Guest columnist

OLIVIA WHITCROFT

"No sooner do you put down your figurative pen than someone goes and changes the rules"

If any of your data moves overseas, you need to keep on top of international data transfer rules – but that's easier said than done

It's tricky writing articles about international data transfers. No sooner do you put down your figurative pen than someone goes and changes the rules.

When I wrote my article on this topic last year (*see issue 322, p116*), there was a constant stream of changes, and I had to plead with *PC Pro*'s editor to publish it quickly so I could stop writing and take a rest. It seems I've now rested for 11 months, which means that much has happened.

First, the EU finalised its much-needed new standard contractual clauses (SCCs) for transfers of personal data out of the EU. Then it approved the UK data protection regime as "adequate", a whisker before the deadline of the end of June 2021.

Fresh with its adequacy decision from the EU, the UK started pumping out consultations on ways to change UK data protection law and guidance, and depart from EU law. International transfer issues formed a big part of these consultations. And the hot news is that the new UK International Data Transfer Agreement came into force on 21 March 2022.

EU data transfer clauses

Finalisation of new EU SCCs for cross-border transfers came on 4 June 2021. Use of SCCs is the most popular option for sending personal data from the EU to a country not deemed to have adequate data protection laws. EU organisations started updating their transfer contracts, with a deadline of 27 September 2021 to stop using old SCCs for new data transfers.

However, the UK didn't permit use of the new SCCs for transfers of data from the UK. British organisations were temporarily left with very limited ways to legitimise data transfers other than to use the increasingly out-of-date EU SCCs approved under the 1995 EU Data Protection Directive. Global organisations, including big tech companies transferring data to the US, needed to use different SCCs for data travelling from the EU to those used for data travelling from the UK. This was undoubtedly a good exercise in mapping out data flows and finding tailored solutions, but it carried with it the knowledge that the UK approach was soon to change again.

Olivia is principal of the law firm OBEP, which specialises in technology contracts, IP and data protection
@ObepOlivia

"Data subjects and the ICO may bring claims against parties for breach of the terms"

Adequacy for the UK

The EU Commission's adequacy decision for the UK arrived on 28 June 2021. This was just in time, as 30 June was the final day of the temporary "bridge" allowing personal data to flow between the EU and the UK without additional safeguards. It was a huge relief for many. While the ICO had recommended that organisations put in place a backup plan before the end of April 2021, a lot of organisations I spoke with were putting faith in the adequacy decision coming through.

But there are limitations on the decision. First, it excludes data transferred to the UK for immigration control. This was one of the sticking points in the debate over whether the UK would achieve adequacy, as UK law exempts organisations from providing certain data protection rights in this context. The decision also has an expiry date of 27 June 2025, and could be repealed before then if the UK's revisions to data protection law depart too far from EU law; this is a risk with the proposals I discuss later.

UK data transfer agreement

The new UK International Data Transfer Agreement (IDTA) prepared by the Information Commissioner's Office (ICO) came into force on 21 March 2022. UK organisations can now escape the clutches of the EU's old SCCs. However, if you really want to, use of the old clauses is still permitted for contracts concluded before 21 September 2022.

As an alternative, the ICO has produced an Addendum to the new EU SCCs. This makes them suitable for transfers from the UK (rather than the EU) and to reflect requirements of UK law (rather than EU law). The Addendum may be useful for global organisations looking for a consistent set of clauses for transfers from the EU and the UK, or those already familiar with using EU SCCs who don't want to deal with yet more new provisions. On the other hand, the new IDTA is a standalone document, has more of a UK style, and may be easier to understand and put into practice.

I shall now attempt to take you on a speed tour of the IDTA. Organisations using the IDTA need to understand their data flows (which was a focus of my article last year). Full details of the parties and transfers must be included in tables at the top. This includes descriptions of data types, data subjects, security requirements and any extra protections arising from transfer risk assessments.

The terms cater for different types of transfer (as do the new EU SCCs), including controller to controller, controller to processor, processor to sub-processor, and processor to

RIGHT Navigating international data-transfer rules can be a minefield

ABOVE **The UK has recently introduced new rules for data transfers**

controller (though the latter may not always be a restricted transfer, as I raise below). There are also provisions that apply to all transfers, and some that apply only to specified types.

The IDTA envisages separate "Linked Agreements", including data sharing or data processing agreements. This means that the transfer agreement can focus on transfer issues, and does not need to address all data protection issues associated with the parties' relationship, such as requirements under Article 28(3) UK GDPR for contracts with a processor.

The majority of the clauses are mandatory, so organisations using the IDTA should generally use them as they are. However, practical changes are permitted, such as making the agreement multi-party, where needed.

To assist in protecting data protection rights, data subjects and the ICO may bring claims against the parties for breach of the terms.

UK consultations

Alongside its consultation on the IDTA in August 2021, the ICO consulted on updates to its international data transfer guidance, together with a transfer risk assessment and tool. The UK government, in September 2021, also published a paper called *Data: A new direction* to consult on reforms to data protection legislation. Chapter 3 of this discusses reducing barriers to data flows.

I have pulled out some of the proposals that cover problems I often ponder. First, the UK government recognises that assessing data transfer risks is not an easy exercise for everyone. Since the Schrems II court decision in July 2020, all organisations, large and small, have been required to do just this. I advise several small companies using cloud-based technology, which involves data transfers outside the UK. When I explain to my clients that they must research and assess the risks of such transfers, and then discuss this with giants such as Amazon, Google and Microsoft, I receive glazed and confused looks that tell me I'm crazy.

Now, of course, just because an organisation is small doesn't mean there are no risks with its data processing and transfer activities. So dispensing altogether with risk assessments would not be a good solution. But the government says it intends to apply proportionality in developing transfer mechanisms, and to provide more practical support for organisations in assessing risks.

Another legislative proposal that my clients may welcome is exempting "reverse transfers" from the rules. Let's say a UK company is providing add-on services to customers of an Australian company. The Australian company sends customer details to the UK company (in line with Australian data transfer rules). The UK company then needs to confirm some of these details, and sends them back to the Australian company. Currently, UK data transfer rules would kick in, creating an additional burden, when this is information that the Australian company already holds and has sent to the UK in the first place. Under the proposals, the transfer rules would not capture sending data back to the originating entity.

On a similar note, the ICO is proposing that where a UK processor has been appointed by a controller outside the UK (which is not otherwise subject to UK data protection law), the transfer of data from the processor to the controller (on the controller's instructions) would not be a restricted transfer. For example, if a US company appoints a UK company to manage payroll on its behalf, the UK company would not then need to apply UK transfer rules each time payslips are sent over to the US company. This would also assist UK processors to stay competitive when pitching for work against providers local to the controller.

The ICO's guidance, and a point on which it consulted, is that transfers are only restricted between legal entities. This includes transfers to group entities, but not to your own staff in another country. I would like to see more clarity on whether this also excludes transfers to the data subjects themselves. Another proposal is that a restricted transfer is made by the party authorising it, which does not necessarily follow the data flow. This could ease (though not erase) the burden on small companies raised above; if a UK company uses a UK cloud provider that appoints a sub-processor in the US, the cloud provider makes the restricted transfer. My view is that this should also work the other way around: if the UK company directs the cloud provider to transfer data directly to an overseas recipient, the UK company makes the restricted transfer.

"Dispensing altogether with risk assessments would not be a good solution"

The government is also proposing to allow repetitive use of derogations to transfer rules. Even though it's generally accepted that use of derogations should be a last resort, sometimes the situation boils down to them being the best option. But UK GDPR recitals indicate that some are only available where the transfer is "occasional". For example, derogation for transfers that are necessary for performing a contract with the data subject could not currently be used if the transfers are repetitive.

A final point is that the government refers to an "ambitious programme of adequacy assessments". Since Brexit, the jurisdictions that the UK deems adequate mirror those of the EU's adequacy decisions, with the addition of Gibraltar (which isn't covered by the EU's adequacy decision for the UK).

On the face of it, these proposals seem sensible and helpful for many UK organisations. But if the UK creeps away from EU data protection law, this leads to the question of whether the UK's regime will continue to be deemed adequate by the EU.

Both consultations ended in 2021. As I write this article, the ICO and government are building up my excitement with signals that full outcomes will be published soon. I'll put down my pen now before something else happens.

POSTSCRIPT: Something else has happened! At the end of March, the US and the EU Commission agreed, in principle, a new framework for transatlantic data flows (to replace the previous Privacy Shield). The UK may not be jumping on board, though, as it's exploring its own data adequacy partnership with the US. Did I mention that it's tricky writing articles about data transfers?

olivia.whitcroft@obep.uk