PAUL HASTINGS

Stay Current

November 2020

Follow @Paul_Hastings

EDPB Publishes Highly Anticipated Recommendations For Supplemental Measures Following Schrems II

By Sarah Pearce & Ashley Webber

On 10 November 2020, the European Data Protection Board ("EDPB") adopted Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (the "Recommendations"). The Recommendations follow on from the Court of Justice of the European Union's ("CJEU") judgement C-311/18, commonly known as Schrems II (further details of which can be read here). To recap, the CJEU stated that exporters are responsible for verifying, on a case-by-case basis and, where appropriate, in collaboration with the importer, if the laws or practices of the third country impinge on the effectiveness of the appropriate safeguards contained in the Article 46 GDPR transfer tools. In those cases where the laws or practices do impinge on the effectiveness, the CJEU stated that the exporter should either cease transferring the personal data or implement supplementary measures that fill the gaps in the protection and bring it up to the level required by EU law.

The CJEU did not specify what supplementary measures could, or should, be implemented in this respect. The Recommendations are intended, therefore, to assist exporters with the "complex task" of assessing third countries and identifying appropriate supplementary measures to protect personal data where needed.

Whilst many may have hoped, or expected, the Recommendations to be the "Holy Grail" with regards supplementary measures, this is not the case, and in reality, couldn't have been given that all transfer-related scenarios or eventualities could not be detailed in the Recommendations, nor could the EDPB review the laws and practices of each third country in the world to determine whether equivalent protection is provided. Instead, the Recommendations offer some very useful suggestions. The EDPB has approached the matter from a practical perspective, using fairly common use cases as examples (discussed further below) for determining whether a supplementary measure would be effective or not. The supplementary measures listed in the Recommendations are expressly stated to be "non-exclusive" meaning organisations still have scope to establish other measures which are suitable for their business and operations. This approach mirrors that taken generally by much of the guidance on the GDPR and implementation of its requirements, i.e., no one size fits all.

It is worth noting that the EDPB does not include commentary specifically on transfers of personal data to the U.S., save for very limited example purposes only. Transfers to the U.S. can therefore be considered as not having been automatically ruled out by the EDPB at this stage: they can take place but existing or future transfers should be carefully analysed in accordance with the Recommendations.

Six Steps to Follow

The Recommendations provide exporters with six steps to follow when transferring personal data to a third country, each of which, the EDPB notes, should be appropriately documented:

1. **Know your transfers**: all transfers of personal data should be recorded and mapped, including onward transfers. This is an essential step to ensure fulfilment of the principle of accountability in any event. An organisation's existing records of processing will be a useful tool to start this exercise.

2. **Identify transfer tools**: for the transfers mapped, identify which transfer tool under Chapter V of the GDPR (e.g., an adequacy decision or Standard Contractual Clauses ("SCCs")) is currently relied upon. If the tool is an adequacy decision, the Recommendations note that no further steps are required.

3. **Assess whether the transfer tool is effective**: as discussed in more detail below, this step requires an analysis be undertaken (in collaboration with the importer if relevant) of the laws and practices of the third country to determine whether any such may "impinge on the effectiveness of the appropriate safeguards" provided by the transfer tool being relied upon.

4. **Adopt supplementary measures**: as discussed in more detail below, if step 3 has revealed the transfer tool is not effective, the exporter must consider (in collaboration with the importer if relevant) if supplementary measures, when added to the existing safeguards, could ensure the personal data is afforded protection essentially equivalent to that guaranteed in the EU.

5. **Procedural steps**: if effective supplementary measures have been identified, the EDPB notes certain procedural steps that may be required before use. For example, if the exporter intends to modify the SCCs themselves or where the supplementary measures "contradict directly or indirectly" the SCCs, the exporter is no longer deemed to be relying on SCCs and must seek authorisation from the competent supervisory authority.

6. **Re-evaluate at appropriate intervals**: the exporter must monitor, on an ongoing basis, developments in the third country that could affect the initial assessment, including implemented supplementary measures.

We have discussed steps 3 and 4 below in further detail, focusing on the suggestions made by the EDPB with respect to undertaking an analysis of a third country and the nature of the supplementary measures proposed.

Assessing Whether the Transfer Tool is Effective (Step 3)

This step focuses on one of the key messages from the CJEU decision: it is the responsibility of the exporter to analyse whether the personal data it transfers is adequately protected in the third country. The EDPB notes that "all actors participating in the transfer" should be considered, and, of course, the more actors, the more complex the assessment will be.

The exporter will therefore need to look into the characteristics of each transfer and determine how domestic legal order of the third country applies to such transfer. The laws of the third country that are applicable will depend on the circumstances of the transfer, including, for example:

- Purposes for the transfer;
- Types of entities involved, e.g., public or private;

- Sector in which transfer occurs;
- Categories of data transferred;
- Whether the data will be stored in the third country or whether there is only remote access.

The EDPB notes specifically that consideration should be given to whether commitments in the Article 46 transfer tool enabling data subjects to exercise their rights (e.g., right of access or erasure) can be effectively applied in practice and are not thwarted by the laws of third country. The exporter should "pay specific attention" to any laws laying down requirements to disclose personal data to public authorities or granting public authorities powers of access to personal data. If such requirements or powers are "limited to what is necessary and proportionate in a democratic society", they may not necessarily impinge on any such commitments.

At the same time as adopting the Recommendations, the EDPB also adopted its Recommendations 02/2020 on the European Essential Guarantees for surveillance measures (the "EEG"), which are discussed and referred to in the Recommendations. The EEG lists certain features which have to be assessed to determine whether the legal framework governing access to personal data by public authorities in a third country such as national security agencies or law enforcement authorities, can be regarded as a justifiable interference or not. The EEG are based on the Charter of Fundamental Human Rights and the European Convention of Human Rights and, as with the Recommendations, state explicitly that "they do not aim on their own to define all elements that might be necessary when assessing the legal regime of a third country". The EEG are as follows:

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 firmly states these EEG should be viewed as "core elements to be found when assessing the level of interference with the fundamental rights to privacy and data protection" and should be assessed on an overall basis as opposed to independently. Applied to step 3 of the Recommendations, the EEG can assist the exporter in assessing whether the powers of a public authority unjustifiably interfere with the importer's obligations to ensure essential equivalence.

The idea is that the step 3 assessment will reveal whether the transfer tool relied upon either:

- Effectively ensures that the transferred personal data is afforded a level of protection in the third country that is essentially equivalent to that guaranteed within the EEA. In this case steps 4 and 5 are not required; or
- Does not effectively ensure an essentially equivalent level of protection. The importer cannot comply with its obligations, owing to the third country's legislation and/or practices applicable to the transfer. In such instances, the exporter should proceed with step 4.

Adopting Supplementary Measures (Step 4)

Where appropriate, the obligation is on the exporter to consider on a case-by-case basis which supplementary measures could be effective for a set of transfers. Such measures may be contractual, technical or organisational in nature, and the EDPB confirms that "combining diverse measures in a way that they support and build on each other may enhance the level of protection",

and ultimately contribute to meeting the equivalency standard. It's worth noting that, in the EDPB's view, contractual and organisational measures alone will generally not overcome access to personal data by public authorities and only technical measures will "impede or render ineffective" public authority access.

Annex 2 of the Recommendations, arguably the most important and anticipated section of the Recommendations, provides examples of technical, contractual and organisational measures that could be considered by an exporter. As noted above, this is a non-exhaustive list of examples, and implementing one or several of the measures "will not necessarily and systematically ensure" the transfer meets the equivalence standard required. We analyse below the various measures listed.

A. Technical measures

The examples of technical measures are split into two types of possible scenario:

1. Scenarios where effective measures ***could be*** found; and

2. Scenarios where effective measures ***could not be*** found.

By displaying the measures in this way, the EDPB has strived to provide practical guidance and, to a degree, has achieved this goal. Of course, the obvious critique of this method is that many scenarios are not considered in Annex 2 and such will still require significant analysis.

As regards scenarios where technical measures ***could be found***, the Recommendations include five use cases whereby the measures listed are intended to ensure that access to the transferred data by public authorities does not impinge on the effectiveness of the transfer tools and, ultimately, does not infringe the rights of data subjects. This is achieved through several instances, including by preventing the authorities from identifying the data subjects, or inferring information about them. Case 1, for example, states that an exporter using a hosting service provider in a third country to store personal data may be able to ensure the personal data is protected if, along with five other measures, the personal data is processed using "strong" encryption before transmission.

In our view, the measures included in each use case require a high standard be met and the EDPB uses language emphasising the significant responsibility on the exporter to ensure the relevant measures are sufficient. For example, in use cases 1 and 3, the encryption algorithm must be "flawlessly implemented", in use case 2 (transfer of pseudonymised data), the additional information must be held exclusively by the exporter in a separate country from the importer, and in use case 5 (split or multi-party processing), the algorithm used for the shared computation must be "secure against active adversaries".

With respect to the scenarios where effective measures ***could not be found***, only two use cases are detailed. Whilst on the face of it, the use cases appear to be commonly executed transfers, it is important to flag that both scenarios will only exist if the power granted to public authorities of the recipient country to access the transferred data goes beyond what is necessary and proportionate in a democratic society.

B. Contractual Measures

The EDPB notes that contractual obligations will not be able to rule out the applicability of the legislation of the third country but the Recommendations do incorporate a series of possible unilateral, bilateral and multilateral commitments that may be included in contractual arrangements to better protect the transferred personal data. The Recommendations do not, perhaps wisely, include exact wording for the contractual provisions but instead provide possible obligations or rights that could be imposed or granted, as appropriate, and the conditions required for the provision to be effective.

In our view, the proposed contractual provisions seek to plug the key gaps that exist when a public authority has the right to access personal data. By providing the conditions for effectiveness, again, the EDPB has sought to deliver practical guidance that still allows organisations flexibility on implementation. Like any situation, however, contractual obligations are only as good as the relevant party's ability or choice to comply. It is therefore crucial that contractual measures are not used in isolation when seeking to achieve equivalence.

C. Organisational Measures

Such measures will be dependent on the nature and size of the organisations. The Recommendations note these may consist of internal policies, organisational methods, and standards controllers and processors could apply to themselves and impose on the importers. Implementing organisational measures will unlikely guarantee a transfer meets the equivalence standard but will certainly assist with improving the awareness of the exporter and its employees, thus demonstrating efforts to comply. The simple adoption of clear governance policies will, for example, assist employees with understanding their roles and responsibilities in relation to transferring personal data.

What's Next?

As discussed above, the Recommendations are undoubtedly a helpful tool for digesting and applying the CJEU's judgement, and include a number of useful practical suggestions, particularly with respect to the supplementary measures. That said, it is important for organisations seeking to use the Recommendations to understand that they are essentially a roadmap, requiring careful consideration and significant input from the organisation undertaking the analysis. Each relevant transfer will need to be assessed on its merits, and it may well be the case that certain transfers cannot be continued, even with the use of supplementary measures. To the extent organisations have not commenced the EDPB's step 1, such organisations should prioritise this a matter of data protection compliance. Finally, it is worth noting that the adoption of the updated SCCs is expected to take place before the end of the year, and organisations pursing the EDPB's Recommendations should be mindful of such upcoming development.

✧ ✧ ✧

If you have any questions concerning these developing issues, please do not hesitate to contact either of the following Paul Hastings London lawyers:

Sarah Pearce
44.020.3023.5168
sarahpearce@paulhastings.com

Ashley Webber
44.020.3023.5197
ashleywebber@paulhastings.com