IP, IT & Media News from Luxembourg

MOLITOR

October 2015

SAFE HARBOUR RULING DECLARED INVALID BY THE EUROPEAN UNION COURT OF JUSTICE

On 6 October 2015, the European Union Court of Justice ("ECJ") gave its eagerly awaited ruling[1] on the European Commission's Safe Harbour Decision, which authorizes the transfer of personal data from the European Union ("EU") to the United States ("U.S."). Accepting the arguments of the Advocate General Yves Bot, the Court considered that the Safe Harbour Decision is invalid. Here are some key elements on the background and impact of the Court's ruling.

Legal context of personal data transfer

Directive 95/46/CE of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data ("**1995 Directive**") governs the transfer of personal data from the EU to third countries.

As a rule, the transfer of personal data outside the EU is only possible to third countries that ensure an "*adequate level of data protection*" in terms of protection of the private life and basic freedoms and rights of individuals. It is up to the European Commission ("**EC**") to decide whether a third country ensures an adequate level of protection.

Transfers of personal data to a country which does not offer an adequate level of data protection are not impossible but in most cases require the prior authorization of the competent national data protection authority ("**DPA**") and such an authorization is only granted – among other requirements and basically – if an agreement which defines the conditions of the personal data transfer and matches the European data protection requirements is entered into between the sender and the recipient of the data.

The EC has recognized very few countries offering an "*adequate level of data protection*". The U.S., as such, is not part of this very close circle. However, on 26 July 2000 the EC adopted a decision[2] recognizing the "*Safe Harbour Privacy*

[1] EUCJ, Maximilian Schrems v Data Protection Commissioner, Case C-362/14

[2] Decision 200/520/EC

Principles" and "*Frequently Asked Questions*", issued by the U.S. Department of Commerce as providing adequate protection for the purposes of personal data transfers from the EU to the U.S. (the "**Safe Harbour Decision**").

As a result, the Safe Harbour Decision allows for the free transfer of personal data, for commercial purposes, from companies located in the EU to companies located in the U.S. that have adhered to the Safe Harbour principles.

More that 4,000 European and American companies are currently relying, on a daily basis, on the Safe Harbour Decision to transfer personal data from the EU to the U.S., including the major players of the ICT sector (Apple, Microsoft, Google, Facebook, Skype, etc.).

Background of the SCHREMS case

After former National Security Agency contractor Edward Snowden leaked details in 2013 about large-scale U.S. collection and processing of personal data transferred under the Safe Harbour scheme under U.S. surveillance programs, the EC called for a review of the Safe Harbour Decision.

The EC requested guarantees from the U.S. that the collection of EU citizens' personal data for national security purposes would be limited to what is necessary and proportionate. The EC did not follow the European Parliament's suggestion to suspend, in the meantime, the Safe Harbour Decision.

After two years of negotiations, the EC was close to finalizing the details of a new Safe Harbour Agreement with the U.S.

Simultaneously, on 19 September 2014, Maximilian Schrems, an Austrian citizen, filed a complaint with the Irish DPA against an Irish subsidiary of Facebook, which was transferring subscribers' personal data to servers located in the U.S. Schrems claimed that, as shown in the Snowden revelations in 2013 concerning the activities of the U.S. intelligence services, the law and practices of the U.S. offer no real protection against surveillance by the U.S. authorities of the data transferred to that country, and that consequently the U.S. did not offer an "*adequate level of protection*", within the meaning of the 1995 Directive.

The Irish authority rejected the complaint on the ground, in particular, that it had no authority to investigate a complaint challenging a binding decision of the EC (in this case, the Safe Harbour Decision).

The High Court of Ireland, before which the case was brought, then submitted to the ECJ the question of whether or not the Safe Harbour Decision has the effect of preventing a national supervisory authority from investigating a complaint alleging the third country does not ensure an adequate level of protection and, where appropriate, from suspending the contested transfer of data.

SCHREMS Ruling of 6 October 2015

In its ruling of 6 October 2015, the ECJ judged that even if the EC has adopted a decision finding that a third country ensures an adequate level of protection of the personal data transferred, the national DPA, when dealing with a claim against a data controller, must be able to examine, with complete independence, whether the transfer of a person's data to a third country complies with the requirements laid down by the 1995 Directive.

Nevertheless, the Court pointed out that it alone has jurisdiction to declare that an EC decision is invalid.

The ECJ then turned to whether the Safe Harbour Decision was invalid or not, and stressed that the EC was required to establish that the U.S. does in fact ensure, through its domestic law or international commitments, a level of protection of fundamental rights essentially equivalent to that guaranteed by the EU under the 1995 Directive and the Charter of Fundamental Rights of the European Union. The Court pointed out that the EC had not made such a finding, but had merely examined the Safe Harbour scheme.

The ECJ also stated that:

- Legislation permitting public authorities to have access on a generalized basis to electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life; and that

- Legislation that does not provide for any possibility for an individual to pursue legal remedies in order to have access to person data relating to them, or to obtain rectification or erasure of such data, compromises the essence of the fundamental right to effective judicial protection.

For all these reasons, the Court declared the Safe Harbour Decision invalid.

Legal consequences of the Court's ruling for companies relying on the Safe Harbour scheme to transfer personal data from the EU to the U.S.

Following this ruling, both the Safe Harbour scheme and the U.S. will no longer be regarded by national DPAs as ensuring an "*adequate level of protection*" within the meaning of the 1995 Directive for personal data transferred from the EU to the U.S.

Consequently, companies based in the EU which currently rely on the Safe Harbour Decision in order to transfer personal data to the U.S. (i.e. European companies using service providers based in the U.S. or European-based subsidiaries of U.S. companies) will have to suspend their transfers of personal data to the U.S. and find other legal bases to make such transfers.

As mentioned above, as an exception to the general rule of prohibition of personal data transfers to non-safe countries, national DPAs may authorize, on a case-by-case basis, the transfer of personal data to these countries when the data controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals, and as regards the exercise of the corresponding rights.

Such authorization is likely to be given when the data controller has (i) entered into data transfer agreements, based on the EC-approved **model clauses**, with companies located outside the EEA to which it wishes to transfer personal data, or (ii) for multi-national organizations, used **binding corporate rules** which will govern the transfer of data across their international organization.

The question is open as to whether the Luxembourg DPA will consider, in the light of the ECJ's ruling, that European data controllers wishing to transfer personal data to the U.S. are offering adequate safeguards, and, therefore, authorize the envisaged transfer of data.

For more information please contact:

Claire LEONELLI

Partner, Avocat, Member of the Paris Bar and the Luxembourg Bar (list IV)

claire.leonelli@molitorlegal.lu

Claire DENOUAL

Senior Associate, Avocat à la Cour, Member of the Luxembourg Bar

claire.denoual@molitorlegal.lu