TUCA ZBARCEA
ASOCIATII

12 November 2015

Legal Bulletin

Data Privacy

In this issue:

Judgment of the Court of Justice of the European Union in Case C-362/14, Schrems

On 6 October 2015 the Court of Justice of the European Union issued its judgment in Case C-362/14 Schrems v Data Protection Commissioner[1], whereby it invalidated Decision 2000/520/EC[2] acknowledging the Safe Harbor system as providing an adequate level of protection for the transfer of personal data from the European Union to the United States.

As a preliminary issue it should be noted that, pursuant to Article 25 of Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, the transfer of personal data to a third country can only be made if the relevant third country ensures an adequate level of protection, as may be ascertained by the Commission through a decision. Such decisions confirming an adequate level of protection have been issued so far by the Commission[3] for Andorra, Argentina, Canada, Switzerland, the Faeroe Islands, Guernsey, Israel, the Isle of Man, Jersey, the New Zealand and, last but not least, the United States according to the Safe Harbor principles – Decision 2000/520/EC. The latter was challenged and invalidated by the Court through the judgement given in Case C-362/14, Schrems, which affects all EU organizations that transfer personal data to the approximately 4,500 US companies self-certified to observe the Safe Harbor principles.

---

1 The text of the decision is available at *http://goo.gl/t3DeYZ*.

2 Commission Decision 2000/520/CE on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, published in Official Journal No. L215/7 of 25 August 2000, available at *http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000D0520*.

3 The list of countries and links to the relevant decisions of the Commission may be accessed at *http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm*.

BACKGROUD

In June 2013 Max Schrems, a young Austrian using Facebook since 2008, filed a complaint to the Irish data protection authority (the Data Protection Commissioner) requesting it to investigate the manner in which his personal data were transferred from Facebook's Irish subsidiary (Facebook Ireland Ltd.) to Facebook's headquarters in the United States. His position was that in the United States the law did not ensure any real protection of the data, which were easily accessed by the intelligence services, in particular the National Security Agency – NSA, as resulted from the Snowden revelations in 2013.

The Irish data protection authority rejected the complaint, considering that it did not have the obligation to investigate the actions referred to by Schrems in his complaint, since on the one hand there was no proof that NSA had access to his personal data and, on the other hand, any issue concerning the adequate nature of personal data protection in the United States must be solved in accordance with Decision 2000/520/EC, whereby the Commission recognised an adequate level of protection.

Schrems appealed this decision at the Irish High Court[4] which, considering that the documents and statements in the main proceedings, whereby "the accuracy of much of Edward Snowden's revelations is not in dispute", proved that NSA and other federal bodies perpetrated "significant over-reach" against EU citizens, who have no effective judicial remedy, decided to stay the proceedings and submit a reference for a preliminary ruling to the Court of Justice, in order to clarify the validity of the Commission's decision recognising an adequate level of protection conferred by the Safe Harbour agreement. More specifically:

"1) Whether in the course of determining a complaint which has been made to an independent office holder who has been vested by statute with the functions of administering and enforcing data protection legislation that personal data is being transferred to another third party country (in this case, the United States of America) the laws and practices of which, it is claimed, do not contain an adequate level of protections for the data subject, that office holder is absolutely bound by the Community finding to the contrary contained in Commission Decision of 26 July 2000 (2000/520/EC) having regard to Article 7, Article 8 and Article 47 of the [Charter], the provisions of Article 25(6) of Directive 95/46/EC notwithstanding?

2) Or, alternatively, may and/or must the office holder conduct his or her own investigation of the matter in the light of factual developments in the meantime since that Commission Decision was first published?"

[4] Despite its name, in Ireland the "High Court" is a first instance court.

THE JUDGEMENT

The Court of Justice reviewed the matters from the two points of view implied by the questions referred – on the one hand the competences of the national supervisory authorities in the case of an adequacy decision by the Commission, and on the other hand the validity of Decision 2000/520/EC.

As concerns the first issue, the Court concluded that a decision by which the Commission finds that a third party country ensures an adequate level of protection, such as Decision 2000/520/EC, does not prevent a supervisory authority of a Member State 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 (par. 66), however pointing out that the Court alone has jurisdiction to declare that an EU act (such as Decision 2000/520/EC) is invalid, the exclusivity of that jurisdiction having the purpose of guaranteeing legal certainty by ensuring that EU law is applied uniformly (par. 61).

In terms of the second matter, the Court reviewed Decision 2000/520/EC, in particular the fact that "national security, public interest, or law enforcement requirements" have primacy over the Safe Harbor principles, which in the opinion of the Court means that "self-certified United States organisations receiving personal data from the European Union are bound to disregard those principles without limitation where they conflict with those requirements and therefore prove incompatible with them" (par. 86). Furthermore, Decision 2000/520/EC (i) "does not contain any finding regarding the existence, in the United States, of rules adopted by the State intended to limit any interference with the fundamental rights of the persons whose data is transferred from the European Union to the United States" (par. 88) nor does it (ii) "refer to the existence of effective legal protection against interference of that kind" (par. 89). It is precisely in these two areas that the Court found grounds to invalidate Article 1 of Decision 2000/520/EC, concluding that (i) "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" set forth under Article 7 of the Charter of Fundamental Rights of the European Union (par. 94), and that "legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data does not respect the essence of the fundamental right to effective judicial protection" set forth under Article 47 of the same Charter (par. 95).

The Court also invalidated Article 3 of Decision 2000/520/EC, since it lays down specific rules regarding the powers available to the national supervisory authorities in the light of a Commission finding relating to an adequate level of protection (par. 100), while the implementing power of the Commission according to Directive 95/46/EC does not confer upon it competence to restrict the national supervisory authorities' powers (par. 103), which means that in adopting Article 3 of the Decision, the Commission exceeded the power which is conferred upon it in Article 25(6) of Directive 95/46/EC, read in the light of the Charter (par. 104).

WHAT DOES THE SCHREMS JUDGMENT MEAN FOR ROMANIAN DATA CONTROLLERS THAT NOTIFIED THE TRANSFER UNDER SAFE HARBOR?

The judgment under discussion has very wide implications both at State level and, in particular, at the level of companies in which the transatlantic transfer of data plays an important role. One of the main conclusions is that personal data protection requirements in the European Union have reached an extremely high level, and the right to protection of such data is a fundamental one, which the Court of Justice will not hesitate to proclaim as such. In addition, this judgment follows a constant practice after the other significant judgments in the field of mass supervision (C-293/12 and C-594/12, Digital Rights Ireland – invalidating Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks), the business activity of legal entities (C-131/12, Google Spain – the right to be forgotten) and individuals (C-212/13, Ryneš – CCTV systems of individuals).

A practical difficulty is easy to anticipate due to the fact that, in particular as a result of the recent Weltimmo judgment, the same actions could be subject to review (and even sanctions) in several Member States. This is a real problem for multinational companies, considering in particular the diverging opinions of national supervisory authorities. Furthermore, such a fragmented approach shatters the trust in the implementation of a "one-stop-shop" system under discussion to be introduced in the future general data protection regulation.

The reality from which the analysis of the measures to be implemented should start is that, at present, the personal data transfer to the United States under the Safe Harbor is no longer legal and, in accordance with the point of view of Article 29 Working Party (a body comprised of representatives of the supervisory authorities of the EU countries) of 16 October 2015[5], companies have a short period of time – by 31 January 2016, to find and implement an alternative ground.

Given the view expressed by the Romanian National Supervisory Authority for Personal Data Processing[6], the alternative grounds that may be taken into consideration by Romanian companies are the standard contract provisions, binding corporate rules, or the data subjects' express consent to the transfer. None of these options is easy or quick to implement, therefore it is advisable to first review the need to transfer personal data in the United States, with a view to reduce or eliminate any unnecessary transfers. Such a reduction could take place if, for example, data centres in the European Union were used, although even in this case it should be taken into account that US companies may be required, under certain circumstances, to provide information that their foreign affiliates hold for foreign citizens.

---

[5] Available at *http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf*.

[6] See the press release at *http://dataprotection.ro/?page=Transper_date_conf_CJUE&lang=ro*.

Secondly, the agreements concluded with US companies should be reviewed so that, if the agreements do not already contain the standard contractual provisions approved by the European Commission (under Decision 2010/87/EU or Decision 2001/497/EC), the existing agreements are replaced with such standard provisions. In this case it should be taken into account that there are two types of standard provisions: controller to controller and controller to processor, each of which is appropriate in different situations. Furthermore, in addition to the provisions that cannot be amended, the standard provisions approved by the Commission also include appendices the content of which is not predetermined and which the contracting parties must fill in following a detailed analysis – such as the categories of transferred data, the processing method, the technical and organizational measures whereby the US data importer ensures an adequate level of protection according to EU standards.

However, it is possible that, although the data transfer was notified under Safe Harbor, the agreement underlying such transfer already includes the standard contractual clauses. That is because, until 6 October 2015, the notice by a Romanian controller of the data transfer to the United States under the Safe Harbor principles completely eliminated the requirement to have the transfer authorised by the Romanian data protection authority, which is not the case for transfers grounded on standard clauses. As a result, whenever the controller concluded an agreement based standard clauses but the US partner (the data importer) was also Safe Harbor certified, then the notification of the transfer was made on the latter ground in order to eliminate the additional time and stricter formalities related to the authorisation. Currently, after the Schrems decision, the relevant controllers must amend their notifications and change the grounds of the transfer into standard contractual clauses (attaching a copy), then wait for the authorisation of the National Supervisory Authority for Processing of Personal Data. This formality may take up to 4 months, which means that the amendment should be made as soon as possible.

For intra-group transfers of personal data (in particular employee data in multinational companies), controllers may implement binding corporate rules (BCR), although this process is usually difficult and costly.

Last but not least, data controllers may request the consent of the data subjects specifically for the transfer. Although this ground has the advantage of excluding the authorisation requirement, obtaining the consent may prove quite cumbersome or even impossible – for instance, as concerns the data already collected from a significant number of data subjects, and continues to be held, even if passively, by the relevant controllers through processors in the United States of America.

Finally, a matter which cannot be ignored is that the reasoning in the Schrems judgment (i.e. the existence of means of uncontrolled supervision by the US authorities) may also be applied to all the other grounds underlying the transfer of personal data to the United States. Such a drastic interpretation would practically result in the impossibility to transfer personal data to the United States, despite the best efforts made by EU companies as well as US ones. Fortunately, at least for now the approach of the Romanian data protection authority is moderate, allowing the use of all transfer grounds other than Safe Harbor. However, this does not eliminate the requirement for

Romanian data controllers to conduct their own analysis and decide their own measures to be implemented as a result of the invalidation of the Safe Harbor agreement.

As Articles 1 and 3 of Decision 2000/520 were found to be invalid and as the rest of the Decision - Articles 2 and 4 of that decision and the annexes thereto - are inseparable, the Court concluded that the Decision 2000/520/EC is invalid in its entirety (par. 105).

No provisional period was provided for the effects of such decision, which means that the invalidity of Decision 2000/520/EC and implicitly the inefficiency of the Safe Harbor principles occurred immediately, as of 6 October 2015.

andreea.lisievici@tuca.ro

Editors

Ţuca Zbârcea & Asociaţii has developed a significant practice in the **Data Privacy** field, in tune with recent years' increased and thorough supervision of data privacy, both on EU and national levels.

Our services cover all aspects regarding data privacy, from notifying the local regulatory authority (i.e. the National Supervisory Authority For Personal Data Processing – "ANSPDCP") on envisaged data processing by data controllers to providing complex analysis covering sensitive data privacy matters; transfer of various categories of data abroad; access to personal data by personnel of companies pertaining to an international group; monitoring of employees, geolocation, call history; creating data bases comprising subjects' data and use of such data bases by entities other than the collector; legal regime of access to cookies; processing of traffic data; data privacy aspects related to the implementation of cloud computing solutions both for cloud customers, as well as for cloud providers, etc.

For further information and other recent news relating to Data Privacy, please feel free to visit our firm's blog – *dataprivacyblog.tuca.ro*

Cornel Popa
Partner
+4 021 204 88 94
cornel.popa@tuca.ro

Andreea Lisievici
Managing Associate
+4 021 204 88 90
andreea.lisievici@tuca.ro

Ciprian Dragomir
Partner
+4 021 204 88 98
ciprian.dragomir@tuca.ro

Cătălin Băiculescu
Partner
+4 021 204 76 34
catalin.baiculescu@tuca.ro

TUCA ZBARCEA
ASOCIATII

Şos. Nicolae Titulescu nr. 4-8
America House, Aripa de Vest, et. 8
Sector 1, 011141, Bucureşti, România
T + 4 021 204 88 90
F + 4 021 204 88 99
E office@tuca.ro
www.tuca.ro