Guest columnist

OLIVIA WHITCROFT

"You need to know where your data is going to identify compliance and risk issues

Data protection expert and lawyer Olivia Whitcroft explains the impact of Brexit and Schrems II on tech contracts and what action you need to take

Last month, I was reviewing the relationship between a UK client and a US technology provider who stored personal data on behalf of my client. The provider's terms stated that it "complies with the EU-US Privacy Shield Framework" for transfers of personal data from the EU to the US. I had a couple of problems with that. Firstly, the UK is no longer within the EU, so a commitment to comply with the Privacy Shield for transfers from the EU doesn't help. Secondly, the EU-US Privacy Shield is no longer valid as a mechanism to permit transfers of data from the EU to the US.

I started writing a long piece of advice to my client explaining the problems with data transfers to the US, the lack of ideal solutions and the potential need for creativity in addressing the issue. Then I discovered that the provider's data centres were in the UK, so there was no need to worry about this after all, and the Privacy Shield reference was somewhat of a red herring. I moved on to the next burning issue.

This experience highlights two important steps for any data transfer review: mapping out your dataflows and tailoring your solutions to the context. You need to know where your data is going to identify compliance and risk issues. And there's no one-size-fits-all approach to addressing those issues.

Transfers take centre stage

The topic of international data transfers has been brought to centre stage in the data protection world following Schrems II and Brexit.

In July 2020, the Schrems II decision of the Court of Justice of the European Union (Case C-311/18) determined that the much-used EU-US Privacy Shield would no longer be a valid way of permitting transfers of personal data from the EU to the US. Transfers commonly take place where cloud providers, data centres or other service providers are located within the US. Previously, if the transferee was certified with the Privacy Shield, this met the international data transfer requirements of the EU GDPR.

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

"The Brexit agreement created a 'bridge' lasting four to six months"

It had also been envisaged that, at the end of the Brexit transition period, certified entities could update their Privacy Shield arrangements to include transfers from the UK (under the UK GDPR). So, the Schrems II decision shook up data transfers for EU and UK organisations, and their US transferees.

The Schrems II decision didn't stop at the Privacy Shield, nor at transfers to the US. The Court also looked at use of standard contractual clauses (SCCs). With no Privacy Shield, SCCs would be the only viable option for many transfers to the US and were already the prevalent option for transfers to other countries not approved as "adequate". Schrems II confirmed that use of SCCs was not quite as simple as just signing the clauses and ticking the compliance box. For each transfer, organisations are also required to do an assessment of the overall risks and consider additional safeguards to protect the data and individuals' rights. These should take into account the legal regime of the country of transfer and the ability of the parties to comply with the clauses. This isn't exactly an easy exercise!

To add to this, the SCCs currently approved by the EU and the UK are not up to date with the GDPR, and do not cater for all common transfer scenarios. These concerns may be addressed by new sets of clauses. The EU published draft new SCCs at the end of last year and the UK ICO intends to prepare its own set for transfers from the UK. I'm writing this article in mid-May and the new EU SCCs are expected to be approved within weeks; the UK SCCs are then due to be published for consultation this summer.

The Brexit factor

What about Brexit? Agreement was, of course, saved to the last minute, so we weren't sure about 2021 data transfers to the UK until we were eating our Christmas turkey the week before. The agreement created a "bridge" lasting four to six months, during which personal data could continue to flow from the European Economic Area (EEA) to the UK without additional restrictions. During this period, the UK has been working towards obtaining an "adequacy" decision, under which the EU Commission would recognise the UK as having an adequate data protection regime and continue to allow data transfers to the UK. This

RIGHT The Schrems II decision has shaken up transfers between the UK, EU and US

draft adequacy decision has been published and is expected to be adopted before the end of June.

Nevertheless, Brexit has brought complexities to data transfers. The UK and the EU now have two different data protection regimes: the UK GDPR and the EU GDPR. The UK needs to make its own arrangements with other jurisdictions to facilitate dataflows, and transfers of personal data to and from the UK need to be assessed separately to those to and from the EEA.

Whilst the UK and EU regimes are currently similar, there's potential for them to diverge away from each other. Indeed, the UK government has declared its intention to enable cross-border flows beyond those recognised as adequate by the EU. The EU is wary of this, and the draft UK adequacy decision contains a four-year expiration date in order to reassess UK law at this stage. The European Data Protection Board (EDPB) has also recommended earlier suspension or repealing of the decision if the UK doesn't continue to ensure an adequate level of protection for personal data.

What should you be doing?

All this matters because breaching data transfer requirements may result in legal and regulatory action. In light of Schrems II, national data protection authorities have been taking action against organisations for failing to carry out proper risk assessments and determine what additional data protection measures are needed prior to a transfer. A German data protection authority found against a company that uploaded email addresses to Mailchimp (in the US) to send newsletters, and the Portuguese data protection authority ordered the Instituto Nacional de Estatística to stop using the services of Cloudflare (in the US) to process data relating to its 2021 census.

As I mentioned at the start, data mapping is key to understanding the proposed transfers. The risks can then be assessed, and solutions tailored to address those risks and to ensure compliance. A formal data protection impact assessment may be a useful way to do this (and is required for processing activities that are likely to carry a high risk). Assessments should also be regularly reviewed during the lifetime of the processing activities. Following Schrems II, the EDPB has published *Recommendations 01/2020 on measures that supplement transfer tools* [such as SCCs] *to ensure compliance with the EU level of protection of personal data*, which may assist with these assessments.

Routine approaches to data transfers may require significant changes to incorporate these steps. Companies I speak to have commonly had a pure compliance approach to data transfers – ticking off the relevant transfer mechanism under Articles 45 to 49 GDPR. I've been helping clients to adapt to examining the detail of the dataflows and risks specific to a particular transfer, and then deciding on suitable tailored solutions. In some cases, we have reached a surprising conclusion, for example that a derogation to the rules (such as explicit consent), coupled with bespoke contractual terms, may be more appropriate than putting in place SCCs.

Given the complexities surrounding international data transfer assessments, the option not to make the transfer at all is also being considered more frequently. I worked with a client on a due diligence questionnaire to send to a US company, which was to provide software and infrastructure services. My client had requested data centres within the EU. However, following completion of the questionnaire, we discovered that the support services were provided from the US and that this may, on occasion, involve access to personal data. This led to us discussing ways in which support could be carried out elsewhere, or without access to personal data.

As well as reviewing new data transfers, existing arrangements may need to be updated. I recently reviewed a data sharing agreement between a UK and an EU entity. It was drafted several years ago, when international data transfer issues only arose should either party appoint a service provider outside the EEA. Now, the core purpose of the contract, which was sharing personal data between the two companies, gave rise to international data transfers – from the UK to the EU and vice versa. The parties were now also subject to different data protection regimes that may vary during the lifetime of the relationship. The existing terms between them no longer worked, so we updated them to recognise the more complex data transfer concerns.

ABOVE **The EU could repeal the adequacy decision if standards aren't maintained**

"Routine approaches to data transfers may require significant changes"

BELOW **National data protection authorities have been finding against organisations**

Rules will continue to change

Things are moving on even as I write. As I raised above, we're expecting the EU to adopt an "adequacy" decision for the UK imminently. If this doesn't arrive before the end of June (or if it is subsequently repealed), additional measures such as SCCs may be required for data transfers from the EEA to the UK, and potentially also from other jurisdictions recognised as "adequate" by the EU. The UK government is meanwhile pursuing its agenda to remove barriers to dataflows to and from other countries, and the ICO is preparing its own new SCCs. There are talks of a future replacement for the Privacy Shield for transfers to the US. Who knows, maybe we shall also see the UK rejoin the EU?

olivia.whitcroft@obep.uk