ULD Position Paper on the Judgment of the Court of Justice of the European Union of 6 October 2015, C-362/14

This Position Paper addresses public and private bodies in Schleswig-Holstein in their function as controllers responsible for the collection, processing or use of personal data [in the context of section 3, para. 7 BDSG (German Federal Data Protection Act) and section 2, para. 3 LDSG (State Data Protection Act of Schleswig-Holstein)]. The Unabhängiges Landeszentrum für Datenschutz (ULD) of Schleswig-Holstein aims to explain the appropriate consequences following the "Schrems"/Safe Harbor Judgment of the Court of Justice of the European Union (CJEU) in case C-362/14.

First, this paper clarifies which statements the CJEU has or has not taken in its judgment. Second, the position paper takes a stand on the question of what options for action are available to the European Commission in line with the judgment. Third, it considers on which legal basis a transfer of personal data to the United States can or cannot be taken into consideration, and, fourth, how to deal with Standard Contractual Clauses for transfers to the United States. Fifth, and finally, it discusses the impact of the court decision – as far as is currently conceivable – on ULD's enforcement action.

1. Contents of the Judgment

The CJEU declared that the Commission's US Safe Harbor Decision is invalid. Until now, the system of self-certification served as a basis for data transfers to the US. However, this is no longer admissible after the delivery of the judgment.

The CJEU refers to a Communication from the Commission to the European Parliament and the Council of November 2013, where the Commission outlines various protection gaps in its Safe Harbor Decision. With reference to the Commission's own findings, the Court argues that the Safe Harbor decision is invalid because it does not limit access or create any sufficient binding measures for public authorities. Likewise, the Safe Harbor Decision lacks the means by which EU citizens can pursue adequate legal protection. Without evaluating the legal system of the United States specifically, the CJEU found that national regulations that make possible indiscriminate access to the content of electronic communications must be regarded as compromising the very essence of the fundamental right to respect for private life.

In addition, the CJEU found that the Safe Harbor Decision overly restricts the supervisory powers of the European data protection supervisory authorities and does not follow the requirements of the provisions that empower the Commission to decide on the level of protection of a third country. Falling short of the obligation pursuant to Art. 25 para. 6 of Directive 95/46/EC, the CJEU argued that the Commission did not make any statement about the level of data protection in the US, but instead chose with the Safe Harbor principles, an inapt construction as compensation for an inadequate level of protection.

Yet, the CJEU has not made a final decision on the current level of protection in the US, but referred the process to clarify these specific questions back to the Irish High Court.

2. The European Commission's options

a) On the basis of Art. 25 para. 6 of Directive 95/46/ EC, the Commission could adopt a new decision in which it finds that the US provides an adequate level of protection. This would need, inter alia, to note the following:

   To ensure the freedoms and fundamental rights of individuals, the level of protection in data protection in the US must, as specified by the CJEU, be essentially equivalent to that guaranteed within the European Union read in the light of the Charter of Fundamental Rights. According to the Conference of Data Protection Commissioners of the Federation and the States, Edward Snowden has revealed that US security authorities systematically and massively access personal data transferred to the United States and thus are likely to seriously violate the Safe Harbor Principles. Therefore, the US can currently show no effective means to ensure protection essentially equivalent to the level of protection guaranteed within the European Union.

   As required by the CJEU, the assumption of an adequate level of protection requires effective legal protection for citizens of the European Union against interference with their fundamental right to privacy. A general access by US authorities carried out on electronic communications violates the essence of the fundamental rights enshrined in Art. 7 of the Charter. If citizens of the European Union have no effective right to access their personal data or to be heard on the question of surveillance and interception and to enjoy legal protection, Art 47 of the Charter of Fundamental Rights is infringed.

   Examining the appropriate level of data protection, the Commission must consider the existing law and means of protection in the United States and subject them to an adequacy check. A regulatory instrument developed by the Commission such as the Safe Harbor Principles are not viable in this context and would not meet these requirements from the outset.

b) The Commission could push for an international treaty such as a data protection agreement with the US. This international treaty would have to meet in particular the requirements of Art. 7, Art. 8, para. 1 and Art. 47 para. 1 of the Charter. To meet this level of protection, the United States would firstly have to regulate by law the domestic data processing, adjust mainly the general and purposeless access to the content of electronic communications, and provide effective judicial protection for EU citizens. According to the requirements of the CJEU, adequate safeguards to protect the fundamental freedoms and rights of EU citizens must be provided especially with regard to automated data processing.

Conclusion: A decision of the Commission on the adequacy of the level of data protection in the US as well as an international treaty on data protection requires a comprehensive change in US law. As appropriate amendments are currently not expected to come into force soon, both courses of action seem to be unfeasible in the short and medium term.

3. Legal basis for the transfer of personal data

The transfer of personal data to countries where no adequate level of protection exists must be assessed for private bodies pursuant to section 4c para. 1 BDSG and for public authorities in Schleswig-Holstein pursuant to section 16 para. 2 LDSG. Based on these regulations, the following guidelines are applicable to data transfers to the US:

a) Section 4c para. 1 no. 1 BDSG and section 16 para. 2, sentence 2, no. 1 LDSG legitimize a data transfer to a third country without an adequate level of data protection on the basis of consent of the person concerned. However, consent must be given "without a doubt", according to Art. 26 para. 1 point a of Directive 95/46/EC and to the Art. 29 Data Protection Working Party, WP 187, p. 32. An effective informed consent requires not only information about the purposes, but also about the risks of data processing and the associated absence of an equivalent or adequate level of protection. The individual concerned (the “data subject”) would therefore have to be informed comprehensively about the missing level of protection, especially on US government access powers, lack of legal protection of data subjects' rights, further processing of the data without purpose limitation, the non-application of the necessity principle, as well as lack of government control in the United States.

   To be effective, consent always requires in particular an explanation of the specific purposes of the processing, in line with section 4a para. 1 sentence 2 BDSG. Furthermore, consent necessarily requires a statement to be in place "for each specific case" for a specific data processing, according to the Art. 29 Data Protection Working Party, WP 187, p. 20 ff. A general statement of consent for a variety of inestimable data processing operations will regularly be invalid. Especially in the context of employment, the employees would remain without choice with respect to their statement in so far as the employer requires consent for the transmission of their personal data into the United States. Consequently, this would not constitute a freedom of choice statement within the meaning of section 4a para. 1 BDSG and section 12 para. 2 LDSG and thus no effective declaration of consent. If US regulations provide for an unrestricted data processing by public authorities, this would already fail the requirements of effective consent.

   Even with adequate information about the risks and in cases in which one could expect a voluntary nature, consent would meet fundamental concerns. The indiscriminate mass surveillance by intelligence services infringes, in the CJEU's view, the very essence of the fundamental right to respect for private life. According to the judgments of the German Federal Constitutional Court, such infringements are exempted from the disposition of the individual, including by means of consent. This can also extend to the disclosure of information in a country in which the essence of the EU's fundamental rights will not be respected. Including consent under such circumstances in the Terms of Service would almost always constitute an offence against good morals in the sense of section 138 BGB (German Civil Code) and would most likely invalidate such clauses.

   Conclusion: Consent for a personal data transfer according to section 4a BDSG and section 12 LDSG regularly provides no option to serve as a legal basis for the admissibility of a transfer of personal data in the absence of an adequate level of data protection in a third country when, as discussed above, the very essence of the fundamental right is affected.

b) In the private sector essentially only section 4c para. 1 no. 2 and 3 BDSG come into consideration as legal bases. Accordingly, personal data transfers are allowed in the context of the performance of a contract between the data subject and the data controller or the implementation of pre-contractual measures that have been taken at the instigation of the data subject, insofar as is necessary, in accordance with section 4c para. 1 No. 2 BDSG. This captures, e.g., travel and flight bookings. Further, personal data transfer would be permissible if it is necessary for the conclusion or performance of a contract which is in the interests of the data subject entered into by the responsible body with a third party (section 4c para. 1 No. 3 BDSG refers). However, both facts do not form a legal basis for transfer of employment data to the US.

4. Use of Standard Contractual Clauses by private bodies

We reference clause 5 letter b of the Commission Decision on Standard Contractual Clauses for the transfer of personal data to processors established in third countries of 5 February 2010 (2010/87/EU). Accordingly, the data importer guarantees to the European data exporter, among other things, that to his knowledge he is not subject to laws that make it impossible to follow the instructions of the data exporter and to comply with the contractual obligations. However, American contractors cannot comply with exactly this contractual obligation with respect to the law in force in the United States. In such cases, the data exporter is entitled to suspend the transmission of data, or to terminate the Standard Contract. The same applies, for example, according to clause 5 letter b of the Commission Decision on Standard Contractual Clauses for the transfer of personal data to processors established in third countries of 27 December 2001 (2002/16/EC) and according to clause 5 letter a of the Commission Decision on Standard Contractual Clauses for the transfer of personal data in third countries of 15 June 2001 (2001/497/EC).

Conclusion: Private bodies, which use Standard Contractual Clauses to transfer personal data to the US, now need to consider terminating the underlying standard contract with the data importer in the United States or suspending data transfers. In consistent application of the requirements explicated by the CJEU in its judgment, a data transfer on the basis of Standard Contractual Clauses to the US is no longer permitted.

5. ULD's enforcement concerning private bodies

a) Concerning Standard Contractual Clauses – e.g. Article 4 letter a of the Commission Decision of 5 February 2010 (2010/87/EU) – supervisory authorities may prohibit or suspend data transfers to the US by an administrative order. The order is suitable if the data importer or sub-processor cannot in accordance with applicable US regulations adhere to European data protection law regarding the requirements of the Standard Contractual Clauses and the requirements pursuant to Art. 13 of Directive 95/46/EC. Data exporters from Europe can avert this only by making use of their contractually existing right to terminate the Standard Contract with the US data importer (clause 5 b of Commission Decision of 5 February 2010 – 2010/87/EU).

b) The transfer of personal data to the United States without a legal basis constitutes an administrative offence in accordance with section 43 para. 2 no. 1 BDSG and can be punished with a fine of up to € 300,000.

Conclusion: The ULD will examine whether orders against private bodies must be issued and on which basis data transfers to the United States must be suspended or banned. Furthermore, we must examine whether private bodies have committed an offence due to the transmission of data to a third country without an adequate level of data protection.

Contact:

Unabhaengiges Landeszentrum fuer Datenschutz Schleswig-Holstein
Holstenstr. 98, 24103 Kiel, Germany
Fon: +49 (0)431 988-1200, Fax: -1223
E-Mail: mail@datenschutzzentrum.de