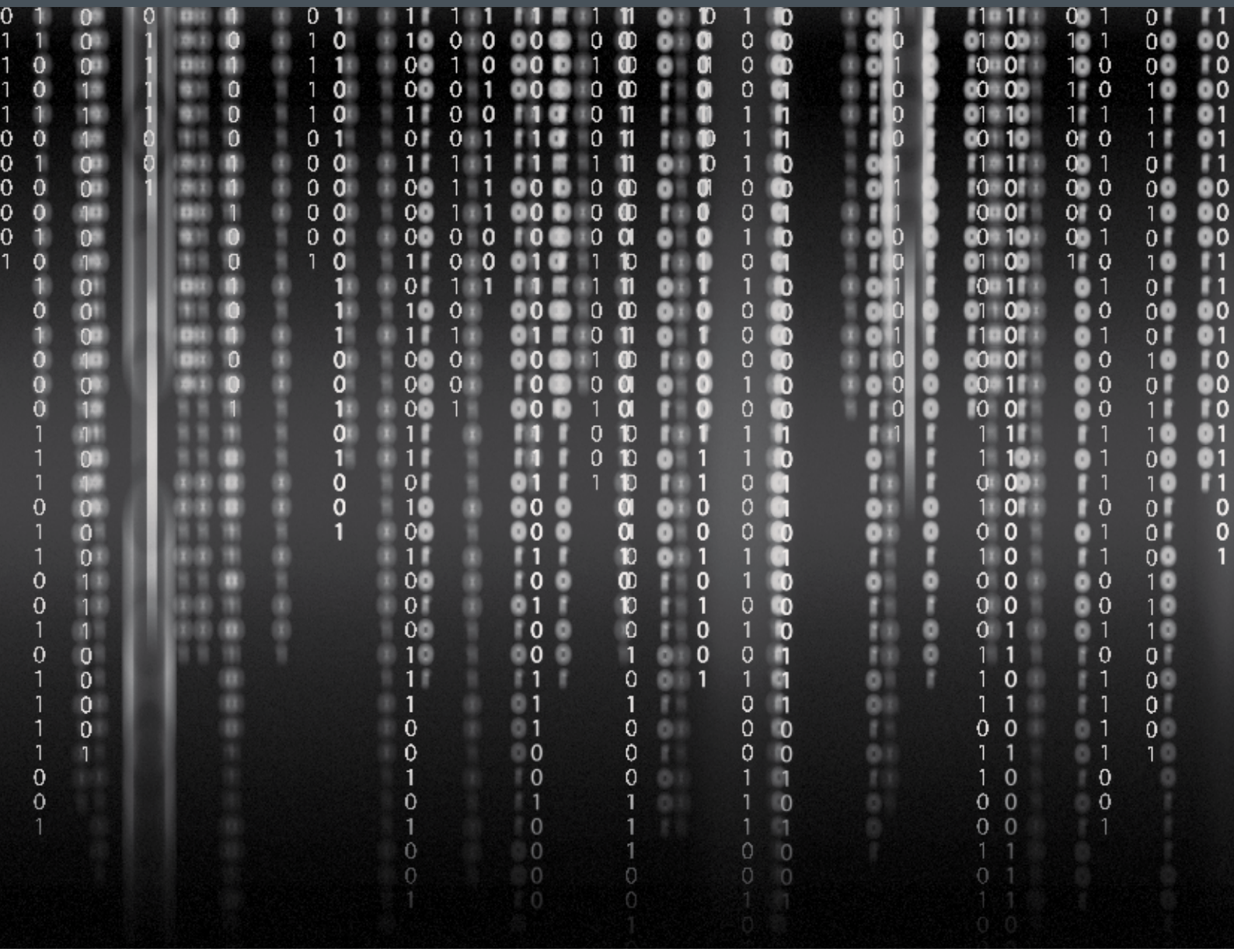

INTERNATIONAL DATA TRANSFERS FROM THE EEA AND UK: TAKE CARE

The *Schrems II* judgment, handed down by the Court of Justice of the European Union (CJEU) on 16 July 2020[1], is significant for any organisation which currently transfers personal data outside of the European Economic Area (EEA) or the United Kingdom (UK). It is especially significant for organisations which currently transfer personal data from the EEA or the UK to the USA.

1 Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems, Case C-311/18.

“A transfer includes a situation where personal data is made available to organisations outside of the UK and the EEA.”

The judgment invalidates the use of the ‘Privacy Shield’ to transfer personal data from the EEA or the UK to the USA. More generally, the judgment creates uncertainty for organisations which use the European Commission’s (Commission) ‘Standard Contractual Clauses’ (SCCs) or ‘Binding Corporate Rules’ (BCRs) to transfer personal data outside of the EEA or the UK. This is because the CJEU has confirmed that EU standards of data protection must travel with personal data when it leaves the EEA or the UK.

The Commission and European Data Protection Board (EDPB) are working to provide guidance on additional measures, whether legal, technical or organisational, which data exporters and data importers may need to take. Meanwhile, the EDPB has recommended that data exporters who rely on SCCs should conduct a risk assessment as to whether SCCs provide enough protection within the data importer’s local legal framework, whether the transfer is to the USA or elsewhere. The EDPB’s Frequently Asked Questions (FAQs) on the judgment are available on the EDPB’s website.[2]

Legal Background

Chapter V of the GDPR requires that organisations which transfer personal data outside of the EEA and the UK ensure that the level of protection which is given to that personal data by the GDPR is not undermined as a result of the transfer. A transfer includes a situation where personal data is made available to organisations outside of the UK and the EEA.

In general, in order to ensure that this requirement is complied with, organisations should ensure that one of the following applies to the transfer of personal data:

- The transfer of personal data is to a country which benefits from a decision of the Commission that the country ensures an adequate level of protection of personal data (Adequacy Decision);
- That one of the safeguards set out in Article 46 of the GDPR – which include use of the SCCs - applies to the transfer; or
- That one of the derogations set out in Article 49 of the GDPR applies to the transfer.

Transfers to countries with an Adequacy Decision in place are straightforward. However, only a limited number of countries benefit from an adequacy decision. A derogation may be available in specific situations, but a derogation cannot be used to justify large-scale or systematic transfers of personal data. Therefore, organisations use safeguards extensively to justify their transfer of personal data: in many cases use of the SCCs will be the only way an organisation can in practice lawfully transfer personal data outside of the EEA or the UK.

Factual Background

Max Schrems, a data protection activist, filed a complaint with the Irish Data Protection Commissioner in 2013 about the transfer of personal data by Facebook from Ireland to the USA. This complaint ultimately led to the *Schrems I* judgment of the CJEU, which determined that the ‘Safe Harbour’ framework, which had facilitated the transfer of personal data between the EEA (including the UK) and the USA, was invalid[3].

Following *Schrems I*, the ‘Safe Harbour’ was replaced by the ‘Privacy Shield’. The Privacy Shield was a type of Adequacy Decision which permitted personal data to be transferred from the EEA or the UK to those organisations in the USA which had signed up to it. Following *Schrems I*, Max Schrems reformulated his complaint, which led the Irish High Court to refer to the CJEU questions regarding:

- the validity of using the Privacy Shield to transfer personal data to the USA; and

2 https://edpb.europa.eu/sites/edpb/files/files/file1/20200724_edpb_faqoncjeuc31118.pdf

3 Maximillian Schrems v Data Protection Commissioner, Case 362/14.

- the validity of using SCCs to transfer personal data to the USA.

Judgment – Privacy Shield

The CJEU found that the Adequacy Decision establishing the Privacy Shield was incompatible with the requirements of the GDPR.

It did so principally because it considered that US Surveillance Authorities had disproportionate access to personal data transferred to the USA, that their access was not sufficiently controlled by US legislation, and that data subjects whose personal data had been transferred did not have sufficient rights of redress in relation to the use of their personal data by US Surveillance Authorities.

As a result, it concluded that the Commission had been wrong when it had determined that transfers of personal data to the USA would receive an adequate level of protection, provided that the recipient in the USA had signed up to the rules of the 'Privacy Shield', which had been designed to provide enhanced safeguards.

On a practical level, organisations should no longer rely on the Privacy Shield in order to transfer personal data to recipients in the USA, as confirmed by the EDPB's FAQs.

Judgment – SCCs

Some commentary on the *Schrems II* judgment has indicated that the CJEU banned the use of the Privacy Shield to transfer personal data to the USA, but allowed organisations to use SCCs to transfer personal data to the USA. Unfortunately, the CJEU's judgment on the use of SCCs is more complex.

The CJEU highlighted that use of the SCCs to transfer personal data to the USA would not be prohibited. However, the CJEU emphasised that use of the SCCs by themselves is not sufficient. The CJEU stated that when using SCCs generally, it is the duty of the sender of the personal data, working with the recipient, to ensure that the law of the country to which the personal data is transferred would not undermine the level of protection afforded to personal data by the GDPR. If the sender cannot be satisfied that this is the case, or the recipient informs the sender that this is not the case, the sender should not transfer personal data to that country, even if the SCCs are used.

The CJEU also emphasised that supervisory authorities in EEA Member States have the power to suspend or restrict transfers to third countries if an adequate level of protection cannot be assured in the third country, even where SCCs are used. Therefore it is possible that individual data protection authorities could prohibit transfers reliant on use of the SCCs to particular third countries. As invited by the CJEU, to avoid divergent decisions, EEA data protection authorities will further work within the EDPB to ensure consistency.

In determining whether an adequate level of protection can be ensured in the third country, the CJEU's judgment provides that, if public authorities in the third country will have access to personal data, the data exporter should consider factors that inform the Commission in determining whether it should make an Adequacy Decision in respect of a third country, such as rights of redress and the proportionality of access by public authorities.

Whilst not explicitly stated in the judgment, given its criticism of the US system on these counts, the CJEU's judgment indicates that it will not be valid to transfer personal data to the USA in reliance on the SCCs, as these do not by themselves ensure an adequate level of protection, and access by public authorities in the US will undermine the level of protection. Therefore, it would appear difficult for exporters of personal data to the USA in reliance on the SCCs to conclude that an

adequate level of protection can be ensured in the USA, as they must do for such a transfer to be lawful.

Implications

The CJEU's judgment has significant implications for any organisation which transfers personal data on a large-scale or systematic basis from the UK or EEA to any country which does not currently benefit from an Adequacy Decision. In these circumstances use of the SCCs will generally be the only option to ensure a lawful transfer of personal data.

However, in order to make a lawful transfer of personal data in reliance on the SCCs, the data exporter must also be satisfied that the law of the country to which the personal data will be transferred will not undermine the level of protection afforded by the GDPR, particularly where the public authorities in the third country will potentially have access to the personal data.

For many organisations, the task of assessing whether a third country ensures an adequate level of protection of personal data will be a significant compliance burden. For SMEs looking to build a global business, it may be overwhelming. Based on the CJEU's judgment, there would also appear to be a number of jurisdictions that are significant in global commerce, including the USA, where it may be difficult for data exporters to conclude that an adequate level of protection can be ensured. In theory, the judgment could lead to an effective ban on the export of personal data to a number of jurisdictions, including the USA.

For our many clients operating in inherently global industries, for whom data localisation in the EEA is simply not possible, the judgment leads to an unacceptable degree of legal uncertainty about whether it will be possible to transfer personal data to individual countries outside of the UK or EEA lawfully. The EDPB will provide more guidance.

For the time-being, organisations could continue to rely on their existing SCC arrangements, but in the knowledge that this will not be free of risk, and should regularly review guidance of the EDPB, the Commission and data protection authorities in the EEA or UK.

For further information, please contact the authors of this briefing;

ANTHONY WOOLICH
Partner, London
T +44 (0)20 7264 8033
E anthony.woolich@hfw.com

JEREMY KELLY
Associate, London
T +44 (0)20 7264 8798
E jeremy.kelly@hfw.com