Allianz Global Assistance USA offices in Richmond, Virginia, photo by Bill Dickinson. Sky Noir Photography.

Exchanges of Personal Data between the EU and the US: After the Safe Harbor

Understanding the ECJ's "Safe Harbor judgment" and an outlook on its impact on Trans-Atlantic data exchanges

by Jana C. Fuchs

The European Court of Justice's (ECJ) decision to invalidate the "Safe Harbor" raises more questions than it answers. For EU companies that exchange personal data with US-based companies or have such data processed in the US, the primary effect of the ECJ's judgment is legal uncertainty. Internal structures for data transfers to the US are now subject to scrutiny. Affected companies cannot resolve the conflicts between US and EU data protection laws without assistance from policy-makers. Although the announcement of a new negotiated framework called "Privacy Shield" suggests a political solution is emerging, it is still too soon to tell if this new framework will hold against the ECJ's judgment.

When information not meant for the public was released in the summer of 2013, people learned that international governmental agencies in both the US and in the EU (e.g., in the United Kingdom) have extensive powers to access personal data, above all online. Because of the revelations by whistleblower Edward Snowden, the PRISM program became known as the basis for extensive spying on global Internet applications by the US National Security Agency (NSA).

At the center of the issue was Facebook, which supplied the NSA with extensive user data. Maximilian Schrems was a Facebook user starting in 2008. In an effort to prevent the transfer of his user data to US security agencies and intelligence services, Schrems filed a claim on June 25, 2013, with the Irish data protection authority. He called upon the authority to prevent Facebook from transferring his personal data to the US-based parent company. He argued that US law and practice fail to adequately protect the personal data stored there from access and surveillance by the US authorities.

The Irish data protection authority dismissed Schrems's claim for two reasons. First, it noted that there was no evidence that Schrems's personal data had been accessed by the NSA. Second, the Irish data protection authority pointed out that Facebook, as a company certified under the "Safe Harbor" framework established by the US Department of Commerce, ensures an adequate level of data protection to satisfy the European Data Protection Directive, Directive 95/46/EC.

US-based Facebook Inc., like more than 4,000 other companies of various sizes and organizations, had been certified in accordance with the "Safe Harbor" rules until the recent decision by the European Court of Justice (ECJ). Consistent with the EU Commission's fifteen-year-old "Safe Harbor decision"[1] US-based companies that were Safe Harbor-certified were deemed to have an adequate level of data protection in accordance with the standards of EU law.

Schrems appealed the decision of the Irish data protection authority to the courts. The Irish High Court found that Irish national data protection law prohibits the transfer of data to the United States despite the Safe Harbor, since an adequate level of data protection cannot be ensured. It noted, however, that the matter is not governed by Irish law exclusively. Rather, it stated that the case relates to the implementation of EU law and that the Safe Harbor decision must be assessed exclusively in accordance with EU law. The Irish High Court further declared that, with his complaint, Schrems was in effect questioning the lawfulness of the Safe Harbor decision. However, a formal challenge to the Safe Harbor decision had not been made.

Questions Referred to the ECJ

The Irish High Court ordered a stay of proceedings and presented questions, which are reproduced below in simplified form, to the ECJ for preliminary ruling:

Question 1: Is a data protection authority bound by the finding of the Safe Harbor decision when making its determination in connection with a complaint related to the inadequate protection of personal data that is being transferred to a third country, notwithstanding the provisions of Article 25(6) of the Data Protection Directive?

Question 2: Alternatively, may and/or must a data protection authority conduct its own investigation of the matter and consider factual developments since the Safe Harbor decision was first published?

Neither question referred to the ECJ explicitly challenged the validity of the Safe Harbor decision.

Briefly, the ECJ's judgment of 6 October 2015[2] can be summarized as follows:

Question 1: No

Question 2: Yes

Unasked: The Safe Harbor decision is invalid.

Because of the revelations by whistleblower Edward Snowden, the PRISM program became known as the basis for extensive spying on global Internet applications by the US National Security Agency (NSA).

The ECJ answered the questions posed by the Irish High Court in its first ruling, which states:

> "Article 25(6) of the Data Protection Directive, read in the light of Articles 7, 8 and 47 of the Charter of Fundamental Rights of the European Union (the Charter), must be interpreted as meaning that a decision adopted pursuant to that provision, such as the Safe Harbor decision, by which the European

> Commission finds that a third country ensures an adequate level of protection, does not prevent a supervisory authority of a Member State, within the meaning of Article 28 of the Data Protection Directive, from examining the claim of a person concerning the protection of his rights and freedoms in regard to the processing of personal data relating to him which has been transferred from a Member State to that third country when that person contends that the law and practices in force in the third country do not ensure an adequate level of protection."

In its second ruling, the ECJ went beyond the scope of these questions and ruled, without solicitation, that the Safe Harbor decision is invalid. As grounds for its decision, the ECJ stated that, in view of its findings with regard to the questions posed by the Irish court, a determination was necessary as to whether the Safe Harbor decision met the requirements of the Data Protection Directive and the charter.

In view of the substantial and direct impact of the judgment, the procedural grounds cited by the ECJ to invalidate a decision whose validity had not been challenged are questionable at the very least.

Significance of the Safe Harbor Judgment

The ECJ's Safe Harbor judgment means that companies that until now had either been Safe Harbor-certified themselves or worked with Safe Harbor-certified service providers will have to modify the legal structure of their data transfers and, in some cases, will have to technically restructure those transfers. As of October 6, 2015, the Safe Harbor no longer ensures an adequate level of data protection in the US.

For now, and until the Privacy Shield is implemented first by policy makers and then by concerned companies, there remain only certain ways to legally transfer personal data from the EU into the US.

In February 2016, the EU and the US announced a new privacy framework called Privacy Shield, which resulted from written assurances that US law enforcement and national security agencies will not indiscriminately conduct mass surveillance on personal data transferred to the EU, and that they will implement "clear limitations, safeguards, and oversight mechanisms" to protect privacy. The US also agreed to conduct an annual joint review on privacy issues and to appoint an ombudsman to field complaints from EU citizens. However, the details of this new framework and the effects it will have on companies on both sides of the Atlantic remains unknown until the terms of the agreement are finalized, which is expected in about three months.

For now, and until the Privacy Shield is implemented first by policy makers and then by concerned companies, there remain only certain ways to legally transfer personal data from the EU into the US.

1. Use of standard contractual clauses

A data controller can use standard contractual clauses that ensure sufficient data protection safeguards for the transfer of personal data to a third country. Pursuant to Article 26(4) of the Data Protection Directive, the EU Commission was authorized to develop standard contractual clauses for data transfers to countries which do *not* ensure an adequate level of data protection. In practice these clauses are also used in cases where the level of data protection in the recipient country cannot be evaluated by the data controller in a definitive manner.

To date, the EU Commission has approved three sets of standard contractual clauses. Two apply to the transfer of data by a controller in the EU to a controller in a third country (a controller-to-controller transfer). The third applies to transfers between a controller in the EU and a processor which processes personal data outside of the EU (a controller-to-processor transfer).

Not covered by standard contractual clauses is the processing of data by a service provider both within (e.g., through subcontractors) and outside of the EU if the processor, in its function as a contract data processor, processes data, either within its corporate group or through subcontractors, for the purpose of executing an order. The Article 29 Working Party[3] developed a draft agreement (processor-processor transfer) but the EU Commission never approved of the draft.[4] In these situations, the Safe Harbor played a dominant role in practice since controllers in the EU cooperated with IT service providers which were positioned internationally, and whose data processing activities often were not confined to any one location.

2. Binding corporate rules

Binding corporate rules (BCR) can also ensure sufficient data protection safeguards for data transfers within a corporate group.

One advantage of such binding corporate rules (in the form of binding internal company data protection policies) is that they are approved by a competent data protection authority after that authority consults with other data protection authorities. As a result, they constitute an individualized form of approval by the supervisory authorities.

Companies with approved binding corporate rules can rely on the fact that, at the time the approval was issued, the competent data protection authority took the view that the policies ensured sufficient safeguards of data protection to allow the exchange of data within the corporate group (including transfers to the US). The legal basis on which data protection authorities can withdraw or modify their approval of BCRs (particularly if it has been established that the corporate group has not violated the BCRs) may be open to question depending on any ancillary provisions and, in case of doubt, may have to be clarified by the administrative courts.

3. Consent

Consent is a permissible means of affording legal protection to the transfer of data to a third country with no additional measures. This rule benefits providers that are in contact with customers, as they are in a position to obtain such consent in the first place. Consent must be declared beyond any doubt. In accordance with the applicable local laws, the rule is that consent requires a free and informed decision.

The requirement that requests for consent be transparent and clearly indicate the intended transfers and that consent be voluntarily given often creates challenges for companies. This is particularly the case with regard to employees, where it is often assumed in many EU countries that, because of the hierarchical relationship between employer and employee, consent cannot be freely given. In addition, consent must be able to be revoked at any time without citing the reasons for the revocation.

4. Contracts with Data Subjects

Another rule for data transfers to a third country can be found in Article 26(1)b of the Data Protection Directive. Under this rule, the transfer of data to a third country without an adequate level of data protection for the performance of a contract between the data subject and the controller is permissible, provided the data transfer is necessary for performance of the contract.

This is comparable to the rule in Article 26(1)(c) of the Data Protection Directive, under which a data transfer is allowed to the extent necessary for performance of a contract which was concluded in the interests of the data subject between the controller and a third party.

In both cases, companies would face legal challenges given the fact that the definition of necessity is subject to a broad range of interpretations. In general, however, "necessity" requires a close and material connection between the data subject and the purposes of the contract in each case.

The data protection authorities have already opposed an all too broad interpretation of this exceptional rule in an opinion from the Article 29 Working Party, formulating strict requirements for the criterion of necessity.[5]

5. Individual approval

Finally, the data protection authority of each Member State can approve data transfers to a third country.

Like binding corporate rules, individual approval by the competent data protection authority affords legal certainty in that an administrative act exists which provides security for the controller within the framework of national laws. It also remains to be seen whether the data protection authorities will make use of this authority, which has existed since the Data Protection Directive took effect, to make their own determinations as to whether a third country can ensure an adequate level of data protection, in order to avoid possible individual approval procedures.

Conclusion

Until the uncertainty arising from the Safe Harbor judgment is resolved, companies will need mechanisms to address data transfers between the US and the EU. Standard contractual clauses, individual approvals, or consent do not limit the rights of the security agencies to access personal data. Companies need a reliable legal framework as soon as possible that ensures a sound foundation for the transfer of data to the US. At the same time, the fundamental right to data protection in light of investigations by secret services should be secured not just for data transfers to the US, but

Safe Harbor *continued on page 37*

Safe Harbor *continued from page 33*

for data transfers within the European Union as well.

The agreement on a "Privacy Shield" marks a step towards a reliable legal framework for data transfers between the EU and the US. Where the Safe Harbor judgment was also interpreted as affecting the validity of standard contractual clauses and binding corporate rules, clear and uniform guidance from the EU regulators will hopefully be forthcoming. On February 3, 2016, the Article 29 Working Party announced that they will analyze the standard contractual clauses and binding corporate rules in light of the Privacy Shield agreement. Until that assessment is finalized, the Article 29 Working Group assumes that those alternative data transfer tools may still be used.

Endnotes:

1 Decision 2000/520 of the EU Commission

2 ECJ, 6 October 2015, Case No. C-362/14.

3 The Article 29 Working Party was established within the framework of the Data Protection Directive, Directive 95/46/EC. It is an independent advisory group and consists of a representative from the data protection authorities of the member states, the EU data protection authority and the European Commission.

4 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp214_en.pdf (viewed: 1 December 2015)

5 Artikel-29-Group WP 114

Jana C. Fuchs is an associate in the Hamburg, Germany, office of Bryan Cave LLP. She started her legal career in-house at an international IT company headquartered in the United States. She focuses her practice in the areas of trade compliance and data protection law.