TECHNOLOGY AND INNOVATION

The Aftermath of Schrems II – Examining the EDPB's Draft Recommendations for International Data Transfers

November 2020

Four months on from the CJEU's landmark decision in Schrems II, the EDPB has published its draft recommendations which provide long-awaited clarity and guidance for transferring personal data outside of Europe in accordance with the GDPR.

The European Data Protection Board (the "**EDPB**") has published its draft recommendations on measures that supplement transfer tools to ensure compliance with the EU level of protection afforded to personal data (the "**Recommendations**"). The Recommendations, which can be accessed here, are open for public consultation until 21 December 2020.

The Recommendations provide much-anticipated guidance in relation to the steps that should be followed when transferring data outside of Europe and, in particular, provide examples of some of the 'supplementary measures' that may be utilised by data exporters.

In this briefing, we examine the key measures set out in the Recommendations which will be relevant to those who export personal data outside of the European Economic Area ("**EEA**") to so-called "third countries".

THE AFTERMATH OF SCHREMS II

The Court of Justice of the European Union (the "**CJEU**") in deciding case C-311/18 ("**Schrems II**") invalidated the EU-US Data Privacy Shield and, while finding that standard contractual clauses ("**SCCs**") remain valid in principle as an appropriate safeguard for international data transfers, the CJEU held that data exporters must verify on a case-by-case basis that the personal data being transferred will be adequately protected in the destination third country in line with the requirements of EU law. For further analysis on the Schrems II judgment, please see our briefing here.

The CJEU in Schrems II also stated that data exporters may implement supplementary measures that complement the appropriate safeguards used under Article 46 of the General Data Protection Regulation ("**GDPR**") in order to bring the level of protection of personal data in destination third countries up to the level required by EU law. However, the CJEU in Schrems II did not specify what would constitute such supplemental measures. Now, over four months after the Schrems II decision, the Recommendations published by the EDPB provide data exporters with a series of steps to follow and some examples of supplementary measures that could be put in place when exporting personal data outside of the EEA.

A ROADMAP FOR DATA TRANSFERS

In line with the principle of accountability in Article 5(2) GDPR, data exporters are responsible for verifying, on a case-by-case basis (and where appropriate, in collaboration with the importer in the third country) if the law or practice of the relevant third country impinges on the effectiveness of the appropriate safeguards contained in the Article 46 GDPR transfer tools. As such, the Recommendations set out a roadmap of six steps for data exporters to take when assessing the level of protection of personal data in third countries and identifying appropriate supplementary measures when needed. These steps may be summarised as follows:

1. **Step 1: Know your transfers**

   Data exporters should map all transfers of personal data to third countries in order to ensure that personal data, wherever it is processed, is afforded a level of protection that is essentially equivalent to that of the EU. Data exporters must also verify that the data transferred is adequate, relevant and limited to what is necessary in relation to the purposes for which it is transferred to and processed in the third country.

2. **Step 2: Verify the transfer tool your transfer relies on**

   Data exporters should use a transfer mechanism from those listed under Chapter V GDPR in order to ensure that the transferred personal data will have the benefit of an essentially equivalent level of protection. If the destination third country is not the subject of an adequacy decision, data exporters must rely on one of the transfer methods available under Article 46 GDPR for transfers that are regular and repetitive. SCCs are one such appropriate safeguard listed under Article 46. In situations where transfers

are occasional and non-repetitive, data exporters may be able to rely on a specific situation derogation under Article 49 GDPR.

3. **Step 3: Assess the sufficiency of the protections in the relevant third country**

   In the context of each specific transfer, data exporters should assess if anything in the law or practice of the destination third country may undermine the effectiveness of the transfer tool selected. This assessment should be primarily focused on the third country legislation that is relevant to the circumstances of the transfer and, in particular, any laws in the third country relating to public authorities' rights to access the transferred data for the purpose of surveillance. In situations where there is an absence of available legislation governing the rights of public authorities to access transferred data, the Recommendations urge data exporters who wish to proceed with the transfer to assess other relevant and objective factors (such as information obtained from reported precedents, legislation and practice relating to the relevant third country authorities), and not rely on subjective factors such as the likelihood of such public authorities' access to transferred data in a manner inconsistent with EU standards. In making these assessments, the Recommendations advise reference to the EDPB European Essential Guarantees recommendations (which can be accessed here).

   The Recommendations indicate that such powers that are "limited to what is necessary and proportionate in a democratic society" may not render the selected transfer tool ineffective for the required purpose. Data exporters should conduct this assessment with due diligence and document it thoroughly, as data exporters will be held accountable for any decisions taken to export personal data on the basis of this assessment.

4. **Step 4: If necessary, identify and adopt supplementary measures**

   To the extent that the assessment carried out at step three reveals that the third country legislation undermines the effectiveness of the transfer tool selected for the relevant transfer, data exporters should identify and adopt the supplementary measures necessary in the context of the specific transfer in order to bring the level of protection of the transferred data to a level that is essentially equivalent to the EU standard. The Recommendations set out a non-exhaustive list of examples of supplementary measures which are considered in more detail below.

5. **Step 5: Take any formal procedural steps that the adoption of the supplementary measures may require**

   The Recommendations specify the formalities that may need to be complied with depending on the selected transfer tool, and for some of them, the data exporter may need to consult the relevant competent supervisory authority. However, it is significant that where supplementary measures are to be put in place in addition to SCCs, authorisation from the competent supervisory authority is not necessary provided that the identified supplementary measures do not contradict the SCCs and are sufficient to ensure that the level of protection guaranteed by the GDPR is not undermined.

6. **Step 6: Re-evaluate the level of protection at appropriate intervals**

   Once measures have been put in place, data exporters should ensure that such measures are kept well-documented. In addition, data exporters must regularly re-evaluate the level of protection afforded to the internationally transferred data and monitor any developments that may affect such level of protection.

A CLOSER LOOK AT SUPPLEMENTARY MEASURES

The non-exhaustive list of examples of supplementary measures provided by the EDPB, which can be used to bring the level of protection of the transferred data up to the required standard, are listed in Annex 2 of the Recommendations and fall into the categories of technical, contractual and organisational measures.

While there is a range of supplementary measures to consider, the additional safeguards implemented in each case will depend on the results of the analysis and risk assessment carried out in relation to the use of the selected transfer tool and the corresponding adequacy of protection in the context of the specific transfer. The Recommendations suggest that a combination of elements from each of the categories of measures may be necessary in order to provide the level of data protection required, as one type of supplemental measure alone may not be sufficient. In a situation where there are no effective supplementary measures available, data exporters must avoid, suspend or terminate the transfer to avoid compromising the level of protection to the personal data.

1. Technical Measures

The Recommendations specify both technical measures that could potentially be effective in certain scenarios, and situations in which no technical measures could ensure an essentially equivalent level of protection. A clear pattern emerging from the Recommendations is that secure encryption or pseudonymisation of the transferred data are considered by the EDPB to be effective supplementary measures (subject to the technical conditions laid out in the Recommendations), and the use of data in the clear (i.e. unencrypted) in third countries is generally not recommended. In a situation where the data importer requires access to the transferred data in the clear to do the assigned task, and the authorities in the third country have powers to access the data beyond what is necessary and proportionate in a democratic society, the Recommendations suggest that there may be no effective technical measure available, and encryption may not remedy the situation where the data importer holds the encryption key.

2. Contractual Measures

The Recommendations call for strengthened contractual transparency and disclosure obligations, whereby the importer should be required to supplement or assist the exporter in conducting its required assessment by sharing (to the extent legally permitted) information on the laws governing government access to data in the recipient third country, along with information on the number of access requests for data received and the importer's responses. Additional proposed contractual measures include audit rights for the data exporter, contractual commitments to enable data subject rights, obligations for the data importer to notify the exporter of its inability to comply with contractual commitments and obligations to challenge government access to data through legal channels prior to disclosing it, to the extent such obligations are legally permissible under the national law of the third country.

3. Organisational Measures

The Recommendations provide examples of organisational measures that the data importer could implement such as transparency policies, data minimisation procedures, internationally recognised security standards (such as ISO standards) and policies or commitments not to transfer the data onward to other countries which do not provide essentially equivalent protections. In addition, the data importer should be obliged to document and record the disclosure requests and all relevant information thereto.

WHAT ARE THE NEXT STEPS?

The Recommendations have delivered long-awaited clarity by providing indicative and non-exhaustive measures for data exporters to consider when transferring data outside of the EEA, which will dispel some of the uncertainty that ensued in the period following the Schrems II ruling. The Recommendations have also provided guidance for transferring personal data both to the US in the absence of the EU-US Privacy Shield, and to the UK if a data adequacy decision has not been achieved once Brexit has been finalised.

At this stage, data exporters should consider the six steps outlined in the Recommendations and take the first steps in mapping and assessing their data transferring arrangements in light of this new guidance. However, as the Recommendations are open for public consultation until 21 December 2020, the guidance may be subject to change and it will be critical for data exporters to monitor relevant developments in the coming months, including updates to the draft set of new SCCs that have just been released by the European Commission (which can be accessed here).

The authors would like to thank Clíodhna Golden for her contribution to this article.

OUR TEAM

Rob Corbet
Partner
+353 1 920 1211
rob.corbet@arthurcox.com

Colin Rooney
Partner
+353 1 920 1194
colin.rooney@arthurcox.com

Olivia Mullooly
Partner
+353 1 920 1060
olivia.mullooly@arthurcox.com

Rachel Benson
Professional Support Lawyer
+353 1 920 1435
rachel.benson@arthurcox.com

Ian Duffy
Associate
+353 1 920 2035
Ian.Duffy@arthurcox.com

Ciara Anderson
Associate
+1 415 829 4247
Ciara.Anderson@arthurcox.com

Caoimhe Stafford
Associate, Techology
+353 1 920 1328
caoimhe.stafford@arthurcox.com

Eoghan Clogher
Associate
+353 1 920 1405
Eoghan.Clogher@arthurcox.com

Aoife Coll
Associate
+353 1 920 1726
aoife.coll@arthurcox.com