Luther.

IP/IT

(Intellectual Property/Information Technology)

European Court of Justice declares US Safe Harbor invalid

Special Newsletter II

European Court of Justice declares US Safe Harbor invalid

On 6 October 2015 the European Court of Justice (ECJ) held that the Commission Decision 2000/520/EC of 26 July 2000 is invalid. This means that there is no longer any legal basis for the transfer of personal data to the U.S. in many cases. The U.S. lose their status as a country that disposes of an adequate level of data protection that is essentially equivalent to that guaranteed by the Data Protection Directive 95/46/EC within the scope of application of the U.S.-EU Safe Harbor certification. At the same time the ECJ strengthens the control rights of the national data protection authorities with this judgment.

1. Case history

The judgment of the ECJ is based on a request for a preliminary ruling under Article 267 of the Treaty on the Functioning of the European Union (TFEU) from the High Court of Ireland, made by decision of 17 July 2014. An Austrian citizen filed the action. He lodged a complaint with the Irish Data Protection Commissioner because of the transfer of his personal data by the European Facebook headquarters, Facebook Ireland Ltd., to the U.S. and insufficient protection of his data in the U.S. without success. The Data Protection Commissioner rejected the complaint on the ground that he would be tied to the considerations of the EU Commission in its Safe Harbor Decision in the year 2000 on the adequacy of the level of data protection in the U.S. In the view of the Data Protection Commissioner the revelations related to NSA surveillance did not affect the validity of this Decision. The Austrian then brought this case before the High Court of Ireland, which in turn submitted the question to the ECJ whether an independent data protection supervisory authority could be tied to the Safe Harbor Decision of the EU Commission insofar as it no longer may perform an own assessment and may not consider more recent developments.

In the Advocate General's opinion he announced at the end of September 2015 that in his view it would not be possible for the EU Commission to restrict the control rights of the national data protection authorities by a decision such as the Safe Harbor scheme. This would call their independence – which is expressly intended under European law - into question. According to the Advocate General it is the task of the Member States to ensure that the national data protection authorities are able to protect the fundamental rights of their citizens. In his view, U.S. legislation allows to store personal data of EU citizens without those citizens benefiting from effective judicial protection. After the new findings concerning the NSA the EU Commission ought to have suspended the application of the Safe Harbor scheme. According to the Advocate General it is not sufficient that the EU Commission is currently conducting new negotiations with the U.S. in order to put an end to potential infringements of data protection law.

2. Matter of the judgment

The ECJ followed the view of the Advocate General.

In the light of Articles 7, 8 and 47 of the EU Charter of Fundamental Rights, Directive 95/46/EC 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 has to be interpreted in such a way that a decision such as the Safe Harbor Decision does not prevent a national data protection supervisory authority from investigating complaints of persons affected, if these persons claim that the law and practice of the country into which personal data is transferred from the EU, do not ensure an adequate level of protection. EU Member States and their responsible supervisory authorities are not entitled to adopt measures contrary to the EU Commission Decision, such as legal acts intended to determine with binding effect that the third country covered by it does not ensure an adequate level of protection. Legal acts of EU institutions are in principle presumed to be lawful and accordingly produce legal effects until such time as they are withdrawn, annulled in an action for annulment or declared invalid following a reference for a preliminary ruling or a plea of illegality. Nevertheless a Commission Decision could not prevent a review by the data protection supervisory authorities.

The ECJ states that the Safe Harbor Decision does not contain sufficient guarantees within the meaning of the EU Data Protection Directive. It allows U.S. intelligence services to have access to personal data based on requirements of national security, public interest or other legal regulations in the US without any differentiation regarding the use of such data. The Safe Harbor Decision, furthermore, does not contain any statements regarding EU citizens' efficient legal protection against interception and surveillance measures of the National Security Agency. In this context the Advocate General noted that all companies involved in the PRISM program of the NSA are certified under the Safe Harbor scheme which means that

the Safe Harbor scheme serves as a door opener for U.S. surveillance authorities to collect personal data originating in the EU.

3. Background

The Safe Harbor Decision of the EU Commission has already been criticized for a while.

The Data Protection Directive 95/46/EC requires that Member States only permit the transfer of personal data to third countries which ensure an adequate level of data protection. Based on Article 25 of the EU Data Protection Directive the EU Commission has determined for certain states with effect throughout the EU that an "adequate level of protection" exists in these states for the data transmitted into these countries. In its so-called Safe Harbor Decision 2000/520/EC dated 26 July 2000 the EU Commission found that the U.S. ensured such an adequate level of protection. U.S. enterprises for which the U.S. Department of Commerce is responsible may join the *Safe Harbor* and have themselves entered in the corresponding list of the US Department of Commerce, if they undertake to adhere to the *Safe Harbor Privacy Principles* and the associated - binding - FAQ. Transfers of personal data from an EU Member State to an enterprise certified under the Safe Harbor scheme therefore no longer required any additional arrangements with regard to the EU requirements for transfers to third countries. Several thousands of U.S. enterprises, such as Microsoft, IBM, Google and Facebook, are U.S.-European Union Safe Harbor-certified.

The Safe Harbor Decision has been criticized not only since the scope of surveillance rights of the U.S. intelligence service NSA was revealed. As early as 28/29 April 2010 the so-called Düsseldorfer Kreis, as an umbrella organization of the German data protection supervisory authorities, determined that German enterprises exporting data have to verify the self-certification of the U.S. importing company in accordance with the Safe Harbor requirements due to problems with the implementation of and adherence to the Safe Harbor standard. Against the backdrop of massive surveillance activities of foreign intelligence services the Conference of data protection officers at national and regional level in a press release dated 24 July 2013 requested the EU Commission to suspend its Decisions on Safe Harbor and the standard contractual clauses until further notice. In this context, the German data protection supervisory authorities announced, not to grant any new permits for data transfers to third parties and to examine the option to suspend corresponding data transfers. It remained unclear, however, how they wanted to put this demand into practice, insofar as data transfers to countries with an adequate level of protection do not require any permit from any supervisory authority. Regardless of this demand and its possibility of implementation in practice as well as the resulting announcement of the EU Commission to review the Safe Harbor Decision, the Decision was still in full force and effect until the current judgment of the ECJ.

4. Consequences of the ECJ judgment

As a consequence of the ECJ judgment the national data protection authorities are required to take current trends into account in their review on a case-by-case basis in future.

The invalidity of the Safe Harbor Decision has substantial consequences for European enterprises that transfer personal data to the U.S. and have ensured the adequacy of the level of data protection in the U.S. via the U.S.-EU Safe Harbor certification of the enterprise based in the U.S. receiving the data so far. This applies to the transfer of personnel and customer data inside a group – for instance, if a European subsidiary exchanges data with its U.S. headquarters – as well as to the transfer of data to U.S. IT service providers and social media platforms. In particular for cloud-based services the exchange of data on a global scale is part of their business model which is why they are particularly affected by the ECJ judgment.

5. Immediate need for action for enterprises

Since the U.S.-EU Safe Harbor certification no longer applies other tools are required for a legal transfer of data. An alternative could be to use the standard contractual clauses of the EU. The European Commission adopted standard contractual clauses for transfers to so-called commissioned data processors (Commission Decision of 5 February 2010 (2010/87/EU)) and standard contractual clauses for controller to controller transfers (Commission Decision of 15 June 2001 (2001/497/EC) and Commission Decision of 27 December 2004 (2004/915/EC) amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries), that ensure adequate guarantees for the transfer of personal data from the EU to third countries that have to be recognized by the national data protection authorities. Enterprises should verify what standard contractual clauses suit their needs and how any existing contractual arrangements with clients and service providers may be embedded. In this context the different

legal requirements, such as the statutory requirement of the written form under Section 11 of the Federal Data Protection Act (*Bundesdatenschutzgesetz* – BDSG), and sub-contracting relationships that may be very complex in individual cases – in particular with regard to the distribution of tasks and the data exchange and contractual relationships affected – have to be taken account of.

For group-internal data transfers in large enterprises or global players so-called 'binding corporate rules' are another option. The European-wide reconciliation procedure between the data protection authorities of the EU and EEA Member States facilitates the process significantly. It is planned to simplify the procedure even further in the future in the draft of the EU General Data Protection Regulation. Depending on the business model affected, it would also generally be a conceivable option to obtain an approval for data transfer from the persons affected. However, such an approval would expressly need to relate to the transfer of data to a third country with inadequate level of protection. Furthermore there are frequent doubts concerning the necessary voluntary nature of such consents. In addition the fact that such consent may be revoked at any time leads to difficulties in the practical implementation. The judgment of the ECJ is immediately valid. The Court did not provide for any transitional period during which data could still be transferred as before. In the coming days the EU Commission wants to prepare requirements in cooperation with the national data protection authorities in order to eliminate the current legal uncertainty that resulted from the judgment. It remains to be seen, whether the data protection authorities will refrain from imposing sanctions for illegal data transfers for a certain period of time, thus in fact creating a transitional period. Enterprises based in the EU are immediately responsible for the admissibility of data transfers to U.S. enterprises. This is particularly the case if the (U.S.) service providers are commissioned data processors that only process the data on behalf of and upon instructions of the controller. The risk of supervisory sanctions and enforcement of claims of persons affected will be borne by the enterprise based in the EU and transferring the data as the controller.

Insofar as IT service providers have not already initiated or announced mitigating measures on their own initiative, it is advisable for the enterprises affected to expressly request such measures and to adjust the contractual arrangements accordingly.

Imprint

Luther Rechtsanwaltsgesellschaft mbH, Anna-Schneider-Steig 22,
50678 Cologne, Phone +49 221 9937 0, Fax +49 221 9937 110,
contact@luther-lawfirm.com
Editor: Dr Stefanie Hellmich, LL.M.
Luther Rechtsanwaltsgesellschaft mbH, An der Welle 10,
60322 Frankfurt a.M., Phone +49 69 27229 24118
stefanie.hellmich@luther-lawfirm.com

Luther Rechtsanwaltsgesellschaft mbH advises in all areas of business law. Our clients include medium-sized companies and large corporations, as well as the public sector. Luther is the German member of Taxand, a worldwide organisation of independent tax advisory firms.

Berlin, Brussels, Cologne, Dusseldorf, Essen, Frankfurt a. M., Hamburg, Hanover, Leipzig,
London, Luxembourg, Munich, Shanghai, Singapore, Stuttgart, Yangon

Luther Corporate Services: Delhi-Gurgaon, Kuala Lumpur, Shanghai, Singapore, Yangon

Your local contacts can be found on our website www.luther-lawfirm.com.

Hits the mark. Luther.

JUVE 2014 AWARDS
Kanzlei des Jahres
für Regulierte Industrien

JUVE 2014 AWARDS
Kanzlei des Jahres
für Energiewirtschaftsrecht

JUVE 2014 AWARDS
Kanzlei des Jahres
für Privates Baurecht

www.luther-lawfirm.com

Taxand