

EDPB adopts New Recommendations to Review International Data Transfers

The Schrems II decision of the Court of Justice of the EU (**CJEU**) caused quite a stir for organisations that transfer personal data outside the EU. First, the decision invalidated the EU-US Privacy Shield scheme, that was designed to permit transfers between the EU and self-certified organisations in the US. On the other hand, it held that Standard Contractual Clauses (**SCC**) that had been approved by the European Commission still provide sufficient safeguards, but nevertheless organisations had to assess on a case-by-case basis whether the SCC should be supplemented by additional measures (see our note on the Schrems II decision [here](#)).

The European Data Protection Board (**EDPB**) has now adopted two recommendations outlining the approach it expects organisations to take when transferring data out of the EU. We provide a short overview of these two recommendations, Recommendations 01/2020 on measures that supplement transfer tools (available [here](#)), and Recommendations 02/2020 on European Essential Guarantees for surveillance measures (available [here](#)), and thus the steps that organisations will need to take to assess their international transfers.

ASSISTING INTERNATIONAL TRANSFERS OF PERSONAL DATA

In Recommendations 01/2020, the EDPB sets out a six-step process for data exporters (controllers or processors, private entities or public bodies processing and transferring personal data out of the EU) to comply with the provisions on international transfers under General Data Protection Regulation 2016/679 (the **GDPR**). These recommendations provide guidance on the steps to follow, on potential sources of information, and on some examples of supplementary measures that could be put in place. In particular, EU data exporters have been advised to:

1. Map all transfers of data outside of the EU.
2. Verify the transfer tools relied on for each transfer.
3. Assess whether there is anything in the law or practice of the third country that may impinge upon the effectiveness of the appropriate safeguards. To carry out this assessment, the EDPB refers to its guidance on “European Essential Guarantees” (see below).
4. Identify and adopt supplementary measures.
5. Take formal procedural steps to implement supplementary measures.
6. Regularly re-evaluate the developments of the transfers.

In addition to the compliance steps, the Recommendations include a non-exhaustive list of supplementary measures that should be implemented in order to effectively guarantee an adequate level of protection for international transfers. For instance, a data exporter uses a hosting service provider in a third country to store personal data, e.g., for backup purposes. If the personal data are processed using strong encryption before transmission, then the EDPB considers that the encryption performed provides an effective supplementary measure.

Finally, the EDPB underlines the importance of documenting this process and the assessments that are made in light of the accountability principle under Articles 5.2 and 24 of the GDPR.

EUROPEAN ESSENTIAL GUARANTEES FOR SURVEILLANCE MEASURES

As set out above, data exporters may need to assess the laws on surveillance measures in the jurisdiction of the data importer to make sure interferences with the rights to privacy and the protection of personal data “*do not go beyond what is necessary and proportionate in a democratic society*”.

Following the analysis of the jurisprudence, including the Schrems I and II cases, the EDPB considers that the assessment of the limitations to the data protection and privacy rights recognised by the Charter is based on four European Essential Guarantees:

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

The EDPB notes that the European Essential Guarantees are a referential standard when assessing the interference by third-country surveillance measures in the context of international data transfers. Such standards derive from EU law and the jurisprudence of the CJEU and the European Court of Human Rights, which is binding on Member States.

Both recommendations are open for public consultation until 30 November 2020 and feedback can be submitted [here](#).