Client Update

Transfers of Personal Data to the United States: European Court of Justice Rules the Safe Harbour Protocol Is Potentially Invalid

FRANKFURT
Dr. Thomas Schürrle
tschuerrle@debevoise.com

LONDON
Karolos Seeger
kseeger@debevoise.com

Matthew H. Getz
mgetz@debevoise.com

NEW YORK
Jeremy Feigelson
jfeigelson@debevoise.com

Jim Pastore
jpastore@debevoise.com

WASHINGTON, DC
Jeffrey P. Cunard
jpcunard@debevoise.com

David A. O'Neil
daoneil@debevoise.com

In a decision that could have significant implications for the transfer of personal data from the European Union to the United States, the Court of Justice of the European Union (the "CJEU") today ruled that the approval previously granted by the European Commission (the "Commission") to the EU-US Safe Harbour protocol ("the Safe Harbour") is not valid. The Safe Harbour has been one of the ways in which personal data may be transferred from countries within the EU to the United States in conformity with the EU Data Protection Directive 95/46/EG (the "Directive"). As a consequence of this decision, companies that have registered under the Safe Harbour can no longer be certain of their ability to rely on that protocol as a lawful method to make such transfers.

BACKGROUND

The Directive and the legislation implemented by Member States of the EU[1] and the other members of the European Economic Area (the "EEA"), which comprises the EU, Iceland, Liechtenstein and Norway, allow transfers of personal data from EU countries to countries outside the EEA only under limited circumstances. Either the destination country must provide an "adequate level of protection" to personal data, or one of a specific set of other conditions must apply to the transfer.

The Commission has made determinations that a number of individual third countries ensure an adequate level of protection, allowing transfers to those countries subject only to the same restrictions on transfers within the EEA.

[1] Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, and the UK.

Although the United States is not among those countries, the United States Department of Commerce and the European Commission agreed upon the Safe Harbour framework in 2000, to enable the transfer of personal data to the Safe Harbour registrants in conformity with the Directive.

Under the Safe Harbour, companies subject to the jurisdiction of the US Federal Trade Commission or the US Department of Transportation could, by registering with the Department of Commerce, self-certify that they apply the following protections to EU-originating personal data: (i) they agree to notify individuals about the purposes for which they collect and use information about them; (ii) individuals are given the opportunity to choose (opt out) whether their personal information will be disclosed to a third party or used for a purpose incompatible with the purpose for which it was originally collected or subsequently authorised; (iii) they take reasonable precautions to protect personal information from loss, misuse, and unauthorised access, disclosure, alteration, and destruction; and (iv) individuals have access to personal information about them that an organisation holds and be able to correct, amend, or delete that information where it is inaccurate.[2]

CLAIM

The CJEU came to consider the validity of the Safe Harbour as a result of a claim relating to Facebook brought by Maximilian Schrems, an Austrian citizen. As with the Facebook data of other users within the EU, some or all of the data provided by Mr. Schrems to Facebook are transferred from Facebook's Irish subsidiary – its main operating arm in the EU – to the United States using the Safe Harbour, to which Facebook subscribed. Mr. Schrems complained to the Irish data protection regulator that the revelations made by Edward Snowden in 2013 concerning the activities of the US intelligence services meant that the United States did not offer sufficient protection against surveillance over his transferred personal data. The Irish regulator rejected his complaint, primarily on the ground that Facebook had self-certified that it complied with the Safe Harbour protocols, which had been approved by the Commission, and the regulator had no power to make a finding contrary to the Commission's determination. Mr. Schrems pursued the issue in the Irish courts, as a result of which the CJEU was called on to consider the issue.

DECISION

In today's decision, the CJEU ruled that that the Commission decision endorsing the Safe Harbour protocol does not limit the powers available to a national data

[2] For additional information about the substance of the Safe Harbour protocols, see https://safeharbor.export.gov/list.aspx.

protection supervisory authority. As a result, national regulators are able and required to examine whether the transfer of data to a third country complies with the applicable legal requirements, regardless of any previous determinations by the Commission.

Therefore, it ruled that the Irish regulator should have made a ruling on whether data transferred under the Safe Harbour would receive an adequate level of protection.

As a next step, the CJEU stated that if a regulator did find that transfers under the Safe Harbour – or pursuant to a different Commission determination – provided inadequate protection, then legal proceedings must be commenced, as only the CJEU has jurisdiction to declare a Commission decision invalid.

Consequently, the CJEU went on to consider whether the Commission's decision relating to the Safe Harbour was valid: it determined that it was not.

The CJEU determined that the Safe Harbour no longer offers adequate protection for two reasons.

First, the CJEU noted that companies subject to US law are bound to disregard the Safe Harbour's rules and protocols protecting data privacy if they conflict with the national security, public interest, and law enforcement requirements of the United States. As a result, the Safe Harbour does not prevent, and indeed enables, interference by US public authorities with the fundamental rights of individuals, as guaranteed by EU human rights law. The CJEU held that legislation allowing US authorities to have access on a generalised basis to the content of electronic communications, without regard for necessity and notwithstanding the Safe Harbour's protections, compromised the fundamental right to respect for private life as reflected in EU human rights law.

Second, the CJEU considered individuals' rights of redress against surveillance by US authorities. The court found that individuals subject to surveillance of their personal data could not pursue adequate legal remedies in order to access, rectify, or erase the data, and held that the absence of such rights compromised the fundamental right to effective judicial protection.

The CJEU is the highest court of the EU and there is therefore no appeal against its judgment to any other court within the EU. The immediate consequence of the decision is that the Irish court (and possibly the Irish data protection authority at some stage) must consider Mr. Schrems's complaint and decide whether the transfer of the data of Facebook's European users to the United States should be suspended on the ground that the United States does not afford

an adequate level of protection of personal data. It will need to do so by considering the factual and legal aspects of the treatment of personal data in the United States.

The wider implications remain to be seen, but may be significant. On the one hand, because the CJEU ruled that data protection authorities must be allowed to review and challenge any previous determinations of the Commission, it is possible that there may be challenges not only to the Commission's findings of adequacy in respect of other third countries, but also to the other currently accepted methods of transferring data from the EU to the United States and elsewhere, such as the use of data transfer agreements (which may, however, also come under some scrutiny in the wake of the CJEU's decision).

On the other hand, companies that have registered under the Safe Harbour regime are not prohibited from transferring personal data to the United States. Nonetheless, the arrangements by which they transfer data, and the adequacy of protection in the United States for such data, may be reviewed by the Member States' data protection authorities. The CJEU's decision confirms the authorities' right and ability to review data transfer arrangements, even those subject to the Safe Harbour framework, but the authorities and courts of the Member States may well view the protections offered by the Safe Harbour in different ways. At a minimum, it can be expected that there will be an ongoing dialogue within each Member State as to the adequacy of the Safe Harbour protection standards and whether personal data is otherwise adequately protected when it is transferred by companies to the United States.

Almost certainly, the discussions between the United States and the EU regarding the Safe Harbour will now be reinvigorated, including with respect to developing other means by which data could be transferred to the United States.

Entities that transfer data from the EU to the United States, whether on a regular or *ad hoc* basis, will need to review and assess the meaning of the ruling of the CJEU, and its consequences, whether they rely on the Safe Harbour or on other mechanisms, such as model contracts, that have been sanctioned by the European Commission.

We will provide a more detailed analysis of the ramifications of this judgment in due course.

* * *

Please do not hesitate to contact us with any questions.