

Schrems II – impact for UCL (updated 31.07.20)

On 16th July 2020, the Court of Justice of the European Union (CJEU) delivered its judgment in the "Schrems II" case.

Background and decision

Most organisations rely on data transfer agreements - Standard Contractual Clauses (SCCs) – to transfer personal data to countries outside the European Economic Area (EEA). Organisations often rely on the EU-US Privacy Shield when transferring personal data to US organisations certified under the Privacy Shield. The CJEU was asked to consider if law and practice in the US relating to access to personal data by the intelligence services should mean that either, or both – of these mechanisms should be invalidated.

The decision concludes that the Privacy Shield is invalid. SCCs remain valid. However, the CJEU sets out a heavy burden on data exporters which wish to use SCCs; the data exporter must consider the law and practice of the country to which data will be transferred, especially if public authorities may have access to the data. Additional safeguards, beyond the SCCs, may be required.

Impact on the EU-US Privacy Shield

The EU-US Privacy Shield was a partial 'Adequacy Decision' by the European Union which provided a mechanism to transfer personal data to commercial US organisations certified under the Privacy Shield. This meant that personal data could be transferred to these organisations without further privacy protections.

This decision means that data transfers to the US relying on the protections in the Privacy Shield are no longer permitted.

This is a clear change, meaning that UCL needs to rely solely on SCCs for new transfers of personal data to the US at least in the short term until the new form of Privacy Shield is agreed (assuming one is agreed) or further guidance is issued by the ICO or European Commission.

Impact on Standard Contractual Clauses (SCCs)

SCCs remain a valid way to transfer personal data outside of the EEA following the CJEU ruling.

However, the CJEU emphasises that organisations using SCCs need to assess whether, in the overall context of the transfer, there are in fact appropriate safeguards in the third country for the personal data transferred out of the EEA, taking into account not only the destination of the personal data but also, in particular, any access by public authorities and the availability of judicial redress for individuals.

What next?

We await further guidance from the ICO regarding steps to be taken with regard to data transfers currently in place which are protected by the Privacy Shield.

In the meantime:

1. Any new arrangements for transfer of personal data to the US should be protected by SCCs;
2. Any agreements which are currently in place which rely on the Privacy Shield do not need to be amended at this stage, until we receive further guidance from the ICO; and

3. Any use of SCCs must also include an assessment of the privacy safeguards in place for the country the data is being transferred to.

We will release further guidance as and when the position becomes more clear.

If you consider that any data you are proposing to transfer to the US is particularly sensitive and/or has the potential to be of interest to the US intelligence services, please do consult the Data Protection Office.

Further reading:

- [Schrems II judgment: Privacy Shield invalid, SCCs survive, but... what happens now?](#)
- [Court of Justice of the European Union PRESS RELEASE No 91/20](#)