Schrems II – what guidance for international transfers ?

Victor Timon, Partner at Lewis Silkin, comments on the recently issued guidance from the EDPB on Schrems II

By now, we are probably all familiar with the facts of the *Schrems II* (C-311/18) verdict. However, for those who may have missed it, it can be briefly summarised as follows.

Max Schrems, a privacy activist, began a case against Facebook in 2015 when he made a complaint to the Data Protection Commissioner ('DPC'). Having successfully challenged the previous Safe Harbor regime for data transfers between the EEA and the US, Schrems turned his attention to Facebook's use of Standard Contractual Clauses ('SCCs') to transfer personal data of EU citizens to the US. In a complaint to the DPC, he argued that the protection of personal data in the US was nowhere near that of the EU, and the access to those data by various surveillance agencies was a violation of the European Charter of Human Rights. In his submission he stated that, as a result, personal data should not be transferred to the US under any circumstances. The DPC added its own concerns about the use of SCCs and the case ended up in the Court of Justice of the European Union ('CJEU'), on a referral from the Irish High Court.

Firstly, in respect of the Privacy Shield, the CJEU determined that it was impossible to conclude that it provided equivalent protection to the GDPR.

In respect of SCCs, the CJEU held that, although they remain a valid mechanism for cross-border transfers of personal data, in order to rely on SCCs, controllers (and processors) must undertake supplementary measures in the form of detailed due diligence, to show that the receiving country can guarantee the same protections for EU data subjects. Further, the CJEU also emphasised that Supervisory Authorities have the ability to audit and review SCCs, and stop data transfers where they find there is no adequate protection afforded by the receiving country.

Detailed guidance

In giving its judgement, the CJEU did not issue any guidance on what form any supplementary measure or due diligence should take. In addition, there was initially very little clarity from the European Data Protection Board ('EDPB') or the DPC for that matter. Crucially, no grace period was offered in the absence of either a Privacy Shield replacement or detailed guidance from the EDPB. So effectively data exporters were left in a limbo, scrabbling around to come up with their own justifications for data transfers outside of the EEA.

Four months later, as with buses, two recommendations from the EDPB have come along at once: one on Essential Guarantees for surveillance measures, and one on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data. The second is in the form of a consultation document, and the period for making any comments closes on 21st December 2020 (extended from the initial date of 30th November 2020). Given the detail in both, and the short consultation period, it's hard to imagine that any substantial changes will be made.

Supplemental Measures Recommendations

In the first set of recommendations on supplemental measures ('Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data') the EDPB sets out a six-step roadmap for data exporters to follow to achieve *Schrems II* compliance. The six steps are as follows:

Step 1: Know your transfers. This encourages data exporters to identify all of their current transfers to non-EEA countries. Of course, this is something that a data exporter may have been required to do in any event for maintaining its data processing records under Article 30 of the GDPR. The recommendations remind controllers and processors that permitting access from a third country also constitutes a data transfer. It also urges particular caution in respect of cloud service providers and where data may be ultimately stored.

Step 2: Identify your transfer tools. These are the various transfer mechanisms under which a data exporter may transfer personal data outside of the EEA. These include countries in re-

Recommendations on supplementary measures
www.pdp.ie/docs/10986

Recommendations on surveillance measures
www.pdp.ie/docs/10987

spect of which the EU has made an adequacy decision, as well as Article 46 mechanisms, such as SCCs, Binding Corporate Rules ('BCRs'), ad-hoc clauses and the like. Finally, there are derogations under Article 49 of the GDPR.

Step 3: Assess the effectiveness of Article 46 tools. The data exporter must assess whether the transferred personal data are afforded a level of protection in the non-EEA country that is essentially equivalent to that guaranteed in the EEA. This won't be the case if the data importer is prevented from complying with its obligations under the chosen Article 46 GDPR transfer tool due to the third country's legislation and practices. The data exporter may need to have the data importer apprise it of the laws applicable to data transfers in that country. It is also recommended that the data exporter uses other sources to re-assure itself, examples (only) of which are set out in an annex to the Recommendations.

Step 4: Adopt supplementary measures. If the conclusion reached pursuant to step 3 is that the tool chosen is by itself inadequate to provide the protection needed, then the data exporter must look at putting supplementary provisions in place. This needs to be done on a country-by-country basis to cover what is required in that particular jurisdiction. Supplementary measures may be contractual, technical or organisational in nature, or a combination of these. Annex 2 of the Recommendations sets out some examples.

According to the Recommendations, contractual measures could include provisions requiring the use of certain technical solutions, transparency (e.g. requiring the importer to report on any access requests), the right for the data exporter to conduct audits, and obligations requiring the importer to challenge any access requests.

Technical measures may include encryption (subject to certain conditions, including quality of the encryption method and the keys being retained by the data exporter or other trusted third party); pseudonymisation (conditions include that the personal data must be pseudonymised prior to export, the algorithm to re-identify individuals must be retained by the data exporter, and the data must only be used by the importer for research purposes); and split or multi-party processing (this involves splitting the data between two or more importers in different jurisdictions, where none of them actually receives any personal data, because it has been divided prior to transfer in such a way that it cannot be re-constructed by any of the importers).

Finally, organisational measures may include internal processes governing transfers (most likely in a group of companies with a presence in other non-EEA jurisdictions); documenting and recording by the importer of requests for access and reporting these to the data exporter (transparency); adoption of best practices, and involving the Data Protection Officer in all international transfers involving non-EEA countries.

Step 5: Procedural steps after identifying effective supplementary measures. After satisfying itself that there are supplementary measures that are appropriate and will work, the data exporter must then take certain steps to put these in place. They will obviously differ depending on the transfer mechanism. For example, if the data exporter is using an SCC, then it may be necessary to build new clauses into the SCC. If those provisions are likely to conflict with the standard SCC, then it would be necessary to seek a derogation from the supervisory authority under Article 46(3)(a) of the GDPR.

Step 6: Re-evaluate at appropriate intervals. Controllers have ongoing accountability obligations under Article 5(2) of the GDPR. Therefore, they will need to continually monitor any supplementary measure put in place to ensure that they remain fit for purpose.

Essential Guarantees Recommendations

To run alongside the supplemental measures recommendations, the EDPB also issued recommendations on four essential guarantees against which the surveillance laws in non-EEA countries should be assessed (Recommendations 02/2020 on the European Essential Guarantees for surveillance measures). The four essential guarantees are:

- processing should be based on clear, precise, and accessible rules;
- the processing is necessary and proportionate to the legitimate objectives being pursued;
- there should be an independent oversight mechanism; and
- effective remedies need to be available to affected data subjects.

The EDPB points out that the four essential guarantees should not be assessed independently, as they are closely interlinked. Rather they should be reviewed on an overall basis, in assessing the safeguards and remedies available to EEA data subjects in third countries.

What now?

Controllers, processors and practitioners have been crying out for guidance since the *Schrems II* decision and now they have it. It will take some time to see how all these recommendations will work and/or be effective in practice. It is not impossible to see a scenario where for certain countries contractual or organisational measures may never be enough. The challenge then will be whether the technical solutions can be implemented in practice.

It is worth noting that the European Commission has now published SCCs — both processor to controller and processor to processor versions (see pages 2 and 3). We will have to see what further impact these new documents may have on non-EEA transfers. Watch this space for further analysis.

Victor Timon
Lewis Silkin
victor.timon@lewissilkin.com