IBA/IFA 32nd
ANNUAL JOINT CONFERENCE

* * * * *

Challenges and Opportunities in International Franchising

* * * * *

THE "FACEBOOK DECISION" BY THE COURT OF JUSTICE OF THE EUROPEAN UNION AND ITS AFTERMATH IN INTERNATIONAL FRANCHISING

—

May 18, 2016

Washington, D.C. U.S.A

Andreas Mundanjohl
SGP Rechtsanwälte
Munich, Germany

Table of Contents

1. **The Judgement of the Court of Justice of the European Union (C-362/14)**
    - **1.1 Affirming the tight to data protection**
    - **1.2 EU law applicable to data transfers to third countries**
    - **1.3 Adequate level of data protection**
    - **1.4 No adequate level of data protection in the USA**
2. **Effect of the Judgement on other data transfer mechanisms**
    - **2.1 Standard Contractual Clauses**
    - **2.2 Corporate Binding Rules**
    - **2.3 Consent**
3. **Legal and financial risks arising from data-transfer to third countries**
    - **3.1 Risks for franchisees**
    - **3.2 Risks for franchisors**
4. **The future: Privacy Shield!?**
5. **Conclusion**
    - **5.1 Limitation of data to be transferred**
    - **5.2 Usage of servers within the European Union**
    - **5.3 Standard Contractual Clauses**

1. The Judgement of the Court of Justice of the European Union (C-362/14)

On 6th of October 2015, the Court of Justice of the European Union ("CJEU" or "Court") ruled on the matter *Maximilian Schrems vs. data protection Commissioner* ("Schrems Case"). Mr. Schrems, an Austrian citizen, uses Facebook since 2008 and filed a complaint at the Irish data protection agency, claiming that the transfer of his personal data onto servers in the USA violates his fundamental rights because of the activity of the National Security Agency ("NSA"). The Irish agency rejected this complaint, stating that the European Commission had ruled in its decision of 26th July 2000 that the USA grant an adequate data-protection-level based on the so-called "Safe-Harbour"rules.

Safe Harbour was a self-regulatory data protection mechanism which US based companies could commit to in order to provide protection for personal data transferred from the EU to the USA. It consisted of a number of principles based on EU data protection law with which Safe Harbour member companies had to commit to comply, and was overseen by the US Federal Trade Commission ("FTC"). In 2000 the Commission issued a formal decision under Article 2524 of the Directive 95/46/EC[1] findding that transfers provide adequate protection under EU data protection law, if the US based receiver of the data commits to comply with Safe Harbour.

In the Judgement of 6th of October 2015 rendered by the Court on the Schrems Case (case 362/14) ("Judgment"), the CJEU points out that the existence of Safe-Harbour does not limit the national data protection authorities in assessing wether or not an adequate data-protection-level is granted in countries like the USA. Furthermore the CJEU points out that Safe-Harbour is only binding for American companies which decide to voluntarily participate in Safe Harbour, but not for state or federal authorities in the USA. The demands of national security overrule Safe-Harbour-principles; therefore American companies are obliged to disregard those Safe-Harbour principles, if necessary in the light of national security. Because personal data transfered from the European Union to the USA, without any limitation or differenciation are beeing stored and used by US authorities, the fundamental right of privacy of European citizens is violated. Therefore, the CJEU rules that Decision 2000/520 of the European Commission (stating that the USA provides an adequate data protection level) is invalid, meaning the end of Safe Harbour and clearly stating that there is (from a EU perspective) no adequate data protection level provided in the USA.

The most important aspects of the Judgement are as follows:

1.1 Affirming the right to data protection

The Judgment repeatedly affirms data protection to be a fundamental right under EU law. In particular, the Court found that generalized access to data by public authorities is a violation of this fundamental right (because it compromises the right to private life under Article 7 of the EU Charter of Fundamental Rights ("Charter"). Main reason is the lack of any proportionality or balancing analysis involving other rights and freedoms under the Charter in those cases of generalized access to data.

[1] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000D0520&from=de

1.2 EU law applicable to data transfers to third countries

The Court pointed out in its Judgment that EU law is applicable to data transfers to third countries. Although the Court did not directly apply EU law to third countries, the effect is the same when the Court states that EU law applied to data transfers since "*the operation consisting in having personal data transferred from a Member State to a third country constitutes, in itself, processing of personal data within the meaning of Article 2(b) of Directive 95/46*" [2], which is subject to EU law.

This aspect of the Judgement is significant as it makes clear that such transfer of data from a Member State of the European Union requires "*essentially equivalent data protection*" in the third county the data is transfered to. In conclusion, the third country has to provide for the same level of data protection as defined by the Charter.

1.3 Adequate level of data protection

The Court defines the adequate level of protection for international data transfers as " essentially equivalent" but not necessarily " identical" to the level provided by EU law[3]. The Court gave a number of points of orientation to interpret the concept of essential equivalence, which set a high standard and which have been "summarized" by the Article 29 Working Party[4] in the form of a four-part test for detemining adequacy of data protection levels:

"A. processing should be based on clear, precise and accessible rules: this means that anyone who is reasonably informed should be able to foresee what might happen with her/his data where they are transferred;

B. necessity and proportionality with regard to the legitimate objectives pursued need to be demonstrated: a balance needs to be found between the objective for which the data are collected and accessed (generally national security) and the rights of the individual;

C. an independent oversight mechanism should exist, that is both effective and impartial: this can either be a judge or another independent body, as long as it has sufficient ability to carry out the necessary checks;

D. effective remedies need to be available to the individual: anyone should have the right to defend her/his rights before an independent body. " [5]

1.4 No adequate level of data protection in the USA

The Judgment on the Schrems case does at no point make any explicit statements concerning the adequacy of the US legal rules on data protection, the details and obvious flaws of Safe Harbour, or the intelligence surveillance in the USA. It does not at all judge the US Legal System. CJEU President Koen Lenaerts later stated. "*We are not judging the U.S. system here, we are judging the requirements of EU law in terms of the conditions to transfer data to third countries, whatever they be*"[6]. However, it remains clear that the judgmenet mainly focusses on a condemnation of US intelligence gathering practices and their effect on fundamental rights under EU data protection law; this is clear

[2] *Schrems v Data Protection Commissioner* [2014] IEHC 310; [2014] 2 ILRM 441, para. 45

[3] *Schrems v Data Protection Commissioner* [2014] IEHC 310; [2014] 2 ILRM 441, para. 73

[4] http://ec.europa.eu/justice/data-protection/article-29/index_de.htm

[5] Statement of the Article 29 Working Party on the Consequences of the Schrems Judgment", 3 February 2016, <http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2016/20160203_statement_consequences_schrems_judgement_en.pdf

[6] CJEU President Koen Lenaerts in „ECJ President on EU Integration, Public Opinion, Safe Harbor, Antitrust", The Wall Street Journal, 14 October 2015.

as Safe Harbour is a US specific mechanism as well as from certain statements in the Judgement regarding US authorities and their access to data in ways that do not meet EU legal standards in areas such as purpose limitation, necessity, and proportionality[7].

The Court defines the adequate level of protection for international data transfers as "essentially equivalent" but not necessarily"identical" to the level provided by the EU.

2. Effect of the Judgement on other data transfer mechanisms

The effect of the Schrems Case seems to be limited on data transfer to third countries based on Safe Harbour, but it is not. As pointed out, one main theme of the Schrems Case is the requirement of an adequate data protection level in any case of data transfer to a third country.

There are other mechanisms to transfer data to a third country, such as Corporate Binding Rules or EU Standard contractual clauses. Those mechanisms – as it might seem - are not directly affected by the Judgement, but given the abovementioned main themes of the Judgement there are obvious implications of the Judgement on those other mechansisms: The Judgement sets very strict criteria for data transfer to third countries, in particular the criteria of adequate level of protection. This criteria of adequacy must be applied to the other mechanisms as well, hence it seems unlikely that those mechanisms remain uneffected. In other words: if an adequate level of data protection cannot be assured, this lack of an adequate data protection level can not be healed by an agreement regarding the adequacy of the data protection level because the parties agree on something that they cannot provide, given the intelligence surveillance of US authorities.

For the remaining mechanisms this has the following effect:

2.1 Standard Contractual Clauses

In reference 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 5 February 2010 (2010/87/EU), standard contractual clauses are one very important mechanism for data transfer to third countries. When entering into such an agreement based on standard contractual clauses, the data protection level at the reveiving party of the agreement is considered adequate, because 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.

In the logic of the Schrems Case, some European countries, in particular the data protection authorities thereof, started to question the validity of standard contractual clauses. The reason lies within the abovementioned main theme of the Judgement: an adequate level of data protection has to *exist*, not just to be agreed upon. As the USA do not provide for such adequate level of data protection, any agreement (like standard contractual clauses) on such an adequate level of data protection level is rendered worthless. For example, one German data protection authority - the " Independent data protection agency of Schleswig-Holstein" ("ULD") (Schleswig-Holstein beeing the most northern German state) - has declared its interpretation of the Judgment as follows: "*However, American contractors cannot comply with exactly this contractual obligation with respect to the law in force in the United States."*[8]

7 Schrems v Data Protection Commissioner [2014] IEHC 310; [2014] 2 ILRM 441, para. 90
8 https://www.datenschutzzentrum.de/artikel/981-.html

The ULD considers Standard Contractual Clauses to be invalid, because within those clauses the data importer has to guarantee that " to his knowledge" he is not obliged by law to handle the personal data in any way that would be a violation of the request of the data exporter. This guarantee cannot be given in a valid way, knowing the activities of the NSA and other authorities.

As this is just one opinion by one state authority, similar tendencies can be witnessed throughout Europe. In the end it can be clearly stated: Standard contractual clauses have to be considered a legal risk, for authorities like the ULD potentially will find any data transfer based on standard contractual clauses not legitimate.

2.2 Binding Corporate Rules

Binding Corporate Rules ("BCR") are internal rules adopted by multinational group of companies which define its global policy with regard to the international transfers of personal data within the same corporate group to entities located in countries which do not provide an adequate level of protection[9].

BCR ensure that all data transfers made within a group benefit from an adequate level of protection. Once approved under the EU cooperation procedure, BCR provide a sufficient level of protection to companies to get authorisation of transfers by national data protection authorities.

As such, BCR used to be a reliable mechanism within multinational groups of companies to transfer data to third countries. But in the same logic as mentioned above for standard contractual clauses, BCR have to be considered a legal risk, since the parties agree on something that they cannot provide.

2.3 Consent

The most effective way to legitimate data transfer to the US used to be the consent of the data subject (for example the customer). But even this mechanism, which relies not on the agreement of two parties but on the free will of the data subject, is considered not sufficient by some data protection authorities. For example, the abovementioned ULD states that consent to transfer of personal data to the USA cannot be given in a valid way:

"Consent for a personal data transfer according to section 4a BDSG (German Data Protection Act) 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"[10].

3. Legal and financial risks arising from data-transfer to third countries

With all possible mechanisms for data transfer to third countries potentially useless (at least in the opinion of some authorities), any data transfer to such third country bears a legal and financial risk:

[9] http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/index_en.htm
[10] https://www.datenschutzzentrum.de/artikel/981-.html

3.1 Risks for franchisees

If a national data-protection authority finds data transfer of a European franchisee to an US based franchisor illegitimate, the financial risk varies in Germany from EUR 50.000,00 to EUR 300.000,00; the fines in other European countries are similar to this.

Apart from the financial risk, the damage of reputation in case of a illegitimate data transfer is very high, considering a high awareness for those issues in Europe not just since the Judgement.

3.2 Risks for franchisors

For franchisors, the financial risks are the same. In addition, franchisors have to be aware of the fact that franchisees might succesfully try to terminate the franchise-greements, claiming that the franchise-agreement states obligations (data transfer to franchisor in a third country) that are in violation of national and European legislation. First attempts in this direction coming from franchisees occur since beginning of 2016.

4. The future: Privacy shield!?

Since the Schrems Case was resolved by the Court, there have been negotiations between EU and US regarding a new agreement, the "*EU-US Privacy Shield*". The EU-US Privacy Shield imposes stronger obligations on US companies to protect Europeans' personal data. It claims to reflect the requirements of the CJEU, which ruled the previous Safe Harbour framework invalid. The Privacy Shield claims to require the U.S. to monitor and enforce more robustly, and cooperate more with European Data Protection Authorities. It includes, for the first time, written commitments and assurance regarding access to data by public authorities[11].

Most legal commentators declare that Privacy Shield will face the same fate as Safe Harbour, as in fact it does not adress all the requirements of the Judgement. For example, the CJEU in *Schrems* found that "*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, as guaranteed by Article 7 of the Charter*". The Privacy Shield presents a confusing picture with regard to its coverage of mass surveillance or the bulk collection of data by US intelligence or national security agencies. On the one hand, in the documentation the European Commission states that "*The US assures there is no indiscriminate or mass surveillance on the personal data transferred to the US under the new arrangement*", and the US notes that under US law, bulk collection of data or mass surveillance is "prohibited". On the other hand, the US also states in the documentation that "*signals intelligence collected in bulk can only be used for six specific purposes*", and that "*any bulk collection activities regarding Internet communications that the U.S. Intelligence Community performs through signals intelligence operate on a small proportion of the Internet*", suggesting that bulk collection does occur[12].

This is just one example of the many inconsistencies in the Privacy Shield-drafts in regards to the Judgement and its main holdings. It is widely expected that Privacy Shield, when in effect mid 2016 will be subject to complaints (Mr. Schrems already declared his intention to do so) and finally will be subject to a Judgement by the CJEU,

[11] European Commission, "Restoring trust in transatlantic data flows through strong safeguards: European Commission presents EU-U.S. Privacy Shield" (n 16).
[12] Kunder, Reality and Illusion in EU Data Transfer Regulation Post Schrems

were – at least in its actual draft – it will fail to convince the judges. Until then, there will be no legal certainty regarding data transfer to third countries.

5. Conclusion

Under the circumstances mentioned above, any transfer of personal data to the US has to be considered a risk for the company responsible for the personal data. This risk can be minimised by the measures described as follows:

5.1 Limitation of data to be transferred

The data protection legislation is relevant only to the transfer of personal data. Personal data is defined as "*any information relating to an identified or identifiable natural person ('data Subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity*".

Best practise would be to limit the data collected and transfered to such data that is not "personal data". For example, only the name of the company should be collected, not the name of the contact or any other employee ("natural person"). In that way, no personal data would be transfered to the US and the company responsible for data protection (franchisee) would bear almost no risk of incompliance with data protection regulations.

5.2 Usage of servers within the European Union

If data collected in Europe would be stored and used on servers within the European Union (or another country which is considered to provide an adequate data protection level), the Judgement would have no relevance for this data, as it only ruled against the data transfer to the US, not against the collecting of the data itself.

5.3 Standard contractual clauses

In combination with the limitation of the data transfered, every franchisee in Europe and the data importing US companies should agree on standard contractual clauses. As mentioned above, those standard contractual clauses are considered to be invalid by some authorities; but most legal experts consider them still a valid mechanism, because they are based on a decision of the European committee which cannot be overruled by national authorities but only by court. As long as there is no such court judgement, the standard contractual clauses are likely to legitimate the transfer of this personal data.

****

Biography of the author

Andreas Mundanjohl from the Munich office of SGP attorneys, is a specialist in the field of IT/IP, data protection and compliance. For years he has been assisting international companies, in particular franchise-systems, regarding data-protection, data-security and the current and upcoming developments in european data protection law