PAUL HASTINGS

Stay Current

June 2021

Follow @Paul_Hastings

# *EDPB Publishes Version 2 of the Supplemental Measures for International Transfers*

By Sarah Pearce & Ashley Webber

On 18 June 2021, the European Data Protection Board ("EDPB") adopted version 2 of its Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (the "Recommendations"). Version 1 of the Recommendations was adopted in November 2020 and is discussed in detail here.

As a reminder, the Recommendations were prepared in response to the decision by the Court of Justice of the European Union in *Schrems II* which said transfers of personal data should only be made to third countries if the personal data would be subject to "essentially equivalent" protection to that provided in the EU. To ensure such protection, the Court noted that the relevant parties may be required to implement additional measures to supplement the chosen transfer tool (e.g., the Standard Contractual Clauses for transfers of data to third countries).

The aim of the Recommendations was to "*help exporters (be they controllers or processors, private entities or public bodies, processing personal data within the scope of application of the GDPR) with the complex task of assessing third countries and identifying appropriate supplementary measures where needed*". The Recommendations sought to achieve this aim through a six-step process:

1. Know your transfers.
2. Identify transfer tools your transfer relies on.
3. Assess whether anything in the law and/or practices in force of the third country may impinge on the effectiveness of the appropriate safeguards of the transfer tools you are relying on, in the context of your specific transfer.
4. Identify and adopt supplementary measures.
5. Take any formal procedural steps.
6. Re-evaluate at appropriate intervals.

The process itself has not changed in the new Recommendations.

Version 1 of the Recommendations received some criticism when it was adopted last year; in the main, this related to the guidance not being as in-depth or practical as expected and not containing sufficient suggestions for technical measures that could be implemented when supplementary measures were identified as necessary. This article discusses and summarises the key updates made to the Recommendations in Version 2.

## Key Updates

### I. Derogations (Step 2)

In paragraph 27, the EDPB reinforces the message stated in the GDPR regarding the use of derogations as a method for transferring personal data to third countries: derogations should not be used in a way which would "*contradict the very nature of the derogations as being exceptions from the rule*", i.e., they should only be used in exceptional cases where the circumstances permit so. The EDPB states clearly that the derogations "*cannot become 'the rule' in practice, but need to be restricted to specific situations*". The removal of the term "occasional" in the updated Recommendations is interesting: is the EDPB opening up the possibility for looking to derogations perhaps where a scenario emerges for which there is no alternative?

### II. Assessing the Transfer (Step 3)

Step 3 of the Recommendations has seen the biggest overhaul in version 2 and the changes provide welcome additional guidance to this crucial step in the analysis process. In version 1 of the Recommendations, step 3 provided a fairly high level overview of the areas which should be considered when assessing the relevant transfer. While the purpose of step 3 remains the same, the new Recommendations now provides a more thorough and focused set of considerations for organisations to assess when transferring personal data.

Step 3 requires the exporter to first assess, where appropriate in collaboration with the importer, whether anything in the law and/or practices in force in the third country may impinge on the effectiveness of the transfer tool it is relying on to transfer the personal data. This includes determining whether the transfer in question ***falls within the scope*** of such legislation and/or practices which may impinge on the effectiveness of the transfer tool. According to version 2, the assessment must be "*based first and foremost on legislation publicly available*" (discussed further below).

The key points to note from the updated step 3 are as follows:

- **Public Authorities**. Step 3 now draws significantly more attention to the possible risks to personal data related to public authorities in the importing country (which was, of course, a crucial part of the *Schrems II* decision). Whilst public authorities were referred to throughout version 1 of the Recommendations, this updated step 3 now delves deeper into the issue and focuses more on this risk highlighted in *Schrems II*. For example, see paragraph 31 which notes any assessment must contain elements which seek to identify whether a public authority would seek to access the personal data with or without the knowledge of the importer.

- **Data Protection Legislation**. Whilst likely the interpretation of version 1, version 2 now specifically states that when analysing the laws and/or practices of the third country, this analysis is limited to the legislation and practices relevant to the protection of the data being transferred, as opposed to "*the general and wide encompassing adequacy assessments*".

- **Specific Circumstances**. Paragraph 33 lists the specific circumstances which may be relevant when assessing a transfer—this list is the same as in version 1.

- **Incompatible Laws**. Obligations or powers which permit or allow access to personal data by public authorities will be considered to impinge/be incompatible with the transfer tool if they:

- do not respect the essence of the fundamental rights and freedoms of the EU Charter of Fundamental Rights;

- exceed what is necessary and proportionate in a democratic society to safeguard one of the important objectives as also recognised in the EU or Member State law (such as those listed in Article 23 (1) GDPR).

- **Publicly Available Legislation**. As noted above, the assessment must be "*based first and foremost on legislation publicly available*". The new paragraph 43 and its sub-paragraphs go into detail on what this means and it is worth highlighting that this demonstrates a shift from the approach taken in version 1 (which essentially stated that if the legislation is lacking, the exporter should look at other relevant and objective factors and ensure thorough due diligence is undertaken and documented). It is thought that the EDPB received criticism that the approach in version 1 provided an "easy way out" and would have led to many exporters not undertaking a sufficiently thorough analysis of the importing laws.

  The new paragraphs highlight some interesting points:

  - According to the EDPB, while an analysis undertaken on a transfer might conclude that the laws of the importing country do meet the standards required, it may be that the practices of public authorities "*clearly indicate that they do not normally apply/comply with the legislation that governs, in principle, their activities*". If this becomes apparent, the exporter must take this into account when considering whether the transfer tool can in fact effectively protect the personal data, possibly with the implementation of supplementary measures.

  - When it is determined that relevant legislation is "*lacking*", an organisation "*cannot automatically infer from this absence*" that the transfer tool can be effectively applied. Unlike version 1, version 2 states that when this occurs, the organisation must check if there are "*indications of practices in force in the country that are incompatible with EU law and the commitments of the transfer tool*". If there are such incompatible practices, the transfer tool will not be able to effectively ensure, by itself, an essentially equivalent level of protection. In such case, supplementary measures would also have to be implemented.

  - The definition of "*problematic legislation*"[1] is introduced and if such legislation is identified, the exporter must suspend the transfer, implement supplementary measures, or continue the transfer without supplementary measures if it believes there is no reason why the problematic legislation would be applied (this must be demonstrated and documented in a thorough report). Note that the idea of problematic legislation and the effects of it being identified was included in version 1 but version 2 has clarified it slightly with the use of this definition.

- **Possible Sources of Information**. The EDPB cites several possible sources of information which should be considered in the assessment.

  - First and foremost, the EDPB notes that the importer should provide the exporter with the relevant sources and information relating to the third country in which it is established and the laws and practices in force applicable to the transfer. This seems to be support from the EDPB as to the approach taken by many organisations towards assessing international transfers: with exporters issuing Transfer Impact Assessments (or other similar documents or questionnaires) to importers requesting information regarding the local laws and practices from the importer.

- In addition to the legal framework, other sources can be referred to as long as they are "*relevant, objective, reliable, verifiable and publicly available or otherwise accessible*" to determine whether the transfer tool can be effectively applied.

- A further source was introduced (and should be welcomed) in the new Recommendations: "*documented practical experience of the importer with relevant prior instances of requests for access received from public authorities in the third country*". This permits exporters to take into account how importers have handled requests from public authorities in the past but note, experience of the importer can only be used as an **additional** source of information and as part of the "*overall assessment of the laws and practices of the third country*". Further, the EDPB confirms that the absence of prior instances of requests cannot be considered, by itself, a "*decisive factor on the effectiveness*" of the transfer tool that would permit the transfer to proceed without supplementary measures.

## III. Annex 2: Examples of Supplementary Measures

Several amendments have been made to Annex 2. However, unlike many may have hoped for, the EDPB has not substantially revised the examples of technical measures. The key points to note from the updated Annex 2 are as follows:

### *A. General updates*

- **Non-exhaustive Measures**. The EDPB reinforces the position that Annex 2 is non-exhaustive and that organisations are able to "*explore other supplementary measures*". The EDPB also notes that "*Future technological, legal or organisational developments may lead to the emergence of new supplementary measures for you to consider*". This is a useful confirmation for exporters because whilst the technical measures may not have been vastly improved in version 2, this subtle amendment to the Recommendations reiterates that the decision as to which measures should be implemented to adequately protect the personal data remains with the exporters and should not be guided entirely by the Recommendations. It also provides a nod to the possibility that certain emerging technologies may provide solutions in the future to scenarios or "Use Cases" for which the EDPB has not identified effective supplementary measures in its version 2 of the Recommendations (see further below).

### *B. Technical Measures (Paragraph 2.1 of Annex 2)*

- **Use Case 3**. Use Case 3 has been narrowed to "*Encryption of data to protect it from access by the public authorities of the third country of the importer when it transits between the exporter and its importer*". The updates to this Use Case reflect the more general amendments to the Recommendations, namely as regards the focus on public authority access and the risks highlighted by *Schrems II*.

- **Uses Cases 6 and 7**. According to the EDPB in version 2, Use Cases 6 and 7 are examples of when "*effective measures are not identified*". The wording used is slightly less restrictive than that in version 1 so may be interpreted by some as meaning effective measures are not, **at this time**, identified, **but may be identified in the relevant circumstances**. This could leave the option open for an organisation to identify such measures itself, but this remains to be seen. Moreover, the small edit seems to recognize technology is constantly evolving and as such, measures may become available in due course for certain of the use cases cited in these paragraphs of the updated version.

- **Use Case 6**. Use Case 6 in particular was the source of controversy and industry backlash in version 1. It was criticised for being too broad and potentially unworkable in its

application. Unfortunately the EDPB's amendments in version 2 do not appear to have quashed such criticisms or provided much clarity for organisations struggling to comply. Use Case 6 covers the situation where an exporter transfers or makes available personal data to a cloud service provider or other processor in order to have personal data processed according to the instructions of the exporter in a third country. Version 2 adds the following language: "*and this data is not—or cannot—be pseudonymised as described in Use Case 2 or encrypted as described in Use Case 1 because the processing requires accessing data in the clear*". The crux of the Use Case remains the same even with the additional text: if an exporter wishes to transfer personal data to a third party in a third country (where the power granted to public authorities is deemed to go beyond what is necessary and proportionate in a democratic society) and **said third party must see the data in the clear in order to be able to provide its services**, according to the EDPB, there are no supplemental measures which could ensure the data is accurately protected. This will, again, likely be criticised and hotly debated.

- **Use Case 7**. Use Case 7 covers transfers of personal data for "*shared business purposes*" where the data must be seen by the importer in the clear. One of the examples provided is sharing data between affiliates for HR purposes which is of course common practice for global companies. Use Case 7 was also the subject of similar criticism as Use Case 6 and, in response, the EDPB has sought to clarify the remit by inserting the same wording as noted above at Use Case 6. Given the nature of the transfers contemplated by Use Case 7, we suspect the EDPB will also, again, receive criticism for the arguably unworkable nature of Use Case 7 particularly in such a common scenario.

## What Next?

Over the coming weeks, we will likely see other industry experts and practitioners form views on the latest Recommendations, some positive and some negative. Data protection regulatory authorities will also undoubtedly provide their own thoughts on the Recommendations. In our view, version 2 is an improvement on version 1 of the Recommendations, particularly as it seems to focus more specifically on the issue regarding public authority access and it permits exporters to apply a more subjective approach to the assessment of whether the level of protection is essentially equivalent. However, the issues around the technical measures, most importantly Use Cases 6 and 7, cannot go unsaid, and arguably have been some of the most problematic areas for organisations looking to comply with the latest data protection requirements with minimal disruption to their continued business operations.

The updated Recommendations have come at a time where the dust is very much still settling post-adoption of the new Standard Contract Clauses for transfers of personal data to third countries (see here for more information on the new Standard Contractual Clauses). Our advice therefore is to continue moving forward with (or start) your organisation's international transfer project. As we have discussed before, reviewing and understanding your data flows is key in complying with the international data transfer requirements. The updated Recommendations will be useful in providing colour to several stages of the international transfer project, including data mapping, and in highlighting areas which are of particular importance to your organisation.

✧ ✧ ✧

*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

[1] "Problematic legislation" is defined in paragraph 43.3 as "*legislation that 1) imposes on the recipient of personal data from the European Union obligations and/or affect[s] the data transferred in a manner that may impinge on the transfer tools' contractual guarantee of an essentially equivalent level of protection and 2) does not respect the essence of the fundamental rights and freedoms recognised by the EU Charter of Fundamental Rights or exceeds what is necessary and proportionate in a democratic society to safeguard one of the important objectives as also recognised in Union or EU Member States' law, such as those listed in Article 23 (1) GDPR.*"