Schrems ii and its impact on data transfers

Wendy Lambert
Partner

Ashley Quenault
English Solicitor

Introduction

The landmark Court of Justice of the European Union (CJEU) case of Data Protection Commissioner v Facebook Ireland Limited, Maximilian Schrems (also known as Schrems II) has sent shockwaves in the field of international data transfers.

Whilst this case represents a decision based upon the General Data Protection Regulation (GDPR), Jersey's Data Protection (Jersey) Law 2018 is heavily based upon the GDPR.

Accordingly, major developments or decisions about the GDPR will have an impact on Jersey's equivalent legislation.

The purpose of this article is to provide a very short summary of the facts of this case and also to identify some practical steps that organisations should be considering in light of this judgment.

Facts

A complaint was lodged by an individual to the Irish Data Protection Commissioner about Facebook Ireland transferring his personal data to its parent company in the US. He alleged that this very act exposed his personal data to mass US surveillance laws. The CJEU had to consider whether two of the key mechanisms that legitimise the transfer of personal data to countries outside of the European Economic Area offer enough protection. Those mechanisms are:

- Standard Contractual Clauses (SCCs) – these are a series of template forms of agreement approved by the European Commission. These are entered into between the data exporter and the data importer with the aim of protecting personal data leaving the European Economic Area and ensuring that data subjects residing within the EU have a right of redress against the data exporter and data importer for any misuse of their personal data as a result of that transfer. These have been the predominant foundation of cross-border data transfers from the EU for many years.
- The Privacy Shield – this is a partial adequacy framework agreed between the EU and the US.

Decision

The CJEU held that the Privacy Shield was invalid with immediate effect. The CJEU held that the personal data of individuals residing in the EU could be at risk of being accessed and processed by the US government for surveillance purposes in a manner which is incompatible with the privacy rights guaranteed in the EU.

The CJEU further concluded that there was no remedy available for EU individuals to ensure protection of their personal data once it is transferred to the US. This means that from 16 July 2020 (being the date of the judgment) the Privacy Shield can no longer be used effectively as an export mechanism for data transfers.

In respect of the SCCs, the CJEU concluded that whilst these remain a valid export mechanism, certain additional requirements must be met which include:

- Data exporters taking a proactive role in assessing, prior to any transfer of personal data, whether there is in fact an adequate level of protection for that personal data subject to the SCC once it is exported.
- Data importers must also take an active role by informing data exporters of any inability to comply with any of the provisions of the SCCs. If a data importer is unable to comply with the terms of the SCCs and there are no additional safeguards in place to ensure an adequate level of protection, the data exporter must suspend the transfer of the personal data and or terminate its contract with the data importer.
- Supervisory authorities have an obligation to assess and, where necessary, suspend and prohibit transfers of personal data to an importing jurisdiction if they conclude

Schrems ii and its impact on data transfers cont.

that the SCCs are not or cannot be complied with in that country and the protection of the data transferred that is required by EU law cannot be ensured by other means. In short this may mean that supervisory authorities (including the Jersey Office of the Information Commissioner) should issue separate lists of countries they consider adequate for SCCs to be used.

Regulator View

The Jersey Office of the Information Commissioner has published its initial views of this judgment. Their recommendations are that data controllers and processors in Jersey should consider:

- The extent to which they already rely upon the Privacy Shield and identify what alternative methods could be relied upon for the data transfer instead of the Privacy Shield
- If SCCs are currently being relied upon, a review should be undertaken to consider whether the receiving jurisdiction can provide the same standard of protection required under the Data Protection (Jersey) Law 2018 and if they cannot such data transfers should be suspended until such issues are resolved

Practical Steps

In light of this judgment and the guidance from the Office of the Information Commissioner, Jersey-based data controllers and processors should consider undertaking the following tasks:

- Ensure senior management are aware of the Schrems II decision and its implications
- Undertake a review of current data transfer arrangements. In particular it will be imperative to understand:
  - What sort of personal data is being transferred and where that data is being transferred to
  - What safeguards are in place in that jurisdiction
  - What is the basis upon which the personal data is being transferred (e.g. Privacy Shield, SCCs or other method)
  - Whether any existing or proposed transfers need to be suspended or at least paused.
- Review existing outsourcing agreements and accompanying risk assessments
- Consider whether it may be possible to keep the personal data within Jersey and thus remove the need to consider international data transfers

This briefing only provides a summary of the subject matter. It does not constitute legal advice. If you would like legal advice, support in considering or dealing with this matter or further information, please contact Wendy Lambert or Ashley Quenault.