CJEU Schrems II decision – what now for international data transfers

The Court of Justice of the European Union (CJEU) has followed the opinion issued by the Advocate General at the end of last year and declared that the model Standard Contractual Clauses (SCCs) (also known as model clauses) are valid. But in a blow for businesses transferring data between the EU and the US, the CJEU has ruled that the EU-US Privacy Shield is invalid and has raised questions about the adequacy of the protection offered to data subjects when their data is transferred to the US.

Background

The General Data Protection Regulation (GDPR) provides that the transfer of personal data from the EEA to a country outside of the EEA (referred to in the regulation as a 'third country') may only take place if that third country ensures an adequate level of data protection (subject to a few narrow exceptions, or having the specific consent of the individual).

Under the GDPR, the European Commission may make a finding that a country's domestic laws or international commitments provide an adequate level of protection. But if there is no adequacy decision, organisations in the EEA (the data exporter) are only permitted to transfer personal data outside of the EEA if they have put in place appropriate safeguards. To date, many organisations have achieved these appropriate safeguards by entering into SCCs with the transferee (the data importer) or, where the transfer is to the US, by only transferring data to organisations which comply with the requirements of the EU-US Privacy Shield.

These appropriate safeguards have now been reviewed by the CJEU and the decision has raised concerns for organisations carrying out international data transfers, in particular transfers to and from the US.

The case

The case, known as "Schrems II" (Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems), arises out of action brought by Maximilian Schrems under which the original "Safe Harbor" arrangements with the US were found to be invalid and were subsequently replaced by Privacy Shield. The referring court asked the CJEU to consider both the Privacy Shield and the SCCs in light of the GDPR.

The CJEU confirmed that data subjects whose data is transferred to a third country must be given a level of protection essentially equivalent to that guaranteed under the GDPR. The CJEU's judgement ruled that the US government surveillance programmes and related limitations do not meet the requirements of proportionality under EU law and do not grant data subjects actionable rights against the US authorities.

The CJEU followed the Opinion issued by the Advocate General at the end of last year and declared that the SCCs are valid but decided that the Privacy Shield's Ombudsperson mechanism does not provide a sufficient remedy to make up for the lack of actionable rights against US authorities and as a result ruled that the Privacy Shield is invalid.

SCCs

Giving its decision, the CJEU declared that whilst the SCCs are valid, in order for an international transfer of data to be permitted there must be appropriate safeguards, enforceable rights and effective legal remedies for the data subjects whose personal information is being transferred. This means that the data exporter must consider both the SCCs and the relevant aspects of the legal system of the third country to which the data is being transferred. Data importers are also obliged to notify exporters if they can't comply with the SCCs,

In addition to expanding the responsibilities of the data exporters and data importers, the CJEU also ruled that, unless there is a valid adequacy decision by the European Commission, the ICO (or other supervisory authority in the data exporter's jurisdiction) must suspend or prohibit a transfer of personal data to a third country where the ICO considers that the SCCs will not be sufficient to provide the protection required under the GDPR for the data being transferred and the data subjects.

What steps are data exporters and data importers required to take?

The CJEU's decision makes it clear that the SCCs can no longer be seen as a simple paperwork solution but raises some uncomfortable questions about how much investigation, monitoring and due diligence an organisation is expected to perform when it exports data outside of the EEA. Following the CJEU's decision the European Data Protection Board (EDPB) has issued a statement which provides that when assessing whether the SCCs will be sufficient to provide the required protection, the data exporter (if necessary, with the assistance of the data importer) should consider the content of the SCCs, the specific circumstances of the transfer, as well as the legal regime in the data importer's country. The CJEU emphasised that these assessments should take place on a case-by-case basis and confirmed that the data exporter may have to consider putting additional measures in place over and above those included in the SCCs. The EDPB has confirmed that it will be looking further into what these additional measures could consist of.

What to do now

In terms of next steps, businesses should now:

- Review their international data transfers and identify the basis on which those transfers are taking place; European Commission adequacy decision, SCCs, Privacy Shield etc.

- Where transfers taking place under the Privacy Shield, these transfers are now invalid following the CJEU's decision so businesses are strongly advised to put SCCs in place to cover those transfers.
- Where transfers are taking place under the SCCs, consider whether the business is able to assess the level of protection for data in the destination countries.
- Consider whether international transfers of personal data are necessary or whether it is possible for the data to remain in the EEA.

Await further guidance

There is mounting pressure on the ICO and other data protection authorities to provide further guidance in this area. The CJEU's decision confirms that it does not consider the US to provide EU citizens with sufficient remedies against government requests for access to data. Does this mean that all data transfers to the US need to cease, or where a particular data importer has not been subject to government requests to access data in the past, can transfers to those importers continue?

Kathryn Rogers

Partner