International Data Transfers:

The US Privacy Shield

An initial review of the 'Schrems II' judgment invalidating the Privacy Shield

July 21st, 2020

Introduction

On the 16th of 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.

Since the decision was issued, most of the European Union national Data Protection Authorities (DPAs) have released notices of receipt and acknowledgment of the judgment, announcing further investigations and analysis on its practical implications for data transfers.

This note is a review of the current situation in the immediate aftermath of the judgment and presents the official positions of the different DPAs. 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

The General Data Protection Regulation ('the GDPR') provides that the transfer of personal data to a third country may, in principle, take place only if the third country in question ensures an adequate level of data protection. According to the GDPR, the European Commission may find that a third country ensures, by reason of its domestic law or its international commitments, an adequate level of protection.

- In this framework the European Commission adopted the 'the Privacy Shield Decision'.
- The CJEU examined the Privacy Shield in the light of the requirements arising from the GDPR and found that the requirements of US national security, public interest and law enforcement have primacy, thus condoning interference with the fundamental rights of persons whose data are transferred to that third country. In the view of the Court, the limitations on the protection of personal data arising from the domestic law of the United States on the access and use by US public authorities of such data transferred from the European Union to that third country are not circumscribed in a way that satisfies requirements that are essentially equivalent to those required under EU law, by the principle of proportionality, in so far as the surveillance programmes based on those provisions are not limited to what is strictly necessary. The Court added that, although those provisions lay down requirements with which the US authorities must comply when implementing the surveillance programmes in question, the provisions do not grant data subjects actionable rights before the courts against the US authorities.
- On all those grounds, the Court declared the Privacy Shield decision invalid.

In the absence of an adequacy decision with the US, international data transfers between the EEA and the US may take place only if the personal data exporter established in the EU has provided appropriate safeguards, which may arise, in particular, from standard data protection clauses adopted by the European Commission, and if data subjects have enforceable rights and effective legal remedies.

- Regarding the assessment of the level of protection required in respect the transfer, the CJEU specified that it must take into consideration both the contractual clauses agreed between the data exporter established in the EU and the recipient of the transfer established in the third country concerned and, as regards any access by the public authorities of that third country to the data transferred, the relevant aspects of the legal system of that third country.
- The CJEU considered that the validity of the SCCs depends on whether they include 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 such clauses are suspended or prohibited in the event of the breach of such clauses or it being impossible to honour them. The Court found that SCCs establish such mechanisms. In that regard, the Court pointed out, in particular, that SCCs impose an obligation on a personal data exporter and the recipient of the personal data to verify, prior to any transfer, whether that level of protection is respected in the third country concerned and that SCCs require the recipient to inform the personal data exporter of any inability to comply with the standard data protection clauses, the latter then being, in turn, obliged to suspend the transfer of personal data and/or to terminate the contract with the former.

In practice – in the EEA

European businesses can no longer rely upon the Privacy Shield and should immediately adopt Standard Contractual Clauses (SSCs) in all the contracts that require international transfers of data to the US and any other 'third' countries[3].

With some caveats.

- SCCs offer only the basic level of protection. Data exporters must assess **on a case-by-case basis** whether additional safeguards are needed. They should verify the legal conditions in a country and in particular the laws which may apply to the particular parties / personal data before making a transfer.
  - ✓ Where necessary, they must put additional measures of protection in place to address any issues.
  - × If the third-country law imposes obligations on the recipient contrary to the SCCs undermining an adequate level of protection against access by the public authorities, the transfer cannot be made.
- SCCs already require recipients to notify the exporter of any change in law affecting compliance with the SCCs.
  - × The CJEU states that if a situation cannot be remedied by the parties, the personal data must be returned or destroyed; transfer in breach may give rise to a compensation claim for damages suffered by individuals whose personal data is transferred.
- Data Protection Authorities (**DPAs**) must suspend personal data transfers based on SCCs where they take the view that, in the light of all the circumstances of a particular transfer, they are not or cannot be complied with in the destination country and the personal data cannot be protected by any other means.
  - ✓ The CJEU noted the obligation under the SCCs on the recipient to make the controller aware of issues in a particular jurisdiction and on the controller to pass this information to the DPA to investigate.

In practice – in the UK

The ICO is currently reviewing both Privacy Shield and SCCs.

Their latest statement available here https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/

If you are currently using Privacy Shield, please continue to do so until new guidance becomes available.

Please do not start to use Privacy Shield during this period.

If you have any specific questions, please call our helpline on 0303 123 1113.

[3] A Third Country is a country that is not in the EEA, nor covered by an adequacy decision https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

Checklist of Key Actions

✘ STOP relying on Privacy Shield

UK Exception	UK businessed can keep on using the Privacy Shield until further notice

✓ Adopt Standard Contractual Clauses

EU controller to non-EU or EEA controller For further information: bit.ly/2Bmw9P8	EU controller to non-EU or EEA processor For further information: bit.ly/2Bmw9P8

✓ Review your contracts

Carry out a case by case assesment	Verify if the laws in the destination country ensure adequate protection of personal data	Review the specific circumstances of each personal data transfer including types, volumes, purposes, recepients.	Take account of the specific risks for personal data being transferred

✓ Consider additional safeguards

Anonymization, encryption, or other security measures that can help mitigate the risks

✓ Record your decision making process

Implement governance changes	Update Privacy Notices

What are Additional Safeguards?

GDPR Recital 108 states:

Those safeguards should ensure compliance with data protection requirements and the rights of the data subjects appropriate to processing within the EU, including the availability of enforceable data subject rights and of effective legal remedies, including to obtain effective administrative or judicial redress and to claim compensation, in the EU or in a third country. They should relate in particular to compliance with the general principles relating to personal data processing, the principles of data protection by design and by default.

Data Protection Authorities reactions

European Data Protection Board[4]

The European Data Protection Board (EDPB) intends to continue playing a constructive part in securing a transatlantic transfer of personal data that benefits EEA citizens and organisations and stands ready to provide the European Commission with assistance and guidance to help it build, together with the U.S., a new framework that fully complies with EU data protection law.

The CJEU's judgment also recalls the importance for personal data exporters and importers to comply with their obligations included in the SCCs, in particular the information obligations in relation to change of legislation in any importer's country. When those contractual obligations are not or cannot be complied with, the exporter is bound by the SCCs to suspend the transfer or terminate the SCCs or to notify its competent supervisory authority if it intends to continue transferring data.

The EDPB takes note of the duties for the competent DPAs to suspend or prohibit a transfer of data to a third country pursuant to SCCs, if, in the view of the competent SA and in the light of all the circumstances of a personal data transfer, those clauses are not or cannot be complied with in that third country, and the protection of the personal data transferred cannot be ensured by other means, in particular where the controller or a processor has not already itself suspended or put an end to the transfer.

Most of the European DPAs welcomed the judgment, announcing further investigation and cooperation with the EDPB in publishing guidance as soon as possible. A few other took a slightly different stand:

Berlin data protection authority[5]

The Berlin Commissioner the Berlin Commissioner highlighted that, following the judgment, personal data should not be transferred to the US until that legal framework is reformed. Data controllers transferring personal data to the US, especially when using cloud service providers, are now required to use service providers based in the EEA or in a country with an adequate level of protection.

Information Commissioner Office[6]

The ICO issues the following statement: "The ICO is considering the judgment from the European Court of Justice in the Schrems II case and its impact on international data transfers, which are vital for the global economy. We stand ready to support UK organisations and will be working with UK Government and international agencies to ensure that global data flows may continue and that people's personal data is protected."

---

[4] https://edpb.europa.eu/news/news/2020/statement-court-justice-european-union-judgment-case-c-31118-data-protection_en

[5] https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2020/20200717-PM-Nach_SchremsII_Digitale_Eigenstaendigkeit.pdf

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