International Data Transfers:

FAQs on Privacy Shield and Standard Contractual Clauses

Follow up to the 'Schrems II' judgment invalidating the Privacy Shield

August 5th, 2020

Introduction

In July 2020, the Court of Justice of the European Union (CJEU) invalidated the US 'Privacy Shield'[1] data transfer arrangements. In the same judgment the Court considered Standard Contractual Clauses[2] (SCCs) are still valid for the transfer of personal data to processors established in third countries.

Shortly after, the European Data Protection Board (EDPB) published a series of answers to some frequently asked questions received by different European supervisory authorities. The document covers the following questions:

- *What did the Court rule in its judgment?*
- *Does the Court's judgment have implications on transfer tools other than the Privacy Shield?*
- *Is there any grace period during which I can keep on transferring data to the U.S. without assessing my legal basis for the transfer?*
- *I was transferring data to a U.S. data importer adherent to the Privacy Shield, what should I do now?*
- *I am using SCCs with a data importer in the U.S., what should I do?*
- *I am using Binding Corporate Rules ("BCRs") with an entity in the U.S., what should I do?*
- *What about other transfer tools under Article 46 GDPR?*
- *Can I rely on one of the derogations of Article 49 GDPR to transfer data to the U.S.?*
- *Can I continue to use SCCs or BCRs to transfer data to another third country than the U.S.?*
- *What kind of supplementary measures can I introduce if I am using SCCs or BCRs to transfer data to third countries?*
- *I am using a processor that processes data for which I am responsible as controller, how can I know if this processor transfers data to the U.S. or to another third country?*
- *What can I do to keep using the services of my processor if the contract signed in accordance with Article 28.3 GDPR indicates that data may be transferred to the U.S. or to another third country?*

The ICO has also published a new statement.

This FAQs note follows the early EFAMRO review of the immediate aftermath of the judgment available here. Whilst this document contains considerations of some of the actions recommended for adoption, it is not legal advice and should not be relied upon as such.

The US data transfer situation is evolving rapidly, and updated guidance will be issued as soon as it is officially adopted by the regulators.

While a large EU/US data transfer challenge has arisen, it is worth remembering that until December 30th, 2020 any decision taken by the EU level is binding for all UK businesses and entities.

[1] EC Decision 2016/1250 on the adequacy of the protection provided by the EU-US Data Protection Shield
[2] EC Decision 2010/87

The 'Schrems II' Judgment

About the Privacy Shield:

- The Court considered that the requirements of U.S. domestic law, and in particular certain programmes enabling access by U.S. public authorities to personal data transferred from the EU to the U.S. for national security purposes, result in limitations on the protection of personal data which are not circumscribed in a way that satisfies requirements that are essentially equivalent to those required under EU law[1], and that this legislation does not grant data subjects actionable rights before the courts against the U.S. authorities.
- As a consequence of such a degree of interference with the fundamental rights of persons whose data are transferred to that third country, **the Court declared the Privacy Shield adequacy Decision invalid**.
- **Transfers of personal data on the basis of the Privacy Shield legal framework are illegal.**

About Standard Contractual Clauses:

- In its judgment, the Court examined the validity of the Standard Contractual Clauses ("SCCs")[3] and considered them valid.
- However, the Court added that validity depends on whether SCCs include effective mechanisms that make it possible, in practice, to ensure compliance with the level of protection essentially equivalent to that guaranteed within the EU by the GDPR and that transfers of personal data pursuant to such clauses are suspended or prohibited in the event of the breach of such clauses or it being impossible to honour them.
- In that regard, the Court points out, in particular, that:
    - **SCCs impose an obligation on a data exporter and the recipient of personal data (the "data importer") to verify, prior to any transfer**, and taking into account the circumstances of the transfer, **whether that level of protection is respected in the third country concerned**; and that
    - **require the data importer to inform the data exporter of any inability to comply** with the standard data protection clauses, and where necessary with any supplementary measures to those offered by those clause, the data exporter then being, in turn, obliged to suspend the transfer of personal data and/or to terminate the contract with the data importer.

In particular:

- Whether or not you can transfer personal data on the basis of SCCs will depend on the result of your assessment, taking into account the circumstances of the transfers, and supplementary measures you could put in place. The supplementary measures along with SCCs, following a case- by-case analysis of the circumstances surrounding the transfer, would have to ensure that U.S. law does not impinge on the adequate level of protection they guarantee.
- If you come to the conclusion that, taking into account the circumstances of the transfer and possible supplementary measures, appropriate safeguards would not be ensured, you are required to suspend or end the transfer of personal data.

[3] European Commission's Decision 2010/87/EC

About "supplementary measures" to SCCs:

- The supplementary measures you could envisage where necessary would have to be provided on a case-by-case basis, taking into account all the circumstances of the transfer and following the assessment of the law of the third country, in order to check if it ensures an adequate level of protection.
    - The Court highlighted that it is the primary responsibility of the data exporter and the data importer to make this assessment, and to provide necessary supplementary measures.
- The EDPB is currently analysing the Court's judgment to determine the kind of supplementary measures that could be provided in addition to SCCs, whether legal, technical or organisational measures, to transfer personal data to third countries where SCCs will not provide the sufficient level of guarantees on their own.

About relying on the derogations of Article 49 GDPR:

- It is still possible to transfer data from the EEA to the U.S. on the basis of derogations foreseen in Article 49 GDPR provided the conditions set forth in this Article apply.
- In particular, it should be recalled that when transfers are based on the consent of the data subject, it should be:
    - explicit;
    - specific for the particular data transfer or set of transfers (meaning that the data exporter must make sure to obtain specific consent before the transfer is put in place even if this occurs after the collection of the data has been made); and
    - informed, particularly as to the possible risks of the transfer (meaning the data subject should also informed of the specific risks resulting from the fact that their personal data will be transferred to a country that does not provide adequate protection and that no adequate safeguards aimed at providing protection for the data are being implemented).

- With regard to transfers necessary for the performance of a contract between the data subject and the controller, it should be borne in mind that personal data may only be transferred when the transfer is occasional. It would have to be established on a case-by-case basis whether data transfers would be determined as "occasional" or "non-occasional". In any case, this derogation can only be relied upon when the transfer is objectively necessary for the performance of the contract.

- In relation to transfers necessary for important reasons of public interest (which must be recognized in EU or Member States' law), the EDPB recalls that the essential requirement for the applicability of this derogation is the finding of an important public interest and not the nature of the organisation, and that although this derogation is not limited to personal data transfers that are "occasional", this does not mean that personal data transfers on the basis of the important public interest derogation can take place on a large scale and in a systematic manner. Rather, the general principle needs to be respected according to which the derogations as set out in Article 49 GDPR should not become "the rule" in practice, but need to be restricted to specific situations and each data exporter needs to ensure that the transfer meets the strict necessity test.

UK: Updated ICO statement on the judgment of the European Court of Justice in the Schrems II case.

"Anyone transferring personal data internationally will have been watching the recent judgment of the CJEU with some trepidation. International data transfers, that are so vital for the global economy, suddenly became open to question.

The CJEU has confirmed how EU standards of data protection must travel with the data when it goes overseas, which means this judgment has wider implications than just the invalidation of the EU-US Privacy Shield. It is a judgment that confirms the importance of safeguards for personal data transferred out of the UK.

The European Data Protection Board (EDPB) has now issued its FAQs on the invalidation of the Privacy Shield and the implications for the Standard Contractual Clauses (SCCs), and this guidance still applies to UK controllers and processors.

Further work is underway by the European Commission and EDPB to provide more comprehensive guidance on extra measures you may need to take. In the meantime you should take stock of the international transfers you make and react promptly as guidance and advice becomes available.

The EDPB has recommended that you must conduct a risk assessment as to whether SCCs provide enough protection within the local legal framework, whether the transfer is to the US or elsewhere. The receiver of the data may be able to assist you with this.

The judgment says that supervisory authorities have an important role to play in the oversight of international transfers. We are therefore taking the time to consider carefully what this means in practice. We will continue to apply a risk-based and proportionate approach in accordance with our Regulatory Action Policy.

The ICO understands the many challenges UK businesses are facing at the present time and we will continue to provide practical and pragmatic advice and support."

https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/07/updated-ico-statement-on-the-judgment-of-the-european-court-of-justice-in-the-schrems-ii-case/

Checklist of Key Actions