Briefing September 2020

Inadequacy of the Swiss-U.S. Privacy Shield - Filling the Gaps around the Federal Data Protection and Information Commissioner's Opinion on Cross-Border Data Transfers to Third Countries

The Federal Data Protection and Information Commissioner ("FDPIC") has now published its opinion stating that the Swiss-U.S. Privacy Shield does not provide adequate safeguards to transfer personal data to the US. At the same time, the FDPIC has also challenged the adequacy of the Standard Contractual Clauses ("SCC") and Binding Corporate Rules ("BCR") for cross-border data transfers to third countries. This presents Swiss companies conducting business at a multinational level with the question – how can we continue to transfer personal data abroad in a privacy-compliant way? This article focuses on the opinion of the FDPIC and also provides some initial steps Swiss companies should consider moving forward.

FDPIC Opinion

Swiss-U.S. Privacy Shield

Last week, the FDPIC issued its opinion on the validity of cross-border data transfers to the US, based on the Swiss-U.S. Privacy Shield Framework. It was to be expected that the FDPIC would update its list of countries that provide an adequate level of data protection in coordination with the European Union with regard to the US (following the Schrems II-Decision of the Court of Justice of the European Union ("CJEU") that invalidated the EU-U.S. Privacy Shield Framework in July 2020). The view of the FDPIC is that the Swiss-U.S. Privacy Shield Framework in its entirety does not provide an adequate level of data protection for cross-border data transfers to the US. Similar to the CJEU, the FDPIC bases its opinion among others on the fact that the Privacy Shield Framework does not provide individuals or companies with adequate legal remedies in case of US government access to their personal data based on US national surveillance laws (cf. BK Briefing on the Schrems II-Decision "The End of the Privacy Shield - Juggling the Requirements for Cross-Border Data Transfers to the US").

The FDPIC has highlighted this issue previously in its annual reviews of the Swiss-U.S. Privacy Shield Framework and so far, the Privacy Shield Framework has remained unchanged. Therefore, as a result of the FDPIC's opinion, – even though the Privacy Shield Framework remains in force until it is officially

invalidated – companies relying on the Swiss-U.S. Privacy Shield for the transfer of personal data to the US should base such cross-border data transfers on other safeguards provided by Swiss data protection law.

Standard Contractual Clauses and Binding Corporate Rules

Following the CJEU, the FDPIC also issued a caveat regarding the use of the SCCs frequently applied by Swiss companies to transfer personal data to third countries. The FDPIC states in its opinion, that neither the SCCs nor the BCRs *"prevent foreign authorities from accessing personal data if the public law of the importing country takes precedence and allows official access to the transferred personal data without sufficient transparency and legal protection of the persons concerned"*. This applies to the transfer of personal data to any third country – not just the US – that does not provide an adequate level of data protection. This statement has, in our view, consequences that go far beyond the FDPIC's declaration that the Privacy Shield Framework does not guarantee an adequate level of data protection, as it calls into question all transfers of personal data to third countries that are not listed on the FDPIC's list of countries.

Swiss companies are now compelled to review all transfers of personal data to third countries and to reassess the permissibility of such cross-border transfers under Swiss data protection law.

The effects of the FDPIC's opinion on the current legal landscape

The Swiss Federal Data Protection Act ("DPA") provides the legal framework for processing personal data under Swiss law.

Amongst others topics, the DPA regulates the transfer of personal data abroad to ensure that the importing company located outside of Switzerland cannot process such personal data in ways which undermine the general principles and rights provided under the DPA. Any violation thereof is subject to civil remedies and may result in reputational risks for the company exporting personal data to third countries.

Country list and Swiss-U.S. Privacy Shield

In general, Swiss data protection law allows cross-border data transfers if the country the data is transferred to ("receiving country"), provides an adequate level of data protection. Currently, this is determined by the FDPIC and reflected in the FDPIC's list of countries that provide such an adequate level of data protection. Companies can consult this list when deciding on cross-border data transfers. However, this list is non-binding and only provides an indication as to which countries provide an adequate level of data protection in the FDPIC's view.

In maintaining the list, the FDPIC considers the following:

– Legislation and its practical application by the third countries and how such legislation is assessed by established principles and jurisprudence;

– Conventions, publications, official statements and decisions by other institutions and authorities on the equivalence or adequacy of the level of data protection afforded by the receiving countries.

If the receiving country is deemed to provide an adequate level of data protection, the assumption is that a Swiss company can transfer personal data freely to a company in that receiving country.

The US reached a compromise with Switzerland over this matter: while the US as a whole does not provide adequate protection, it agreed to put in place a mechanism under which US companies can self-certify that they provide an adequate level of data protection. Until now, the US was listed as a country that provides an adequate level of data protection if personal data is transferred to a company which has been certified according to the Swiss-U.S. Privacy Shield Framework. Therefore, companies in Switzerland could freely transfer personal data to such companies. According to the FDPIC's opinion, this is no longer possible. Therefore, the FDPIC amended its assessment of the US in the list of countries as follows:

"Data processors who are on the list of the US Department of Commerce and sign up to the Privacy Shield regime between the US and Switzerland in relation to personal data obtained in Switzerland shall grant special protection rights to persons in Switzerland. However, these rights do not meet the requirements of adequate data protection as defined by the [DPA]."

Once the revised DPA enters into force, the Federal Council will have to decide on the adequacy of a country's data protection laws and their decision will be binding, providing more legal certainty to companies.

Standard Contractual Clauses and Binding Corporate Rules

In the absence of such an adequacy decision, personal data can, for example, be transferred abroad if the exporter and the importer sign SCCs approved by the FDPIC that aim to establish data protection rules between the parties that are equivalent to the protection of personal data under the DPA. Furthermore, companies that conduct business on a multinational level can implement binding corporate rules for intra-group data transfers to different countries around the globe.

As described above, the SCCs and BCRs as a mechanism to transfer personal data across borders were equally under review in the FDPIC's opinion. According to the FDPIC, these transfer mechanisms may also not provide an adequate level of data protection when transferring personal data to a third country that does not provide adequate legal remedies in cases of government access to the imported personal data. In effect, this means that it may no longer be sufficient to "just" sign SCCs (or agree on BCRs) with a foreign contractual partner, file the SCCs (or BCRs) and then forget about them. According to this assessment, Swiss companies need to make sure that the SCCs or BCRs provide the required level of data protection and should therefore, carry out a risk assessment. The company exporting personal data should check whether the SCCs or BCRs cover the data protection risks existing in the non-listed receiving country. This includes examining whether the transferred personal data may be subject to access by local government authorities and in that case, whether the receiving company can provide the necessary cooperation to ensure legal remedies for the affected individuals or legal entities. If necessary, the SCCs or BCRs should be amended. However, the FDPIC states that such amendments *"remain of limited effect if the public law of the given country takes precedence"*.

Other safeguards

Other measures for the legitimate transfer of personal data abroad include justifying the cross-border data transfer on the fulfilment or conclusion of a contract with the affected individual or legal entity, the necessity to transfer personal data abroad for the establishment, exercise or enforcement of legal claims before a court as well as obtaining the affected person's explicit consent. These safeguards remain unchanged.

Steps your business can take now

The FDPIC has indicated that it soon intends to provide further guidance on how Swiss companies can transfer personal data to third countries in a manner compliant with the DPA. Furthermore, the European Data Protection Board ("EDPB") issued a statement last week saying that it plans to publish additional recommendations to the FAQs issued in July 2020 to assist companies with their duty to identify and implement appropriate supplementary measures to ensure adequate protection when transferring personal data to third countries. Together with the EU Commission, the EDPB further expects to provide a final updated version of the SCCs by the end of the year, that companies will be able to rely on, on a case-by-case basis.

Based on the above, and as an update to our advice provided in our initial BK Briefing on the Schrems II-Decision "The End of the Privacy Shield - Juggling the Requirements for Cross-Border Data Transfers to the US", we advise companies to carry out a case-by-case analysis of their cross-border data transfers and take the following initial steps with regard to these transfers moving forward:

- First, you should evaluate whether you are transferring any data to the US or other third countries that do not provide adequate legal remedies or transparency with regard to government access and also assess what type of data you are transferring and for what purpose you need to transfer the data.

- As a next step, you should ask yourself under which mechanism you are transferring personal data abroad.

  - If the answer is the Swiss-U.S. Privacy Shield, you need to implement a different mechanism for your transfers as soon as possible.

  - If the answer is SCCs or BCRs, you must first analyse whether the receiving country provides appropriate legal remedies and transparency with regard to government access.

  - If this is not the case, you should review whether the measures under the SCCs or BCRs contain provisions that address the identified issues and whether the importing company can actually ensure compliance with these safeguards.

  - If this does not apply, you should contractually agree on potential additional measures that ensure the required level of data protection. Such measures are, for example, a code of conduct, additional protective duties (e.g., a duty of the importing company to inform you of any government access and who the affected individuals or legal entities are; if public laws allow, a duty of the importing company to assist the affected individuals or legal entities in defending their rights according to your instructions; a duty of the importing company not to provide government access voluntarily if no legal duty applies), the implementation of effective legal remedies or additional encryption measures (as suggested by the FDPIC, in particular, for the mere storage of personal data in a cloud). Furthermore, companies can contact the FDPIC or other supervisory authorities for further assistance or guidance.

  - However, if the importing company cannot assist you or the affected individuals or legal entities with legal remedies, then you should preferably base your cross-border transfers on other measures such as the consent of the individual or legal entity or the necessity of the transfer for the performance of a contract.

  - If you are relying on other mechanisms for cross-border data transfers to the US or other third countries such as explicit consent of the affected individuals, currently, no action is necessary.

Once the FDPIC and the EDPB have provided further guidance on cross-border data transfers to third countries, companies should carry out a second assessment based on these and adapt their cross-border data transfers accordingly.

Authors

Dr. Corrado Rampini
Partner

T: +41 58 261 52 83
corrado.rampini@baerkarrer.ch

Dr. Rehana Harasgama
Associate

T: +41 58 261 54 51
rehana.harasgama@baerkarrer.ch

Further contacts

Dr. Jan Kleiner
Partner

T: +41 58 261 53 84
jan.kleiner@baerkarrer.ch

Dr. Christian Kunz
Associate

T: +41 58 261 52 66
christian.kunz@baerkarrer.ch