Clash of the Titans: Safe Harbour deemed invalid

Rehana Harasgama, M.A. HSG, PhD Candidate, Legal Services, rehana.harasgama@ch.ey.com

1. Background

Both the EU and Switzerland allow the transfer of personal data abroad only if the recipient third country offers an adequate level of data protection according to the EU or Switzerland (Art. 25(1) of Directive 95/46/EC and Art. 6 of the Swiss Data Protection Act, DSG). If the law of the country concerned does not provide adequate data protection then businesses have to ensure the appropriate standards by implementing other safeguards (Art. 26(2) of Directive 95/46/EC and Art. 6(2) DSG). On that basis, the US entered into the so-called “Safe Harbour Agreements”, first with the EU (EU Commission Decision 2000/520) at the turn of the century, and subsequently with Switzerland, in 2008. These agreements were intended to ensure that US-based companies that are Safe Harbour certified (“self-certification”) comply with the relevant data protection principles when processing personal data. According to doctrine, whether or not US companies actually comply to the principles is questionable, and in 2013 the European Commission declared that the protection provided under the agreement is inadequate. However, the Commission did not revoke the agreement itself.

In Case C-362/14 Maximillian Schrems v Data Protection Commissioner, the Court of Justice of the European Union (CJEU) held that the Safe Harbour Agreement between the EU and the US is invalid, with far-reaching consequences for data transfers to the US. This judgment was followed by the Swiss Federal Data Protection and Information Commissioner (FDPIC) in an opinion of 22 October 2015. Data transfers to the US - including access to data in the EU/Switzerland by US-based firms - can therefore no longer be based on the Safe Harbour certification of the US firms concerned. The Court of Justice also had to decide whether a decision of the EU Commission (Art. 25(6) in conjunction with Art. 31(2) of Directive 95/46/EG) - such as the mentioned Decision 2000/520 on the Safe Harbour Agreement - restricts national authorities from deciding whether data transfers to a third country are based on the appropriate level of data protection.

2. Grounds

2.1 Main argument of Schrems

Schrems challenged the transfer of his data to the US by Facebook Ireland on the basis that the derogation clause in the Safe Harbour Agreement allows US authorities to access and retain data stored in the US - de facto without restrictions - where national security and other public interests or US domestic legislation require this (Commission Decision 2000/520, Annex IV). He argued that the practice of the US authorities constitutes a direct and unconditional breach of a human right recognised in the EU (Art. 7 and 8 of the EU Charter of Fundamental Rights; in Switzerland this corresponds to the fundamental right to data privacy enshrined in Art. 13(2) of the Federal Constitution, BV).

2.2 Grounds of the CJEU judgment

The CJEU based its judgment on the following arguments:

- National data protection authorities must be completely independent in the exercise of their functions. On this basis,
the CJEU found that the Safe Harbour Agreement adopted by the EU Commission does not restrict the discretion of those national authorities.

- Primarily, the CJEU found the Safe Harbour Agreement to be invalid because of Edward Snowden’s revelations which brought to light the mass surveillance measures employed by US intelligence services. These allow US authorities almost unrestricted access to personal data from the EU and Switzerland and are based on the derogation clause in the Safe Harbour Agreement. Furthermore, the Agreement does not provide any restrictions or justification requirements for this derogation nor does the Agreement offer any possibility for claims against such interferences with the protected rights.

3. Practical consequences for Switzerland

3.1 Data exchange within an organisation/group

The transfer of personal data between two member firms of the same organisation or group can also no longer be solely based on the Safe Harbour Agreement. Therefore, it is advisable to implement so-called internal Binding Corporate Rules (BCR) which require all member firms to adhere to the same data protection principles as the EU. Switzerland recognises the EU’s data protection standards as equivalent to its own. Therefore, there is no need for action with regard to data transfers from Switzerland to the US within an organisation/group as long as BCR have been implemented.

3.2 Data transfer outside of an organisation/group

If data is transferred to third parties outside an organisation/group then alternative data protection safeguards must be put in place (Art. 6(2) DSG). The FDPIC accordingly recommends to ensure the appropriate data protection level contractually via alternative safeguards, e.g. the EU’s standard contract clauses (model contracts), BCR or the like. Such safeguards oblige US data recipients to ensure compliance with EU/Swiss data protection principles. The FDPIC also states that the persons concerned by such data transfers must be informed of the fact that their data may be accessed by the authorities, so as to enable them to exercise their rights. Finally, it is also possible to obtain data subjects’ consent to the transfer of data.

According to the FDPIC’s recommendations new safeguards should be implemented and where necessary reported (Art. 6(3) DSG) by the end of January 2016, in order to comply with statements within the EU. However, it is highly unlikely to introduce BCR within this timeframe.

4. Conclusion

The striking down of the Safe Harbour Agreement poses major challenges for international firms involved in crossborder data transfers. Companies and individuals alike must look to new safeguards for the transfer of their data to the US. As of now, the introduction of EU standard contract clauses, BCR or other contractual arrangements are accepted as alternative safeguards, even if - strictly speaking - such measures also do not offer protection against access by US authorities. A company transferring personal data to the US without such safeguards in place will be in breach of data privacy law (Art. 13 DSG).

Under these circumstances we recommend to carry out an assessment of the current data transfer practices and their legal basis, to put in place suitable safeguards, and to modify contractual arrangements resp. insert new terms into existing contracts where this is necessary.

Contacts Legal
Basel: Jürg Strebel
juerg.strebel@ch.ey.com
Bern: Daniel Bachmann
daniel.bachmann@ch.ey.com
Gent: Aurélien Muller
aurelien.muller@ch.ey.com
Zürich: Jvo Grundler
jvo.grundler@ch.ey.com

Legal News: Publication in German, French and English
Registration/address changes
www.ey.com/ch/newsletter
www.ey.com/ch/legal

© 2015 Ernst & Young Ltd
All Rights reserved.

Disclaimer
This publication contains information in summary form and is therefore intended for general guidance only. Although prepared with utmost care this publication is not intended to be a substitute for detailed research or professional advice. Therefore, by reading this publication, you agree that no liability for correctness, completeness and/or currentness will be assumed. It is solely the responsibility of the readers to decide whether and in what form the information made available is relevant for their purposes. Neither Ernst & Young Ltd nor any other member of the global EY organization accepts any responsibility. On any specific matter, reference should be made to the appropriate advisor.