Standard Contractual Clauses Are Under Scrutiny: Keep Calm and Carry On

Avid readers of this blog will know that shortly before the new year holidays advocate general Hendrik Saugmandsgaard Øe (a.g.) gave his opinion on how European Court of Justice (**CJEU**) should deal with the second Schrems case (**Schrems II**) on international data transfers. You'll find the summary we wrote at the time here.

This is the first in a series of blogs, on different impacts the opinion might have particularly on the available data transfer mechanisms. This update focuses on how EU data controllers who are exporting personal data to countries outside the EEA (ex-EEA) should react. The updates to follow will concentrate more specifically on the Privacy Shield, Binding Corporate Rules and other lawful transfer options.

The a.g.'s Opinion

Remember that this is an advisory opinion only. The a.g. is there to advise the judges— they are free to ignore that advice. Nothing therefore will change immediately. However, the judges are much more likely to follow the a.g.'s opinion than not. It would nevertheless be prudent for any company involved in ex-EEA data transfers to consider what might happen when the judgement is given.

The opinion advises the CJEU to affirm the validity of standard contractual clauses (SCCs) as a means of legitimising transfers from the EEA to third countries. That said, the a.g. also points out that the exporting controllers have the responsibility, and the national supervisory authorities the powers, to suspend data flows that do not comply with the SCC obligations.

We can expect activist data subjects to be more aware of the possibility of regulating cross-border transfers regardless of the final outcome of this case. So now is the right time for exporters of data to consider whether they are at increased risk.

What Should Exporters Do?
Now is a good time for exporters of personal data to review their ex-EEA data flows. Why? Because the exporting data controller will be the primary target of regulatory scrutiny. Here are some suggested precautions to take:

- **Identify existing ex-EEA data transfers to non-adequate countries.** Exporters to jurisdictions without an adequacy decision, having an insufficient level of data protection in the view of the European Commission, should have a clear record of what data is sent to what recipients. This should have been part of their data mapping and record of processing exercise in preparation for GDPR already, otherwise it's now the time to complete this exercise.
- **Review the available transfer mechanisms.** Is an another way of legitimising the transfer other than through SCCs available? (a) For example: For intra-group transfers, Binding Corporate Rules might be a solution in the medium to long term. (b) Can one of the derogations in GDPR art 49 justify the transfer? For example, it may be possible to legitimise the transfer on the basis that the data subject has explicitly consented, on the basis of a contract with the data subject (for instance, a booking with an airline), or that it is a one off non-repetitive transfer and the controller has sufficient safeguards in place.

- **If SCCs are the only option, consider whether the importer can in fact comply.**
  In some instances, the exporter may be able to find no basis for the transfer other than SCCs. In that scenario, the exporter should be aware that merely having evidence of the SCCs in place, without any assurance that the importer will comply with its obligations, will not be sufficient. The controller should therefore consider:

  - Whether the importer is likely to comply with the SCCs. If the importer has a history of non-compliance, or there is any other reason to suspect that it will not comply, then there may be some risk in continuing with that importer.
  - Secondly, and a matter of greater difficulty for controllers, is the assessment of whether there are other reasons why the use of the SCCs will not protect data subjects' rights because of third-party action, for example through government surveillance activities. A serious concern in that respect is whether transfers to the United States in some circumstances may render the transfers unlawful despite the presence of SCCs. This needs to be kept under review and will to a significant extent depend on the nature of the transfer: there is a world of difference between, for example, the large scale data transfers by social networking platforms and less extensive transfers in other industries or businesses. The same might apply for other countries. Watch this space.

Needless to say all the above analysis should be carefully documented. It's worth noting that this is not simply a precaution against the consequences of any judgment from the CJEU, but is also in keeping with the general GDPR requirements of accountability and transparency.

Finally . . .
Do not panic. In light of the a.g.'s opinion, it is not expected that the SCCs will be found to be invalid. However, exporters should be aware that the mere existence of the SCCs does not relieve the exporter of their obligations to ensure that the clauses are properly complied with and that data subjects' rights are maintained.