BÄR & KARRER

Briefing July 2020

The End of the Privacy Shield - Juggling the Requirements for Cross-Border Data Transfers to the US

The Court of Justice of the European Union ("CJEU", the "Court") issued a ruling that invalidated the EU-U.S. Privacy Shield Framework for cross-border data transfers to the US. However, the Court also confirmed the validity of the EU Standard Contractual Clauses ("SCCs") as a mechanism for such transfers. At the same time, the CJEU stated that companies exporting personal data abroad have a responsibility to ensure an adequate level of data protection when using SCCs. In this Briefing, we will address what the ruling means, how it changes the existing legal landscape, and what the consequences might be for you and your business.

Facts leading up to the ruling

Maximilian Schrems, an Austrian privacy activist, filed a complaint with the Data Protection Commission of Ireland ("DPC") in 2015. He took issue with the fact that Facebook Ireland transferred his personal data to its parent company Facebook Inc. in the US, that his transferred data was then available to the US administration under the latter's far-reaching surveillance laws, and that he as a EU-citizen had no recourse against this intrusion into his privacy.

Schrems therefore asked the DPC to order Facebook Ireland to stop such transfers. The DPC concluded that such an order would not be possible without a judicial review of the legal framework under which the data transfer took place, referred the matter to the Irish High Court, which, in turn, escalated the issue to the CJEU for a preliminary ruling.

Last week, the CJEU issued its decision on the validity of cross-border data transfers to third countries, in particular the US, based on SCCs adopted by the EU Commission or the EU-U.S. Privacy Shield Framework. The Court found that while the SCCs provide a valid mechanism to transfer personal data legitimately outside of the EU in accordance with GDPR, it invalidated the EU-U.S. Privacy Shield Framework in its entirety. As a result, companies relying on the EU-U.S. Privacy Shield for the transfer of personal data abroad must implement other measures for such transfers as soon as possible.

Legal landscape before the ruling

The EU General Data Protection Regulation (GDPR) provides the legal framework for processing personal data under EU law.

Amongst others topics, the GDPR regulates the transfer of personal data abroad to ensure that the importing company located outside of the EU cannot process such personal data in ways which undermine the general principles and rights provided under the GDPR. Any violation thereof is subject to potentially serious fines, *i.e.* up to 20 Million Euros or 4% of global annual turnover, whichever is higher.

Adequacy decisions

In general, GDPR and Swiss data protection law allow cross-border data transfers if the country the data is transferred to ("receiving country"), provides an adequate level of data protection. This is determined by the EU Commission (or for Switzerland the Federal Data Protection and Information Commissioner, "FDPIC") that examines the laws of the receiving country (or of a sector thereof) to ensure that the level of data protection is equivalent to that granted under EU or Swiss data protection law. This includes the ability of individuals to enforce their data protection rights, such as their rights to access, information or deletion, in the receiving country as well as the granting of effective legal remedies to individuals if their privacy is infringed in the receiving country.

If such an adequacy decision has been rendered to a third country, personal data can flow freely from the EU to that country and the competent supervisory authorities, generally, cannot prohibit or suspend such transfers (it can however review the adequacy based on a complaint received from an individual).

The US reached a compromise with the EU (and Switzerland) in this matter: while the US as a whole does not provide adequate protection, they agreed to put in place a mechanism under which US companies can self-certify that they provide an adequate level of data protection. Until last week, personal data from the EU could be freely transferred to US companies that were certified according to this so-called EU-U.S. Privacy Shield (for Switzerland: Swiss-U.S. Privacy Shield).

Other safeguards

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 EU Commission or FDPIC that aim to establish data protection rules between the parties that are equivalent to the protection of personal data under GDPR.

Other measures for the legitimate transfer of personal data abroad include binding corporate rules for intra-group cross-border data transfers, the necessity to transfer personal data in order to fulfil or conclude a contract with the affected individual as well as the affected person's explicit consent.

The ruling of the CJEU and the changes to the legal landscape

The CJEU was asked to verify whether the EU-U.S. Privacy Shield and SCCs as legal frameworks provide sufficient protection of individuals' privacy when their personal data is transferred abroad under EU data protection law.

EU-U.S. Privacy Shield

As mentioned before, the US has extensive surveillance laws which for instance permit the National Security Agency to request personal data of foreign nationals in bulk if said data is, for example, stored in the US by a telecom or cloud services provider. In such cases, the CJEU stated that US national surveillance law may not limit the processing of personal data to what is strictly necessary for the surveillance programme.

Furthermore, the CJEU confirmed that the EU-U.S. Privacy Shield Framework explicitly stated that if a US company has a conflict between its obligations arising out of its certification under the EU-U.S. Privacy Shield and US surveillance laws, the latter will prevail.

This primacy of US surveillance law, the broad definition of its scope and the absence of effective legal remedies against such bulk data collection thereunder led the Court to rule that the EU-U.S. Privacy Shield Framework does not provide adequate protection of EU citizens' personal data. In consequence, the CJEU invalidated the EU Commission's decision that qualified the EU-U.S. Privacy

Shield as providing adequate data protection according to GDPR, thus voiding the EU-U.S. Privacy Shield of its purpose as a mechanism to transfer data from the EU to the US.

Standard Contractual Clauses

The SCCs as a mechanism to transfer personal data across borders were equally under review in this case. The argument was that the SCCs only apply to the parties having signed them, but not to the government (US or other) of the receiving country. So, while a data importer located in a foreign country might be willing to honour its duties as specified in the SCCs, the data importer may be prevented from doing so by a government intent on collecting the imported data for national security, *e.g.* surveillance, or other reasons.

In this regard, the Court confirmed the validity of the SCCs as a transfer mechanism. However, it took note of the issue posed by national surveillance laws and added a caveat: the data importer must actually uphold the content of the SCCs – for instance by providing effective recourse against violations – and the data exporter must implement additional safeguards to ensure an adequate level of data protection if it is necessary in light of the receiving country's laws, *e.g.* national security laws, that violate EU data protection law.

On-paper compliance

The CJEU's decision in effect, concludes that it is not sufficient anymore to "just" sign SCCs with a foreign contractual partner, file the SCCs and then forget about them. According to this ruling, any company to which the GDPR applies needs to make sure that their counterparty can actually fulfil the terms set out in the SCCs and therefore, has a burden to review the receiving country's laws to ensure that such laws in combination with the SCCs provide an adequate level of data protection.

If the required adequacy can no longer or cannot be ensured at all by the measures set out in the SCCs, the exporter may have a duty to stop or suspend such transfers and (re-)evaluate the necessary measures to ensure the required adequacy. Should the exporting company fail to do so, an individual whose personal data is transferred based on SCCs can lodge a complaint with the competent supervisory authority which has a duty to review the implemented measures. If the supervisory authority concludes that such measures are not adequate, it can prohibit or suspend the data transfer until (new) adequate measures have been implemented by the parties.

Coupled with the fact that the CJEU reminded us all that supervisory authorities have the obligation to pursue lodged complaints with the due diligence required, this might indicate the beginning of the end of "on-paper GDPR compliance through SCCs". With increased diligence required by the data exporters and importers as well as the DPAs and a precedent requiring actual and not just formal compliance, the approach of doing the necessary data protection paperwork and then quietly forgetting about it might be ending sooner than many companies had hoped for.

Unaffected transfer mechanisms

If you rely on other mechanisms such as binding corporate rules, contractual necessity or explicit consent to transfer personal data abroad, these mechanisms remain unaffected by the present ruling.

Relevance to your business

You might be asking yourself "How does this decision impact my (Swiss) business?" The question must be answered on a case-by-case basis.

Even as a Swiss company, the GDPR might apply to your business if you are offering goods and services to persons located in the EU or if you are monitoring the behaviour of persons located in the EU. Irrespective of whether GDPR applies to you or you are subject to Swiss data protection law, the following steps should be taken based on the CJEU decision:

– First you should evaluate whether you are transferring any data to the US or any other third country outside of the EU or Switzerland as well as what type of data you are transferring.

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

– If the answer is the EU-U.S. Privacy Shield and you are subject to GDPR, you need to find a different mechanism for your transfers as soon as possible, *e.g*. signing SCCs with the importing company.

– If the answer is the Swiss-U.S. Privacy Shield and you are only subject to Swiss data protection law, no immediate action is necessary. However, you should keep in mind that, based on the CJEU ruling, the FDPIC is reviewing the Swiss-U.S. Privacy Shield Framework and it is likely that it will be invalidated too (the FDPIC followed the CJEU in its decision to invalidate the predecessor of the Privacy Shield Framework – the Safe Harbor Agreement – in 2015).

– If the answer is SCCs, you should review whether the measures under SCCs can be considered as providing adequate protection according to data protection law and whether the importing company can ensure compliance with these safeguards. If this is not the case, you should start a dialogue with the importing company to identify and agree on potential additional measures that ensure adequacy under Swiss and EU data protection laws such as, for example, a code of conduct, effective legal remedies or additional encryption measures. By doing so, companies exporting personal data to third countries can avoid the suspension or prohibition of their cross-border data transfers in case supervisory authorities increasingly begin to scrutinise signed SCCs based on this CJEU ruling.

– 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 or binding corporate rules, no action is necessary at present.

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

Manuel Hofmann
Junior Associate
T: +41 58 261 53 26
manuel.hofmann@baerkarrer.ch