US Personal Data Transfers – still an issue

August 17, 2020

Due to the recent judgement of the European Court of Justice regarding the validity of the EU US Privacy Shield (Case C-311/18, "**Schrems II**"), European data controllers and processors find themselves in a world of legal uncertainty. Most of them have business partners or service providers located in the United States (the "**US**") and such business relations often require the exchange of personal data. Many of the US entities, in particular bigger service providers, which were operating under the EU US Privacy Shield ("**Privacy Shield**") certification, have promptly switched to Standard Contractual Clauses ("**SCC**"), informing their clients that this would be a reliable alternative to the Privacy Shield.

It is only understandable in this situation that the European controllers and processors are eager to believe this argument. The usual advice of the European data protection authorities ("**DPA**") to stop transfers of personal data to the US, is – let's face it – often commercially unfeasible, for example simply because there is no alternative EU-based service provider for some industries. In addition, as the ECJ did not declare the SCC invalid, one could indeed erroneously believe that one could simply switch the legal instrument.

This article will shortly explain, why it is not possible to rely on the SCC as we did before and what could be the options.

Schrems II – what was that about again?

To sum up, the ECJ declared one of the most important legal instruments for transfer of personal data to the US – the EU US Privacy Shield – invalid on July 16th. ECJ criticises the surveillance programs of the US intelligence authorities, which lack legal protection for EU data subjects and finds the mechanisms established by the Privacy Shield as insufficient. Therefore, according to the ECJ, there is no adequate level of data protection compared to the EU. Accordingly, from this day transfers of personal data to the US need to find another legal basis for international data transfers.

What are the options?

Another important legal instrument for international transfer of personal data from the EU to third countries (including the US) are the SCC. As a reminder – SCC are contracts defining the obligations of data exporters and data importers pre-drafted by the EU Commission. Depending on the structure of the processing, there are three versions of SCC, which could be used (two versions for transfers between data controllers, who equally determine the respective means and purposes of the processing and one version for the transfer from a data controller to a data processor, acting on behalf and upon instructions of such controller).

Further, the General Regulation on Data Protection (EU) 2016/679 ("**GDPR**") defines other legal instruments, which

can be implemented as the legal basis for international data transfers (e.g. so called binding corporate rules, which would require an authorization from the DPA) as well as some exemptions in extraordinary cases (e.g. consent, contract fulfilment etc.). Although many globally operating companies use BCR, it is obvious that this is not a legal instrument that can be implemented on a short-term basis. In addition, one can assume that it will be quite difficult to obtain an authorization of the DPA under the current circumstances. The exemptions, on the other hand, are clearly not suitable for data processing in the course of a daily business operation.

What is the problem with the SCC?

As the ECJ did not declare the SCC as invalid, one could assume that it is reasonable to make a fast switch to this well-established instrument.

However, the ECJ only dealt with the data protection level within the US. Basically, the SCC can be used for data transfers into any third country outside the EU, not only the US. While the Privacy Shield was an instrument applicable for the US transfers only, the validity of the SCC cannot be linked to one country's legal situation.

The ECJ nevertheless points out that

- "In so far as those standard data protection clauses cannot […] provide guarantees beyond a contractual obligation to ensure compliance with the level of protection required under EU law, they **may require** […] **the adoption of supplementary measures by the controller** in order to ensure compliance with that level of protection".

Further, it is up to the

- "controller or processor to verify, on a case-by-case basis and, where appropriate, in collaboration with the recipient of the data, whether the law of the third country of destination ensures adequate protection, under EU law, of personal data transferred pursuant to standard data protection clauses, by providing, where necessary, additional safeguards to those offered by [the SCC]."

The ECJ, therefore, makes the validity of the SCC depending on whether such SCC

- "incorporate effective mechanisms that make it possible, in practice, to ensure compliance with the level of protection required by EU law and that transfers of personal data pursuant to the [SCC] are suspended or prohibited in the event of the breach of such clauses or it being impossible to honour them."

Considering that the ECJ found that the US law does not ensure an adequate level of data protection and that the measures of the Privacy Shield were found as not sufficient to correct this, it is – euphemistically speaking – doubtful whether the SCC can ensure such adequate level in their original form. The German DPA clearly state that

- "after the ECJ judgment, SCC are in principal not sufficient for data transfers to the USA without additional measures".

However, it is not clear what kind of supplementary measures can be implemented, when it comes to protection from state authorities of the respective third countries. Even the European Data Protection Board ("**EDPB**") phrases laconically that they are "looking further into what these supplementary measures could consist of and will provide more guidance".

Summing up, if the transfer of personal data into the US is based on the SCC concluded without any further amending measures, risk assessments etc., it will most likely not be sufficient and the European data protection authorities will most likely suspend or prohibit such transfer, probably accompanied by issuing fines for the infringement of the

GDPR.

We don’t have transfers to the US - are we safe?

The same principles regarding an adequate standard of data protection, in particular with regard to the rights and possibilities of the respective countries authorities and the factual legal remedies apply to any other country. There are quite some third countries, where the European data controllers and processors should be aware of the possible risks that may be caused by the political and legal realities.

What now?

The usual answer from the data protection authorities and the most secure recommendation is to stop transfers of personal data to the US. Some controllers or processors could surely identify some transfers, that could be based on the exemptions pursuant to Art. 49 of the GDPR, while awaiting more clear guidance from the European DPA.

Further, the EU Commission and the U.S. Department of Commerce issued, on 10 August 2020, a joint statement announcing that they are evaluating the potential for an enhanced Privacy Shield framework to comply with the ECJ judgement.

If the suspension of transfers of personal data to the US (or similar third country) is not an option, there is – frankly speaking – not much one can do to fully avoid the risk of being fined for an ongoing GDPR infringement. However, data controllers and processors could try to mitigate the practical risk by showing awareness and setting up compliance processes and documentation, in order to at least minimize the data flows or identify additional measures themselves. Further, the US partners should be informed about the potential invalidity of the SCC in order to make them more receptive to implementation of additional measures (e.g. acceptance of pseudonymized data, implementing access restrictions, using EU-based servers or similar). Such measures will most likely not be sufficient given the extensive powers of the official authorities, which were the “offence mark” in the first place, but may be considered by the European DPA when exercising their discretion regarding the amount of the fine.

Your Key Contacts

Dr. Constantin Rehaag
Partner, Frankfurt
D +49 69 45 00 12 248
constantin.rehaag@dentons.com

Valeria Hoffmann
Counsel, Frankfurt
D +49 69 45 00 12 144
valeria.hoffmann@dentons.com