The merely supposedly safe harbor – employment law consequences of the latest ECJ ruling on "Safe Harbor"

INTRODUCTION

In a major and far-reaching ruling yesterday, October 6, 2015, the European Court of Justice (ECJ) declared the existing arrangement on the exchange of personal data between the EU and the United States to be void. Aside from the expected impact on the current talks between the EU and the United States on a new transatlantic data protection treaty and the pending negotiations on the free trade treaty TTIP, this judgment also has broad legal consequences for the transfer of personal data into the United States. These consequences also affect labor and employment law and how companies handle the personal data of their employees.

ECJ JUDGMENT OF OCTOBER 6, 2015, CASE NUMBER C-362/14

The judgment was handed down in the matter C-362/14 in which the Austrian jurist Maximilian Schrems, as a Facebook user, challenged the treatment of his data by that company. Generally speaking, the data of Facebook users are at least also partially stored by the Irish Facebook subsidiary, which is responsible for Europe, on servers in the United States. The plaintiff initially lodged a complaint with the Irish data protection authorities against exactly this situation and put forward the view that the law and its practical application in the United States did not warrant sufficient protection for his data which had been transferred to the United States - particularly in light of the activities of the U.S. intelligence services revealed by Edward Snowden - and that his personal data was not sufficiently protected there from government access.

The Irish data protection authority had first dismissed the complaint and noted that, in its so-called Safe Harbor ruling on July 26, 2000, the European Commission had classified the level of data protection in the United States as being reasonable and that the transfer of data to the United States was unobjectionable. Mr. Schrems filed a suit against this decision of the authorities before an Irish court, which presented the matter to the European Court of Justice for its decision.

OPINIONS OF THE ADVOCATE GENERAL

The Advocate General at the ECJ, Yves Bot, had already noted and emphasized in his opinions concerning the European Data Protection Directive (Directive 95/46/EC of the European Parliament and of the Council of October 24, 1995) that this directive only allowed the transfer of the personal data of EU citizens to a third country under the condition that the third country offers a reasonable level of data protection. He also noted that the European Commission was allowed to determine in general whether a particular third country offered a reasonable level of protection (cf. Art. 25 (6) of the Directive).

However, contrary to the estimation of the Commission in 2000, he was assuming that the laws and legal practice in the United States did not, indeed, offer a level of protection that satisfied European standards. In particular, the access of American intelligence services to the transmitted data constituted an illegal encroachment into the rights of European citizens. The laws and legal practice in the United States of America particularly allowed that the personal data of citizens of the European Union was collected on a broad scale without the warranty of effective judicial protection. From this he furthermore concluded that the "Safe Harbor" decision of the Commission from 2000 was invalid and that the existence of such a decision by the Commission did not otherwise remove or limit the control authority of the national data protection authorities.

As is perfectly normal in practice, the European Court of Justice has now concurred with the view of the Advocate General by also deeming U.S. practice to be a violation of European constitutional rights and ultimately deeming the Safe Harbor decision of the Commission to be void.

CONSEQUENCE OF THE RULING

The judgment of the ECJ addresses the American practice of handling the data of EU citizens and is leveled against the Safe Harbor decision of the Commission and the conduct of the Irish data protection office which, in the view of the ECJ, removed itself from its responsibility through a mere reference to the Safe Harbor principles.

The ruling is of major importance: It is important, first of all, that it by no means affects only Facebook and the relations of that company to the Irish data protection office. Rather, the principles put forward in the ruling are relevant to all national data protection authorities in the EU, as well as for all companies which have transmitted the data of European citizens, be this as customers, users or as employees, into the United States. Companies with an international presence which have previously transmitted data in this manner to the United States will be presented with the challenge of finding new ways to effect a transatlantic transfer of data that conforms with the law.

LABOR AND EMPLOYMENT LAW CONSEQUENCES

The ruling must occasion a critical review of how data is handled in a company, particularly with regard to employees. A transfer of the personal data of employees of American corporations with an international presence to the parent companies in the territory of the United States of Ameri-

ca takes place often and in a variety of contexts (e.g. for the purpose of uniform corporate personnel data management). In addition, not only international, but also national businesses regularly work together with external providers that store the employee-related data of their clients on services located in foreign countries, including servers in the United States, such as if IT systems are operated by external providers, including the use of globally uniform technology support in the United States or in data storage by another provider in a cloud on servers located in the United States.

From an employment law standpoint, the task will now be to review for compliance with the change in the framework conditions and find alternative solutions, where necessary, for shop agreements on data processing, the agreements executed with affiliated companies or with external providers (e.g. for contract on commissioned data processing or service level agreements) and, where appropriate, for the individually executed permissions for the transfer of data to the United States.

One must bear in mind that the lawfulness of the transmission of data into so-called third countries outside of the EU is generally governed by a dual level procedure: In addition to compliance with the national data protection regulations (Sections 4, 28, 32 Federal Data Protection act as the first level), the special requirements regarding the transfer of data to third countries must also be met (Sections 4b, 4c Federal Data Protection Act as the second level). While the first level has not been directly affected by the decision of the ECJ, a mere reference to "Safe Harbor Certification" will no longer suffice to comply with the special requirements placed on data transfer to third countries on the second level. Alternative legal grounds for a data transfer in these cases could be Binding Corporate Rules or the use of the EU model clauses, which have already been applied in the past when data was transferred to third countries outside of the EU.

Depending on the specific individual case, it may be also necessary to include the federal data protection official at the supervisory authority in the relevant German state within an approval procedure. Following the most recent ruling of the ECJ and the legal uncertainty this has created, it will be particularly interesting to see what position the German authorities will take in the near future on this subject.

CONTACTS

Dr. Henning Reitz
h.reitz@justem.de

Dr. Daniel Klösel
d.kloesel@justem.de

www.justem.de