Expert comment

Oisin Tobin is a Partner at Mason Hayes & Curran. The views expressed are his own. Oisin is a Member of the Examination Board on the Practitioner Certificate in Data Protection Programme (www.dataprotection qualification.ie)

They're finally here! On the 4th of June, the European Commission adopted Commission Implementing Decision (EU 2021/914), better known as the new Standard Contractual Clauses ('SCCs').

There's a lot that one can say about the new SCCs. This article is a brief overview of some of the key issues that are arising in practice as regards transfers of personal data from EU countries to third countries.

Key dates

When it comes to managing the new SCCs, timing is key. There are three dates which are important here, since those will drive how organisations need to approach implementation.

The first date to note is 27th June 2021 — the date that the new SCCs came into force and could be used in practice. The second key date relates to the use of the previous SCCs — old SCC decisions are being repealed with effect from 27th September 2021. Practically speaking, this means that until late September 2021, organisations have the option to either use the old SCCs or the new ones. The final date for the calendar is 27th December 2022, which is when the old SCCs cease to be valid. By this date, all organisations need to have fully transitioned to the new SCCs.

In establishing this timetable, the European Commission has given controllers and processors reasonable grace periods to facilitate an orderly transition. Work definitely needs to be done, but it can be broken into two batches.

First, between now and September 2021, all standard form agreements that rely on SCCs need to be redrafted to transition over to the new requirements. Expect a lot of frantic work over the summer, particularly for B2B businesses, as standard terms need to be rewritten.

Second, once September passes, organisations need to spend the next year looking back over all their existing agreements and contact their partners to transition those over to the new SCCs. The Commission has provided a reasonable amount of time to get this done, but the size and complexity of this task will likely depend on the quality of the contract management system that each organisation operates.

What agreements do we need to think about?

Broadly speaking, organisations need to consider three distinct sets of agreements when looking to revise their SCCs in line with the time frames discussed above.

First are customer data processing agreements ('DPAs'). These are vital for any organisation that sells a service that involves data processing. To meet customer expectations and get ahead of any issues, organisations need to start work to update such agreements as soon as they can. Getting this right is a key priority for organisations because if new agreements aren't ready by September, they may be unable to sign any new contracts with customers. Further, after September 2021, work will need to be done to transition existing customers over to the new SCCs before December 2022.

Second are vendor/supplier DPAs. These are the converse of the customer DPAs, and cover cases where an organisation has standard terms on which it buys services that involve data processing. Again, to avoid any interruption in an organisation's ability to procure services on its terms, such template agreements should be updated by September, and then work should be done to transition vendors over to new SCCs in the course of the next year.

Finally, there are intra-group agreements, which deal with data sharing between affiliates (particularly Irish/ EU companies and their US affiliates). Assuming that these aren't amended, they can be left as is until December 2022.

However, organisations should note that if any new affiliates are added after 27th September, the new SCCs will need to be used. For larger groups, this could cause a headache, since transfers to different affiliates could be based on different sets of SCCs.

For groups with an evolving structure, I would recommend transitioning to new SCCs fairly promptly, notwithstanding the grace period.

Can we use Irish law?

Yes!

The new SCCs generally require that governing law allows for third party beneficiary rights (to ensure that data subjects can bring claims where appropriate).

One of the key distinctions between Irish and UK law, and indeed the usual position in the US, is that Irish contract law is quite restrictive when it comes to third party beneficiary rights.

This led to suggestions from some quarters that Irish law could not be used. This possibility was not received well by the Irish legal profession, which was working on various types of structures to address any issues lest Irish organisations find themselves unable to contract under their local law.

Helpfully, the issue was resolved on 24th June 2021 with the publication of the European Union (Enforcement of Data Subjects' Rights on Transfer of Personal Data Outside the European Union) Regulations 2021.

These regulations amend the Data Protection Act 2018 to expressly provide for third party beneficiary rights when it comes to the SCCs. There was a similar provision in the old Data Protection Acts 1988 and 2003, though it was unclear as to whether it survived the adoption of the Data Protection Act 2018.

In any event, Irish law can be used, and any debate as to whether Irish law would have been appropriate in the absence of the new Regulations is (thankfully) academic.

See the article on pages 4-5 of this edition for in depth commentary on this topic.

What if I'm an Irish processor that services a non-EU customer?

One of the more head scratching issues that comes up with international data transfers is the situation where a non-EU company chooses to avail of services provided by a processor in the EU. Suppose, for example, a construction company in Dubai uses HR software sold from, and hosted in, Dublin. The original transfer of the data from Dubai to Dublin would not give rise to any issues under the GDPR's transfer rules, but the transfer of that data back from Dublin to Dubai could potentially comprise a processor to controller transfer. There was no clear way to legalise such a transfer given that the existing SCCs focused on controller to processor transfers.

The new SCCs deal with this by creating specific (lightweight) provisions to cover the processor to controller situation. This seems like a reasonable attempt by the Commission to plug a perceived gap in the framework while, at the same time, not making European data processors uncompetitive by requiring that they impose onerous terms when dealing with non-European controllers. However, EU processors that service non-EU controllers will now need to adopt SCCs for the first time.

Do we still need to transfer impact assessments?

The *Schrems II* (C-311/18) judgment set out the Court of Justice of the EU's expectation that organisations transferring data in reliance on SCCs perform diligence on the recipient jurisdiction to ensure that data transferred on the basis of SCCs would enjoy sufficient protection.

These requirements can be quite onerous for organisations, particularly SMEs, given that they effectively require doing a legal analysis of the laws and practices of a foreign state.

The new SCCs codify this requirement. Under Clause 14, both parties are required to warrant that they believe that the 'laws and practices' in the recipient jurisdiction respect the essence of fundamental rights and freedoms, and do not go beyond what is necessary and proportionate in a democratic society to safeguard certain public interests. As part of this warranty, the parties need to assess the specific circumstances of the transfers, the laws and practices of the recipient jurisdiction and any supplemental safeguards that have been put in place.

The language in the SCCs implies that a transfer impact assessment ought to be conducted before SCCs are signed. However, the actual factors that the Commission says ought to be considered are helpful and represent a liberalisation of the position from that which appears to have been adopted by the European Data Protection Board.

In particular, the Commission stressed that both laws and practices can be considered, and the circumstances of the transfer need to be considered. This approach implicitly rejects the idea that entire jurisdictions (notably the US) can be blacklisted because of concerns about how certain of their laws could be applied. It's clear that a nuanced risk assessment, looking both at the laws on the books and what the practical risks are, need to take place. While this may be burdensome, it may ultimately provide some comfort to many organisations which can document why the risks applying to their transfer of data outside of the EU is low.

Oisin is leading a Workshop on 'Apps — Unique and Challenging Compliance Issues' at the 16th Annual Data Protection Conference taking place in central Dublin (and by livestream for virtual attendees) on 12th November 2021. See www.pdp.ie/conferences for further information.

Oisin Tobin
Mason Hayes & Curran
otobin@mhc.ie