TRANSCENDENT GROUP INSIGHT

Highlighting EDPB's recommendations for data transfers following Schrems II

The European Data Protection Board (EDPB) published two documents on November 11, 2020, aimed at providing guidance on supplementary measures to be taken to ensure data transfers are GDPR-compliant following the Court of Justice of the European Union (CJEU) Schrems II ruling in July 2020.

The EDPB published:

1. Recommendations 01/2020 "on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data" to assist data exporters in identifying and implementing appropriate supplementary measures where necessary; and
2. Recommendations 02/2020 "on the European Essential Guarantees for surveillance measures" that offers elements to determine if the legal framework governing public authorities' access to data for surveillance purposes in third countries can be regarded as justifiable.

This long-awaited EDBP guidance – under public consultation until November 30, 2020 - fills part of the void left by the Schrems II ruling which invalidated the US-EU Privacy Shield. With Privacy Shield invalidated, companies and privacy professionals scrambled to interpret and adhere to the court ruling and the numerous, sometimes conflicting, national interpretations by local authorities that followed.

The challenge has been, and continues to be, navigating the new legal context and ambiguity of the ruling: on the one hand, Privacy Shield has been declared invalid as a mechanism for cross border transfers as it lacked sufficient protection of EU citizens from exposure to US surveillance activities. On the other hand, Standard Contractual Clauses (SCC) were deemed to continue to be a viable measure to ensure data transfer under the GDPR, if data exporters performed their own analysis of the privacy laws in the respective country, the risks associated with the data transfer as well as the need to implement supplementary measures to safeguard the transfers. The requirement for these case by-case assessments mirrors the requirement for controllers to be responsible for and able to demonstrate compliance with the GDPR's principles relating to processing of personal data (such as the principle of accountability in Article 5.2).

The EDBP's recommendations contain clear guidance and a roadmap of steps for data exporters to establish whether they need to implement supplementary measures to continue to transfer data outside the EEA compliant with EU law. In addition to a proposed series of steps, the EDPB provides potential sources of information and examples of supplementary technical, contractual and organisational measures.

EDBP step-by-step roadmap for data exporters

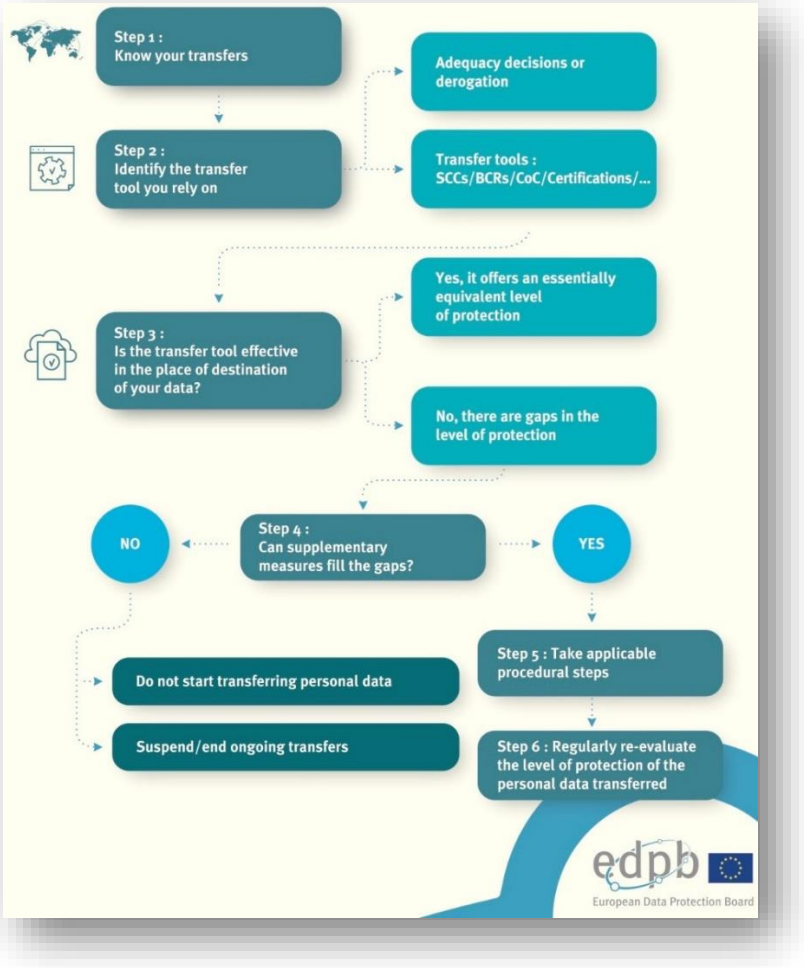

Figure 1: EDPB Infographic – Roadmap for data exporters

1. Know your transfers

Map all data transfers outside the EEA, and not just those to the US: The Schrems II ruling affects all transfers outside of the EEA to countries who do not have an adequacy decision from the Commission.

2. Verify the transfer tool

Review the transfer tool relied upon against the provisions of the GDPR (Chapter V on international transfers) and EU findings on specific countries. This includes the use of SCCs as transfer tool.

3. Assess the law or practice of the third country

Review the local legislation relevant to the transfer and whether it may undermine the necessary level of protection provided by the transfer tool. For this step, the EDPB issued its second set of recommendations, the European Essential Guarantees. In essence, these are:

A. Processing should be based on clear, precise and accessible rules
B. Necessity and proportionality with regard to the legitimate objectives pursued need to be demonstrated
C. An independent oversight mechanism should exist
D. Effective remedies need to be available to the individual

4. Identify and adopt supplemental measures

If your assessment in step 3 concludes that the relevant local legislation jeopardises the effectiveness of the transfer tool, you must identify and adopt supplementary measures "necessary to bring the level of protection of the data transferred up to the EU standard of essential equivalence." As a key element of its recommendations, the EDBP provides a non-exhaustive list of example supplementary measures with conditions they require to be effective (see also below).

5. Take formal procedural steps

Comply with formalities involved in implementing safeguard measures, including consultation and/or approval processes with the relevant supervisory authority.

6. Regularly re-evaluate actions taken

Ensure an ongoing monitoring of the level of protection afforded to the data transferred to third countries as well as changes in regulatory guidance requiring action.

Supplemental measures

In the core of its recommendations, the EDPB provides examples for supplemental measures that have been the focus of much discussion over the past months. The list presents an extensive but not exhaustive list with details on relevant technical (e.g., encryption, pseudonymization), contractual (commitments, incl. importer commitments to transparency, audits) and organisational (e.g., policies, training) measures. In this context it is stressed that contractual and organisational safeguard measures can only complement, but not replace, sufficient technical measures.

In addition, the EDPB calls for data transfers to cease where the analysis has identified deficiencies in the transfer tools that cannot be remedied by supplementary measures:

"Selecting and implementing one or several of these measures will not necessarily and systematically ensure that your transfer meets the essential equivalence standard that EU law requires. You should select those supplementary measures that can effectively guarantee this level of protection for your transfers. Any supplementary measure may only be deemed effective in the meaning of the CJEU judgment "Schrems II" if and to the extent that it addresses the specific deficiencies identified in your assessment of the legal situation in the third country.

If, ultimately, you cannot ensure an essentially equivalent level of protection, you must not transfer the personal data."

Updated SCC in the making

The area of contractual measures continues to pose special challenges in establishing sufficiently effective and enforceable safeguards. In this context, and one day after the publication of the EDPB recommendations, the EU Commission published its draft Implementing Decision on standard contractual clauses for the transfer of personal data to third countries, aimed at updating the current SCC templates. This draft will be under consultation until December 10.

Next steps

The extensive EDPB recommendations will be scrutinized over the coming weeks. While providing clear and explicit guidance, the recommendations - not unexpectedly - leave it to controllers and processers to analyse and conclude on each individual data transfer.

The complexity and challenge facing data exporters, especially regarding effective and enforceable contractual measures, will likely remain until the execution of a new adequacy agreement between the EU and US, which seems unlikely in the short term.

As a starting point, data exporters should closely analyse the EDPB guidance when reviewing relevant data flows outside the EEA based on the board's roadmap and suggested measures provided. Further guidance may follow over the coming weeks and months, with EU authorities busy working on the regulatory framework for data protection post Schrems II. This includes the revision of the current SCC templates.

Meet the Schrems – background to the court cases

In 2011 Max Schrems, an Austrian lawyer and activist, began filing numerous complaints with the Irish data protection authority, including against Facebook's European operations, incorporated in Ireland. Schrems alleged widespread intrusion into users' privacy due to Facebook's processing of personal data without consent, e.g., the inability to block one's name and photo being tagged by others in the platform. Following revelations of vast US surveillance programs in 2013, including the National Security Agency's direct access to data processed by Google, Facebook, Apple and other tech giants, led to renewed judicial action by Schrems and eventually to a CJEU ruling in October 2015.

In what became known as **Schrems I**, the CJEU ruled in judgment C-362/14 in Schrems' favour, condemning US surveillance activities as interfering with the fundamental rights of EU citizens and declaring the EU-US data transfer agreement of the time, known as "Safe Harbour", as invalid.

In the aftermath of Schrems I, the EU and US agreed on a new data transfer agreement – "Privacy Shield" - which, among other measures, is based upon the use of SCCs stipulating the terms, roles and responsibilities of parties involved in the data transfer.

Not happy with the perceived lack of improvement of privacy arrangements under the new agreement, together with the continued surveillance activities by US authorities, Max Schrems filed a new case in 2018, just two months after the GDPR came into effect.

The CJEU issued its judgment C-311/18 on July 16, 2020, known as **Schrems II**. With its ruling, the court invalidated Privacy Shield, noting that US surveillance activities were not limited as envisaged by the agreement to the continued detriment of EEA residents. At the same time, the ruling upheld the use of SCCs as a valid transfer mechanism provided case-by-case assessments and additional safeguard measures are implemented as appropriate.

Sources and useful links:

EDPB – recommendations 01/2020 and 02/2020

Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data - version for public consultation

Recommendations 02/2020 on the European Essential Guarantees for surveillance measures

EDPB Roadmap: Applying the principle of accountability to data transfers in practice

EU Commission draft Implementing Decision

https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12741-Commission-Implementing-Decision-on-standard-contractual-clauses-for-the-transfer-of-personal-data-to-third-countries

The Guardian article "The background to EU citizens' court win over US tech giants", accessed 2020-11-13.

Please reach out

andreas.liese@transcendentgroup.com

+46 70 143 5049

ranjit.mahida@transcendentgroup.com

+47 9381 3156