INTERNATIONAL DATA TRANSFERS: THE EVOLVING LANDSCAPE

Authors: John Magee, Partner at DLA Piper and a member of the ACOI Data Protection & Information Security Working Group. James Clark & Eilís McDonald are members of global law firm DLA Piper's data protection, privacy & security team.

> *"In July, the European Data Protection Board (EDPB), issued FAQs regarding the Schrems II decision. Importantly for organisations, there is no grace period for compliance."*

2020 has been a turbulent year in many ways – one topic that will not have escaped the attention of compliance practitioners is that of international data transfers.

The invalidation by the Court of Justice of the European Union (CJEU) of the EU-US Privacy Shield in the Schrems II decision in July has created significant uncertainty for many companies and their compliance teams. While the CJEU did not invalidate standard contractual clauses (SCCs), a more widely used transfer mechanism, the CJEU found that businesses need to conduct a case-by-case assessment to verify whether the conditions of transfers made pursuant to standard contractual clauses (including the legal regime in the destination country) offer appropriate safeguards to individuals' personal data.

At the same time, compliance teams are facing significant uncertainty due to the impact of Brexit on their data protection arrangements, a situation now complicated further by the Schrems II decision and ongoing uncertainty around the EU-UK trade negotiations and an adequacy decision for the UK.

Given the increasing importance of data to organisations from all sectors, finding practical solutions to these issues is becoming increasingly important for compliance practitioners.

Schrems II

As well as invalidating the EU-US Privacy Shield as a GDPR transfer mechanism, the CJEU found that SCCs continue to be a valid mechanism for transferring personal data to countries outside the EEA but subject to important limitations. SCCs may not always constitute a sufficient means of ensuring, in practice, the effective protection of personal data transferred to a third country, in particular where the law of that third country allows its public authorities to interfere with the rights of the data subjects to which that data relates. The judgment requires businesses, and ultimately EU data protection regulators, to suspend or prohibit transfers where such appropriate safeguards cannot be provided.

Regulatory Response

In July, the European Data Protection Board (EDPB), issued FAQs regarding the Schrems II decision. Importantly for organisations, there is no grace period for compliance. Transfers relying on Privacy Shield must immediately stop. Those relying on SCCs must be assessed and supplemental measures to safeguard the personal data which are subject to the transfer should be implemented, where required. There has been no concrete guidance as to what these 'supplemental measures' might look like; however, further guidance is expected by the end of 2020. The Data Protection Commission (DPC) issued a statement in the immediate aftermath of the decision noting that "it is clear that, in practice, the application of the SCCs transfer mechanism to transfers of personal data to the United States is now questionable". Meanwhile other European regulators (notably the Data Protection Authority of the German federal state of Baden-Württemberg) have begun to comment on contractual measures

which could be implemented, placing obligations on data importers and exporters, however no single consistent approach has emerged post Schrems II.

Recent Developments

In a recent development closer to home, Max Schrems has applied for and been granted permission to raise a judicial review against the DPC in Ireland. Schrems alleges the DPC has not yet made a decision on his original complaint from 2013 and that the DPC withheld information regarding alternative transfer mechanisms used by Facebook for US transfers. This is the second judicial review which has been granted in connection with this case since July: Facebook has been allowed to continue its transfers to the US on a temporary basis following a preliminary suspension order – issued by the DPC following the judgment – being stayed.

Practical Steps

Against this noisy backdrop, organisations could be forgiven for thinking that solutions remain elusive. In fact, the CJEU has been relatively clear regarding the analysis that needs to be performed. In what are now being termed "transfer impact assessments" or "TIAs", data exporters are looking at the following steps:

1. Analyse data flows which involve transfers of personal data outside the EEA and determine which transfer mechanism is being used. Existing compliance controls can be used to identify transfers, such as Article 30 records of processing activities (RoPA), data protection impact assessments (DPIAs) and other data mapping controls.

2. For US transfers relying upon Privacy Shield, an alternative transfer mechanism must be found as a priority.

3. To the extent a business is currently using, or considering using (as an alternative to Privacy Shield), SCCs for transfers to any third country, it must assess the level of appropriate safeguards provided by that transfer to determine whether SCCs are a suitable mechanism. A TIA will typically involve an assessment of the following criteria:

a. the legal regime in the destination country including (i) the strength of regulation of data privacy; (ii) regulation of public authority access to private data; and (iii) rights of redress for affected data subjects;

b. additional safeguards or supplementary measures that may mitigate or exacerbate privacy risks, such as (i) provisions in the contract between exporter and importer that affect disclosure; and (ii) technical and organisational measures implemented by the exporter or importer which impact the privacy protection; and

c. the real-life risks of the transfer, within the context of the sector / industry and other relevant factors including the identity of the data subjects and the categories of data being transferred.

Brexit

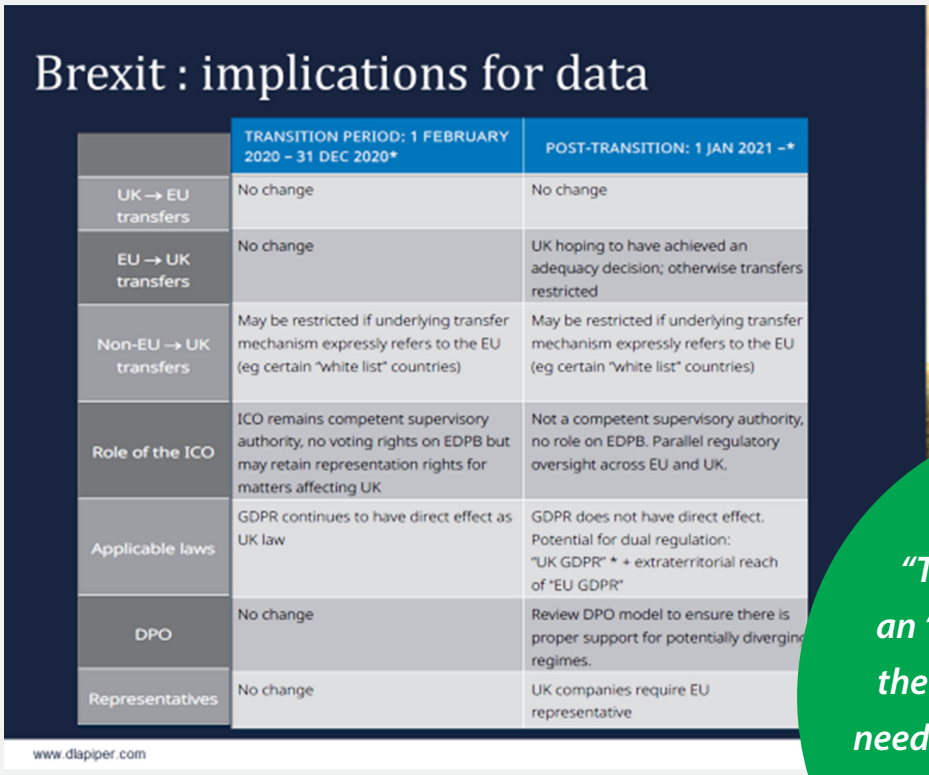
As the clock ticks down towards 1 January 2021, compliance officers are dusting down no-deal Brexit plans drawn up in the run up to cliff-edge no-deal eventualities in March and October 2019.

Impact on Data Transfers

While the UK Government has stipulated that – at least in the immediate term - it does not intend to apply any restrictions on transfers of personal data from the UK to the EEA, the EU has not granted similar modification in respect of transfers to the UK. Accordingly, compliance teams are formulating plans on the basis that transfers of personal data from the EEA to the UK will be restricted from 1 January. This will have a major impact on any organisation that routinely transfers personal data from the EEA to the UK. The situation will have a particular impact on the island of Ireland, where transfers of data to Northern Ireland will be affected.

SCCs as a Solution

Impacted organisations will need to adopt specific legal safeguards to support the lawful transfer of personal data to the UK. For many organisations the best approach will be to adopt SCCs; however, following Schrems II their usage is more complex, coming as it does with the requirement to carry out a TIA. It is also important to be aware that SCCs cannot be used to safeguard all transfers – for example SCCs do not exist for transfers between an EU-based processor and a UK-based controller (a common scenario given the number of cloud service providers who have data centres in Ireland), nor for transfers on an inter-company basis (such as between a parent and a branch entity). This is a known area of risk to regulators, which impacted organisations may decide to 'risk manage' where data repatriation is not a realistic option.



"The UK hopes to secure an 'adequacy' finding from the EU that will obviate the need for SCCs or other specific safeguards between the UK and the EU."

Adequacy Decision

The UK hopes to secure an 'adequacy' finding from the EU that will obviate the need for SCCs or other specific safeguards between the UK and the EU. The EU has started to work on this, and it is possible it will form part of the hoped-for EU-UK trade deal, an announcement on which is expected very shortly.

Dual Regulatory Exposure

If an organisation has processing activities that span the EU and UK, following Brexit it is likely that the organisation will be subject to regulatory responsibilities under both the EU and UK versions of the GDPR. Depending on the circumstances, this may result in additional compliance requirements to:

1. Appoint a separate data protection officer (DPO) for both the UK and EU;
2. Nominate a new lead supervisory authority (LSA) in the EU as well as registering with the ICO in the UK;
3. Appoint a local representative in the EU/UK; and
4. Manage potential exposure to sanctions/fines under both the EU and UK regulatory enforcement regime, i.e. risk of double jeopardy for any infringement.

Other Actions to Take

Be sure that all references in governance records, contracts and transparency notices are updated to reflect the post-Brexit position of the UK being outside the EU. This may require changes to:

1. Records of processing activities, in respect of international transfers;
2. Privacy Notices, which should refer to any data transfers to 'third countries' as well as including correct details of any DPO, local representative and/or LSA;
3. DPIAs which may need to be updated if they refer to a transfer which becomes a transfer to a 'third country' on exit-date; and
4. Contracts with third parties, if they include specific reference to the GDPR, EEA or anticipate a data transfer between the EU and the UK. ICQ

EDITOR'S NOTE : *New draft SCCs and recommendations on supplementary measures have been issued for consultation by the European Commission and the EDPB respectively. ACOI members are encouraged to familiarise themselves with both documents and participate in the consultation process as each will have a significant impact on the future of international data transfers.*