The future of international data transfers

Eduardo Ustaran, Partner at Hogan Lovells, examines the future of international data transfers

With the current focus on the General Data Protection Regulation ('GDPR') coming into effect, one could (almost) be forgiven for forgetting about the question of international data flows. However, given the political and legal developments currently affecting the future of international data transfers, that would be a very serious strategic mistake. Legitimising data globalisation remains a top business priority in our uber-digitised world. Coming of age of cloud-based services, the continuous advance of mobile communications and the push by developed and developing countries to reach a global market have made international data transfers more essential than ever. At the same time, the level of regulation affecting those transfers is becoming more impenetrable and politically charged.

Against this background, what are the issues that need to be taken into account to develop a solid global data flows legal strategy?

The constant scrutiny affecting the Privacy Shield

The EU-US Privacy Shield has never had a smooth ride. After nearly two years in operation, the criticism that this framework receives from all angles is still relentless. Fairly or unfairly, the abrupt end of the original Safe Harbor framework that led to the creation of the Privacy Shield still casts a shadow over its robustness. The fact that both the European Commission and the Article 29 Working Party — now replaced by the European Data Protection Board ('EDPB') — have been prepared to see the glass half full has not provided the necessary degree of confidence.

In June 2018, the European Parliament delivered yet another blow to the credibility of the Privacy Shield as a suitable framework for the protection of European personal data handled in the US. In a dramatic statement, the Parliament's Civil Liberties ('LIBE') Committee called on the European Commission to suspend the EU-US Privacy Shield due to its alleged failure to provide enough data protection for EU citizens.

According to the LIBE Committee, the framework should be suspended unless the US complies with it by 1st September 2018, and remain suspended until the US authorities comply with its terms in full.

In particular, the LIBE Committee has called on the US authorities to act upon the revelations regarding the use of Facebook profile data for political targeting and to remove companies that have misused personal data from the Privacy Shield list. EU data protection authorities are also called to investigate such cases, and to suspend or ban data transfers under the Privacy Shield. In addition, Members of the European Parliament are also concerned about the adoption in the US of the so-called CLOUD Act, which is aimed at granting law enforcement authorities access to personal data across borders.

When coupled with the ongoing political uncertainties surrounding the US government, it is understandable that the Privacy Shield continues to be under scrutiny. In this respect, it will be crucial to see the outcome of the 2nd annual review by the European Commission and the EDPB, due in the Autumn of 2018, in order to assess whether the Privacy Shield is a sufficiently reliable mechanism to legitimise data transfers to the US.

Model clauses to be examined by the EU's top court

Next year, the Model Clauses adopted by the European Commission — their first version was 17 years ago — for the purposes of legitimising international data transfers through a contractual mechanism will face the same judgement mechanism that brought down Safe Harbor. Not the most promising of prospects. The route to the Court of Justice of the European Union ('CJEU') is a familiar one. Activist Max Schrems prompted the Irish Data Protection Commissioner to investigate the way in which Facebook legitimises its personal data flows between Europe and the US, and in light of the CJEU Safe Harbor decision, the Commissioner decided to put the model clauses to the test.

After a long and intricate judicial process, in April 2018, the High Court of Ireland decided to progress the Commissioner's request and referred a number of critical questions about the validity of the current model clauses to

(Continued on page 8)

Eduardo will be speaking on International Data Transfers at the 17th Annual Data Protection Compliance Conference taking place in London on 11th and 12th October 2018.

See www.pdpconferences.com for further details about the event.

(Continued from page 7)

the CJEU. The extremely detailed nature of the questions posed to the EU's top court reveals the complexity of the matter. The core aspects affecting the validity of the Model Clauses that the CJEU is being asked to decide on are as follows:

- does EU law, including the Charter of Fundamental Rights of the EU ('the Charter'), even apply to the processing of personal data for national security purposes;
- aside from the law as such, do the relevant administrative, regulatory and compliance practices and safeguards, as well as other practical procedures matter in order to assess the level of data protection of a country outside the EU;
- does US law allow mass indiscriminate processing of personal data in breach of the rights of Articles 7 and 8 of the Charter;
- does US law respect the essence of an individual's right to a judicial remedy for breaches of privacy and are any limitations proportionate and necessary;
- can the Model Clauses provide an adequate level of protection for international data transfers irrespective of the level of data protection of the importer's country;
- if the level of surveillance in that third country is incompatible with EU law standards, should a data protection authority simply suspend the data flows to that country; and
- does the Privacy Shield ombudsperson amount to an effective remedy for individuals when their data is transferred under the Model Clauses?

These are all very technical legal questions that will require a detailed analysis by the CJEU, but they clearly highlight the perceived shortcomings of the existing contractual model.

Given the fate of the original Safe Harbor, the fact that the CJEU has been tasked with determining the validity of the existing Model Clauses is a serious concern. As a result, further work by the European Commission on refining and strengthening the contractual approach to legitimising international data transfers is to be expected in the coming months.

> ***"Fairly or unfairly, the abrupt end of the original Safe Harbor framework that led to the creation of the Privacy Shield still casts a shadow over its robustness."***

BCRs to the rescue

Partly by design, partly by elimination, Binding Corporate Rules ('BCRs') have emerged as the go-to solution for any organisation seeking a robust yet flexible approach to legitimising global data flows.

BCRs top the list of options available in the GDPR for this purpose, and regulators appear sensitive to this situation. For this reason, it is probably not a coincidence that of all of the Article 29 Working Party guidance documents expressly endorsed by the EDPB on the day of the coming into effect of the GDPR (a list is available from www.pdpjournals.com/docs/887923), five of them concern BCRs, namely:

- Working Document Setting Forth a Co-Operation Procedure for the approval of 'Binding Corporate Rules' for controllers and processors under the GDPR ('WP 263');
- Recommendation on the Standard Application for Approval of Controller Binding Corporate Rules for the Transfer of Personal Data ('WP 264');
- Recommendation on the Standard Application form for Approval of Processor Binding Corporate Rules for the Transfer of Personal Data ('WP 265');
- Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules ('WP 256'); and
- Working Document setting up a table with the elements and principles to be found in Processor Binding Corporate Rules ('WP 257').

In other words, the loud and clear message from the regulators is that they are prepared to facilitate and support the necessary investment that is required to adopt and implement BCRs. In truth, they will also need to walk the walk and ensure that their level of engagement as part of the authorisation process is sufficiently active to make it all worthwhile, but the signs are good.

The UK has a plan

Speaking of countries outside the EU, the UK will become one in a few months' time. One of the implications of Brexit is that transfers of personal data from the EU to the UK will also need to be legitimised. The UK government is well aware of this fact, and has made it very clear that one of its priorities following Brexit is to ensure the free movement of personal data with the EU. To that effect, the UK has embraced the GDPR as its own data protection framework, and appears confident that an adequacy finding will be forthcoming.

In fact, in a bold move, the UK government has issued a concrete proposal for a special agreement with the EU aimed at maintaining the free unhindered flow of personal data between the EU and the UK. This agreement is meant to build on a standard adequacy arrangement, but its objectives go significantly further. As stated in the proposed framework for the UK-EU partnership on data protection, the new agreement would achieve the following:

- ensuring the same high standards of protection for personal data flows between the UK and the EU;
- providing for continued regulatory cooperation and consistent enforcement through an appropriate ongoing role for the Information Commissioner's Office ('ICO') on

the EDPB; and

- ensuring that UK businesses and consumers are effectively represented under the EU's 'One Stop Shop' mechanism for resolving data protection disputes in relation to cross-border data processing activities.

This would provide an optimum outcome in the context of EU-UK data transfers.

From an EU law perspective, the European Commission would still need to issue an adequacy decision as envisaged by Article 45 of the GDPR, confirming that the UK ensures an adequate level of data protection. As part of this process, the European Commission would need to carry out a proper legal assessment taking into account the rule of law, including the respect for human rights and, crucially, the controls on access to personal data by the state.

In principle, this should be within reach of the UK given that the GDPR is already part of the UK legal framework, but the UK will still have to demonstrate its democratic credentials. Ultimately, the UK will need to convince the European Commission that any investigatory powers involving the collection and use of personal data are compatible with the privacy rights of individuals as understood by EU law.

Brexit politics aside, it will certainly be in everyone's best interests if such an agreement is reached as a way of guaranteeing not only the free flow of data between the EU and the UK, but the protection of such data across jurisdictions.

Eduardo Ustaran
Hogan Lovells
eduardo.ustaran@hoganlovells.com