September 2020

Newsletter No.

145

According to the FDPIC, the Swiss-US Privacy Shield does not provide an adequate level of data protection:

The FDPIC thus follows – not surprisingly – the considerations of the European Court of Justice (ECJ) on the EU-US Privacy Shield in its judgement "Schrems II". Even standard contractual clauses are in many cases not a sufficient basis for data transfers to third countries. Swiss companies should therefore examine how they can transfer personal data to third countries lacking an adequate level of data protection in the future in a way that complies with data protection regulations.

walderwyss attorneys at law

By Jürg Schneider
Dr. iur., Attorney at Law
Partner
Direct phone: +41 58 658 55 71
juerg.schneider@walderwyss.com

and David Vasella
Dr. iur., Attorney at Law
Partner
Direct phone: +41 58 658 52 87
david.vasella@walderwyss.com

and Lena Götzinger
Attorney at Law (Bar Association Frankfurt am Main)
Associate
Direct phone: +41 58 658 56 63
lena.goetzinger@walderwyss.com

In a statement dated 8 September 2020, the FDPIC informed the public that he had removed the USA from the list of States he deems to offer an adequate level of data protection. Generally, data transfers from Switzerland to the USA solely based on the Privacy Shield should therefore no longer occur. Furthermore, Swiss companies cannot rely on standard contractual clauses without closer scrutiny. Companies in Switzerland thus need to take action.

The result was hardly surprising

The statement of the Swiss Federal Data Protection and Information Commissioner (FDPIC) that the Swiss-US Privacy Shield no longer ensures an adequate level of data protection for data transferred to the USA on its basis is not surprising after the Schrems II ruling of the European Court of Justice (ECJ). In its decision, the ECJ invalidated the EU-US Privacy Shield with immediate effect and imposed additional requirements on the use of standard contractual clauses for data transfers.

The FDPIC justified his assessment (following the ECJ) essentially by referring to the broad surveillance by US intelligence services of transferred data and the lack of sufficient legal remedies for data subjects. Accordingly, the FDPIC has removed the United States from the list of States that guarantee an adequate level of data protection. Notably, the Swiss-US Privacy Shield remains legally valid. The list of States simply establishes a rebuttable presumption as to whether (and, if so, under what conditions) an adequate level of data protection exists in the country of destination. In practice, however, a data transfer to the USA based on the Swiss-US Privacy Shield is no longer recommended.

Instead, data transfers to the USA should rely on other safeguards in the future. At least for large data sets and for regular data transfers, companies will focus on the safeguards mentioned in Article 6 para. 2 lit. a FADP, in particular the EU standard contractual clauses. According to the FDPIC, however, these standard contractual clauses fail "in many cases" to provide an adequate level of data protection because they are not capable of preventing access to personal data by foreign authorities. From this point of view, they no longer represent a real "standard"; rather, they should be supplemented on a case-by-case basis (although the FDPIC does not clarify how this should be done).

Need for action for Swiss companies

Standard contractual clauses – and, where appropriate, binding corporate rules (BCRs) – must therefore be examined on a case-by-case basis to verify whether they provide adequate protection for data transfers to the respective country of destination. This applies to standard contractual clauses already in place as well as to their future use. Importantly, this does not only apply for data transfers to the USA. Instead, the FDPIC's assessment with respect to contractual safeguards is relevant for all States listed as States without an adequate level of data protection.

If transfers are based on contractual safeguards, the data exporter must, according to the FDPIC's statement, examine on a case-by-case basis (by means of a risk analysis) whether additional measures are necessary to ensure an adequate protection of the exported personal data. According to the FDPIC, special consideration must be given to whether the data importer is subject to a legislation which allows foreign authorities to access the data transferred to the importer. This renders the applicability of

such legislation to the data importer the decisive factor. A more differentiated approach in this respect would have been preferable. The theoretical risk of data access by foreign authorities should not determine alone whether a data transfer complies with data protection regulations. In fact, depending on their business model, some providers will be more likely targeted than others by foreign authorities, although all these providers may be equally subject to the relevant legislation; data exporters can and should take this likelihood into account.

Where the risk analysis reveals that standard clauses are insufficient, they need to be supplemented by other clauses. However, the FDPIC remains silent on the concrete nature of such supplementary clauses. If supplementary contractual safeguards are not able to sufficiently mitigate the risk assessed by the exporter, the FDPIC recommends implementing technical measures to prevent or impede access by the authorities.

For this purpose, according to the FDPIC, it is conceivable to encrypt the data to be transferred – in line with the principles of BYOK (bring your own key) and BYOE (bring your own encryption) – if the data is only stored by the recipient. This means that no clear data is available in the country of destination. However, in the FDPIC's view, technical measures are "challenging" for services that go beyond mere data storage in the country of destination, which is certainly no understatement. If the access of foreign authorities cannot be prevented by technical measures, the FDPIC recommends that the transfer of personal data to the non-listed country should not take place based on contractual safeguards.

What to do

We recommend that Swiss companies first create a directory of all data transfers in their area of responsibility, if such a directory does not already exist (e.g. as part of a record of processing activities or as part of vendor or third-party management). Thereby it can be determined whether data is transferred to a company's own contracting party in third countries without an adequate level of protection or whether the data is forwarded to subcontractors of a company's own contracting party operating in such countries. If this is the case, Swiss companies should then consider contacting the relevant contracting parties abroad, inform them of the FDPIC's statement and the consequences resulting therefrom and – in the case of larger providers – enquire about remedial measures taken by the provider.

Based on the directory, a risk analysis can be carried out as a next step. The service provider or the contracting party will be able to provide support in this process if necessary - for example, in clarifying which administrative practices are pursued by authorities in the country of destination or which legal protections are available to data subjects. If data is transferred not only from Switzerland, but also from the European Economic Area to countries without an adequate level of data protection, it is advisable to examine at the same time whether the requirements of the ECJ and the competent data protection authorities call for amendments to be made to the existing transfer practice.

Further action depends on the risks. If an addition to the standard contractual clauses can sufficiently mitigate the risks, Swiss companies should agree with the data recipient on a modification of the provisions of the standard contractual clauses. The orientation guide (only in German) published by the State Commissioner for Data Protection and Freedom of Information of Baden-Württemberg can provide guidance in this regard.

If contractual amendments prove to be insufficient, technical measures may help to reduce the risk. However, for many services – especially SaaS and PaaS services – encryption is de facto hardly possible. Alternatives may be anonymisation or pseudonymisation of transferred data.

If neither contractual amendments nor technical measures can adequately counteract the risks, the only remaining question is whether a service provider in a country with an adequate level of data protection is a suitable option. Such countries will particularly be countries of the European Economic Area (in which case it must be examined whether and under what circumstances data access from another location is possible and what risks result from this possibility).

The ECJ and the authorities have passed the buck of a political problem to companies. However, this problem – which is based on a different understanding of data protection and its importance – cannot be solved by adapting business practice. Data protection authorities will therefore have to act in accordance with the principle of proportionality if corporate data protection is to remain credible. The EU is at least conducting talks with the USA. For the time being, it can therefore be hoped that a "Privacy Shield Plus" and the already announced standard contractual clauses adapted to Schrems II will bring solutions. In addition, the FDPIC has announced that he will provide further information in due course on the export of personal data to the USA and other non-listed third countries in a manner compatible with data protection. We hope that this information will soon be available and of relevance.