't of Commerce (last updated Dec. 18, 2013), *available at* http://1.usa.gov/1GvVxhl.

[2] 2000 O.J. (L 215) 7, *available at* http://bit.ly/1RxUqOi.

[3] *Schrems v. Data Prot. Comm'r*, CJEU Case C-362/14 (Oct. 6, 2015), *available at* http://bit.ly/1XuircM.

[4] *Safe Harbor Privacy Principles*, U.S. Dep't of Commerce (July 21, 2000), *available at* http://1.usa.gov/1GvUGgo.

[5] *Schrems, supra* note 3, at *29.

[6] Christoph Ritzer, Christoph Zieger, Daniel Ashkar & Marcus Evans, *German Data Protection Authorities Suspend BCR Approvals, Question Model Clause Transfers,* Data Prot. Rep. (Oct. 26, 2015), http://bit.ly/1PSOjpw.

[7] Angelique Carson, *Safe Harbor Decision Trickles Down: ILITA Revokes Prior Authorization,* Privacy Advisor (Oct. 20, 2015), http://bit.ly/1WgpJUx. *See also* Francoise Gilbert, *Israel Revokes is Acceptance of Safe Harbor* (sic.), Francoise Gilbert on Privacy, Security and Cloud Computing (Oct. 20, 2015), http://bit.ly/1k7O0uq.

[8] *See* Press Release, Article 29 Working Party, Statement on Schrems Judgement (Oct. 16, 2015), http://bit.ly/1jPinpU.

[9] *See* Press Release, Info. Comm'r's Office, ICO Response to ECJ ruling on personal data to US Safe Harbor (Oct. 6, 2015), http://bit.ly/1GH4ZxU.

[10] *See Overview on Binding Corporate rules,* European Commission, *available at* http://bit.ly/1kIBUIJ (last visited Oct. 26, 2015).

[11] EU Directive 95/46/EC – The Data Protection Directive, Art. 26 (1), Data Prot. Comm'r, http://bit.ly/1LxGkek.

[12] *Id.*

[13] *See* Nicola Regan, *How Max Schrems Scored an Own Goal by Toppling Safe Harbor*, IAPP Privacy Perspectives (Oct. 7, 2015), http://bit.ly/1Mfbpkf .

[14] *See* Art. 29 Data Protection Working Party, Working Document 1/2009 on Pre-Trial Discovery for Cross-Border Civil Litigation, 00339/09/EN WP 158 (Feb. 11, 2009), *available at* http://bit.ly/1Wel2VZ.

Kenneth N. Rashbaum is a partner at **Barton LLP** in New York, where he heads the privacy and cybersecurity practice. He counsels clients on federal and state laws, industry regulations and international standards for information governance, and he represents multinational organizations and health care providers in government proceedings and litigation regarding privacy and security. He is also an adjunct professor at the Fordham University School of Law. He can be reached at krashbaum@bartonesq.com. A version of this article appeared in Barton LLP's Oct. 9 client alert.