ELVINGER HOSS
LUXEMBOURG LAW

EDPB Recommendations 01/2020 and 02/2020 on transfers of personal data after Schrems II

What happened?

On 10 November 2020, the European Data Protection Board ("**EDPB**") adopted two sets of recommendations on the transfer of personal data from the European Union ("**EU**") to third countries further to the Court of Justice of the European Union ("**CJEU**") ruling in the Schrems II case[1]:

- Recommendations 01/2020 on measures that supplement data transfer tools to ensure compliance with the EU level of protection of personal data ("**Recommendations on Supplementary Measures**"), open for public consultation; and
- Recommendations 02/2020 on the European Essential Guarantees for surveillance measures ("**EU Essential Guarantees**").

Significance of these recommendations

These two sets of recommendations were highly anticipated by businesses and organisations with regard to the CJEU's (i) invalidation of the EU-US Privacy Shield and (ii) call for compliance with the requirements to be me for standard contractual clauses ("**SCCs**") to be valid in practice under the EU General Data Protection Regulation ("**GDPR**").[2] Although the ruling, aside from the EU-US Privacy Shield, only concerns the standard contractual clauses, the principles set out by the ruling equally apply to other transfer mechanisms, such as the binding corporate rules.

In a nutshell, the Recommendations on Supplementary Measures provide for a road map of good practices for data exporters while the EU Essential Guarantees outline certain features that need to be evaluated to assess whether the legislation of the third countries governing access to personal data by public authorities is to be regarded as a justifiable interference or not.

What are the main practical takeaways?

In its Recommendations on Supplementary Measures, the EDPB suggests following a methodology oriented around the six following steps.

- **Step 1: Know your transfers.** Data exporters should record and map all international personal data transfers and verify whether they are adequate, relevant and limited to what is necessary in relation to the purposes for which they are operated. Organisations should aim to be fully aware of their data transfers (including onward transfers) despite the existence of numerous processors and sub-processors.
- **Step 2: Identify the transfer tools relied upon.** Organisations should identify the appropriate mechanism for the data transfer (e.g. adequacy decision, SCCs, derogation for specific situations of Article 49(1) GDPR, etc.). The EDPB notes that no further steps are required for transfers relying on an adequacy decision, provided that the data importer has implemented measures to comply with the obligations of the GDPR as appropriate.
- **Step 3: Assess whether the transfer tool you relied upon is effective in light of all the circumstances of the transfer.** Organisations are responsible for assessing and analysing whether the laws and practices of the third countries concerned are effective enough to meet the appropriate safeguards set by the GDPR. This assessment shall include the circumstances as well as all the players participating in the transfer previously mapped in Step 1.

  Special attention should be given to the EU Essential Guarantees. According to these, organisations must:
  - Assess whether the processing is based on clear, precise and accessible rules; and
  - Evaluate the third countries' legislation providing for the disclosure of personal data to public authorities or grant public authorities powers to access personal data. The EDPB highlights that those laws must be publicly available and limited to what is regarded as justifiable interference and therefore not jeopardise the commitment taken in the appropriate safeguard concerned
- **Step 4: Adopt supplementary measures.** If the appropriate safeguard adopted for the data transfer is not effective according to the assessment in Step 3, organisations (in cooperation with data importers) will have to adopt supplementary measures along with that appropriate safeguard to attain an equivalent level of data protection, as is required by the GDPR.
- **Step 5: Adopt procedural steps if you have identified supplementary measures.** Organisations which have identified adequate supplementary measures will have to implement supplementary procedural steps or additional requirements before use.
- **Step 6: Re-evaluate at appropriate intervals.** Data exporters must continuously monitor significant developments that may affect the level of data protection in the third countries concerned. If a country has passed a new national security law, organisations might, for example, have to repeat Step 3.

What's next?

The recommendations are and constitute a first useful and practical response to the Schrems II ruling. Data exporters will have to make extra efforts and, on a case-by-case basis, assess their current and intended transfers of personal data. In parallel, data exporters must stay tuned as regards the adoption by the European Commission of updated SCCs as a

new set of SCCs has now been published for public consultation.[3]

This may also interest you :

- CJEU invalidates the Privacy Shield: implications for EU-US personal data transfers
- EDPB's FAQ about the invalidation of the Privacy Shield
- EDPS publishes its strategy for Union institutions' compliance with "Schrems II" ruling

1 Case C-311/18 Data Protection Commissioner v Facebook Ireland and Maximillian Schrems. For more information on the ruling in this Case, please read our previous **publication**.

2 Regulation (EU) 2016/679.

3 On 12 November 2020, the European Commission has published its draft Implementing Decision on standard contractual clauses for the transfer of personal data to third countries which will be open for public consultation until 10 December 2020. The draft SCCs can be consulted at **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**.

Subscribe to EHLO, our dedicated ICT, IP, media and data protection news