Data transfers—the aftermath of Schrems II

03/08/2020

Information Law analysis: Victoria Hordern, partner and head of data privacy at Bates Wells, considers the impact of the judgment taken by the Court of Justice on 16 July 2020 in Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems, Case C-311/18 (Schrems II) on European data protection law.

European data protection law includes restrictions on the ability of EU organisations to transfer personal data to a non-EEA recipient. These restrictions are not new. They existed in an earlier form in the original Data Protection Directive, Directive 95/46/EC. However, the way that these restrictions have been interpreted by the Court of Justice over the years has led to a complicated picture.

Back in 2015 (and before the General Data Protection Regulation (GDPR), Regulation (EU) 2016/679) the Court of Justice ruled that the Safe Harbor regime permitting data transfers from the EU to the US was invalid due to a lack of controls on the US Government's access to transferred personal data (a decision colloquially known as *Schrems I (Schrems v Data Protection Commissioner*, Case C-362/14, [2015] All ER (D) 34 (Oct)) since instigated by a privacy activist called Max Schrems). The defeat of Safe Harbor led to the birth of Privacy Shield intended to be an improved version and designed to provide the controls on the US Government's access to personal data that *Schrems I* indicated were lacking. However, in a decision of 16 July 2020 and also instigated by a complaint from Mr Schrems (*Schrems II,* Case C-311/18), the Court of Justice ruled that Privacy Shield was invalid as the controls failed to properly protect personal data.

The Court of Justice additionally ruled that another data transfer mechanism—the 2010 Standard Contractual Clauses—was valid. However, the court ruled that those that rely on Standard Contractual Clauses (SCCs) or other appropriate safeguards (eg Binding Corporate Rules (BCR) etc) are expected to demonstrate (based on a case-by-case assessment) that the appropriate safeguard provides an adequate level of protection in practice. This may require the use of supplementary measures or where this is not possible the transfer must not proceed.

What are the key implications of Schrems II for those transferring personal data outside the EEA (including the UK)?

The key implications are:

- exporters can no longer transfer personal data to the US by relying on the Privacy Shield. They must now rely on an alternative mechanism. For most, this will mean signing SCCs
- the ability of the US Government to access personal data due to surveillance laws makes effective protection for personal data transferred to the US very challenging. But the Court of Justice stopped short of saying that all data transfers to the US are unlawful and must cease
- the standard for appropriate safeguards (eg SCC, BCRs etc) under Article 46 of Regulation (EU) 2016/679 (GDPR) is effectively that they must provide 'essential equivalence' to the protections afforded to individuals under EU law. All data transfers relying on appropriate safeguards must be assessed according to this standard
- the SCCs and other appropriate safeguards (eg BCRs) remain valid but an exporter (and importer) will need to undertake a case-by-case assessment of each transfer to ensure that in

practice the appropriate safeguard provides essentially equivalent protections to individuals as afforded under EU law
- it is the responsibility of the exporter in the EEA (and European data protection authorities) to take action where the data transfers are not properly protected ie to cease the transfers

How are large businesses and SMEs in the EEA that transfer personal data outside the EEA which relied on Privacy Shield or appropriate safeguards (eg SCCs or BCRs) under Article 46 responding to Schrems II?

Many organisations in the EEA transferring personal data will have been surprised by *Schrems II*. Within a matter of four years, the replacement to Safe Harbor has been invalidated and there are now additional pressures on the use of SCCs and BCRs. Large organisations with an international reach will have a significant amount to do in order to carry out Transfer Risk Assessments for each data transfer using SCCs or BCRs. Most that were relying on the Privacy Shield for transfers intend to move to rely on the SCCs. However, many organisations are waiting to see whether the European Commission will publish the updated SCCs shortly so that they can put the updated SCCs in place, whether as a replacement for Privacy Shield or the existing SCCs. It is unlikely that many organisations will simply stop transferring personal data outside the EEA given how critical many data transfers are to business as usual. Having said this, businesses will need to consider their own risk appetite especially if they operate in an EU jurisdiction where the data protection authority has expressed serious concerns about data transfers eg the Berlin data protection authority's press release of 17 July 2020 indicated that transfers to the US are currently not possible.

Smaller organisations including SMEs will face more uncertainty if they rely on numerous third party providers outside the EEA and have not yet had a clear indication from those third parties how they will help the SME meet its obligations. A European SME can ask a US tech platform to sign a SCC, but the US platform may choose not to respond. The options then available for the SME are to terminate the contract (and potentially cause themselves disruption plus additional costs) or continue to use the US platform hoping that in time it will approach its customer base with its own solution.

Significantly, the European Data Protection Board (EDPB) has confirmed in FAQs that if the exporter's assessment of the transfer reveals that appropriate safeguards in the third country cannot be ensured, it must (i) cease the transfer or (ii) if it continues with the transfer, it must notify the relevant data protection authority.

What steps should EEA businesses which transfer personal data to the US or other jurisdictions outside the EEA take: (a) now; and (b) in the medium to longer term?

The ICO has recommended organisations should take stock of the international transfers they make and react promptly as guidance and advice becomes available.

EEA organisations should take the following steps in the short term:

- identify the personal data transfers being made in reliance on Privacy Shield and appropriate safeguards (eg SCC and BCRs). This includes data transfers as part of outsourcing contracts where sub-processors are based outside the EEA
- where possible, implement SCCs for each data transfer relying on the Privacy Shield. This will require reaching out to the importer to help with the process

In the short to medium term, EEA organisations should:

- devise a Transfer Risk Assessment—while there is no clear guidance on the scope of this assessment yet from data protection authorities, the ruling in *Schrems II* (which pointed to the elements under Article 45 (2)) and commentary in the EDPB FAQs can help organisations put together a preliminary assessment document which can be updated over time as more guidance becomes available (asking, for instance, in relation to the third country: How can government authorities access personal data? What are the enforceable rights for individuals? What effective legal remedies are there?)

- for each data transfer based on appropriate safeguards (eg SCCs or BCRs), instigate the Transfer Risk Assessment
- having carried out the assessment, consider whether any supplementary measures are necessary to ensure that appropriate safeguards are lawful. At present there is a lack of guidance from courts and regulators as to what safeguards may be used, although some commentators have suggested these might be contractual, technical (eg encryption) or organisational. Implement the supplementary measures

The medium to longer term steps are:

- keep an eye out for new versions of the SCCs due to be published by the European Commission. Once published, you'll want to update your SCCs
- watch for further guidance from data protection authorities about what they will expect you to evidence in your Transfer Risk Assessment
- consider whether other appropriate safeguards might be suitable eg BCR, codes or certifications (when existing)
- especially for more high risk data transfers to organisations clearly subject to US surveillance law (eg cloud providers), explore whether the provider can store your data in the EEA or consider re-procuring services in the EEA
- consider whether you need to make any additional change to your existing GDPR compliance framework eg updating privacy notices

Interviewed by Gloria Palazzi

XXXXXXX (add link to MTE) is a XXXXX at XXXXXXX, and a member of LexisPSL's Q&A Expert Panel. Suitable candidates are welcome to apply to become members of the panel. Please contact lexisask@lexisnexis.co.uk.