CAREY OLSEN

The data transfer challenge: Schrems II and the Channel Islands

Service area / Cybersecurity and Data Protection, Regulatory
Legal jurisdictions / Guernsey, Jersey
Date / July 2020

Both Jersey and Guernsey have based their data protection laws on the GDPR and in doing so have incorporated many of the decisions of the European Commission in regulating data protection in the Channel Islands.

This means that when there are major developments in European law which relate to data protection, Jersey and Guernsey data protection law will often also be subject to significant change.

In deciding the case of *Irish Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems* (Case C-311/18), a case which has become known as *Schrems II*, the European Court of Justice ("**ECJ**") has delivered such a major development and the impact on Channel Islands data protection law is likely to be accordingly significant.

International data transfer

One of the key areas of focus for European data protection law since 1995 has been the extent to which personal data may be transferred outside of the EU/EEA to other jurisdictions, many of which do not provide an equivalent level of protection for personal data.

Both the General Data Protection Regulation (Regulation (EU) 2016/679 – the "**GDPR**") and the 1995 Data Protection Directive which it replaced (Directive 95/46/EC – the "**Directive**") took a similar approach to international transfer – an approach which is essentially transposed into Channel Islands law by the primary data protection legislation in Jersey and Guernsey (currently the Data Protection (Jersey) Law 2018 (the "**DPJL**") and the Data Protection (Bailiwick of Guernsey) Law, 2017 (the "**DPGL**")).

Similar to the approach taken in the Directive, the GDPR permits data transfers without restriction to countries (which include Jersey and Guernsey) whose legal regime is deemed by the European Commission to provide for an "adequate" level of protection for personal data.

In the absence of an adequacy decision, transfers are permitted outside the EU/EEA under certain other specified circumstances, in particular where such transfers take place subject to "appropriate safeguards", which include:

- Legally binding and enforceable instruments between public authorities;
- Binding corporate rules ("**BCRs**");
- Standard data protection contractual clauses adopted by the European Commission ("**SCCs**").

Schrems and the USA

Due in part to the dominance of the United States of America in the provision of online services, data transfers to the USA have been the subject of a significant amount of regulatory and judicial consideration.

Transfers to the USA were previously authorised by a limited adequacy finding by the European Commission in July 2000, known as the US Safe Harbor.

The Safe Harbor was invalidated by the ECJ as a result of a case brought by Maximilian Schrems, at that time an Austrian law student and privacy campaigner. A Facebook user, he objected to Facebook transferring the personal data of its European users to servers located in the United States. Mr Schrems complained to the Irish Data Protection Commissioner (Facebook's main EU subsidiary being based in

Ireland). The Irish Data Protection Commissioner refused to investigate on the basis that it was bound by the Commission's Safe Harbor decision. Mr Schrems challenged this decision before the Irish High Court, which referred the matter to the ECJ.

Mr Schrems relied on the disclosure of the USA's state surveillance activities by Edward Snowden and claimed that the laws and practices of the US did not provide for a sufficient level of protection for personal data or rights for EU citizens to obtain redress.

The ECJ (in *Maximillian Schrems v Irish Data Protection Commissioner* (Case 362-/14) which has become known as *Schrems I*) agreed and struck down the Safe Harbor.

Schrems v the Privacy Shield and SCCs – Schrems II

The ECJ judgment in *Schrems I* left open the possibility of transfers to the United States utilising either BCRs or SCCs. The European Commission also subsequently negotiated a new adequacy mechanism to replace Safe Harbor– the EU-US Privacy Shield.

Mr Schrems then reformulated his complaint to challenge the transfer of personal data on the basis of the SCCs – which was the mechanism which Facebook utilised to legitimise its EU-US data flows.

The Irish Data Protection Authority brought proceedings before the Irish High Court, which referred a number questions to the ECJ for determination – a case which became known as *Schrems II*.

On 16 July 2020, the ECJ handed down its decision in *Schrems II*. In short, the key issue before the ECJ was broadly the same as in *Schrems I* – whether the legal and regulatory (and practical law enforcement) environment in the United States meant that either or both of the Privacy Shield mechanisms should be held to be invalid.

In summary, the ECJ concluded that the Privacy Shield is invalid as providing insufficient protection for EU data subjects. SCCs remain valid. However, the ECJ's decision on SCCs came with a significant sting in the tail.

The ECJ's decision imposed potentially significant additional burdens upon data exporters which use or wish to use SCCs. The ECJ stated that data exporters must perform an assessment which considers 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 to address any shortcomings. It is yet to be seen what such safeguards might look like and there must be significant questions as to what type of safeguards could ever satisfy the ECJ that transfers to jurisdictions which enable significant national security and/or State access to personal data as a matter of course would be permissible.

The SCCs themselves are overdue for reform; the existing forms approved by the European Commission date from 2010 and reform has been put on hold pending the judgment in *Schrems II*. Any revised versions will need to reflect the necessity for an assessment of the jurisdiction to which personal data is to be transferred.

Why is this important in the Channel Islands?

The dominant industry in Jersey and Guernsey remains the finance industry, which is reliant on the free flow of data from jurisdiction to jurisdiction, particularly where businesses are part of international groups or where their client base is international.

Whilst Jersey and Guernsey are both "adequate" jurisdictions for the purposes of the GDPR, this status is subject to review and international transfer is likely to be squarely in the spotlight.

The provisions of the DPJL and the DPGL broadly mirror those in the GDPR so far as international transfer is concerned meaning the invalidating of Privacy Shield by the ECJ will also invalidate it for DPJL/DPGL purposes.

Additionally, many controllers and processors in the Channel Islands will be subject to the GDPR itself as result of its extra-territorial provisions.

Accordingly, any controllers or processors in the Channel Islands should be considering the impact of *Schrems II* on their international transfer provisions.

It should also be noted that whilst the decision of the ECJ focussed on the USA, its logic almost certainly applies to every jurisdiction without an adequacy finding.

Available guidance

The European Data Protection Board ("**EDBP**") has issued some initial FAQs. The EDPB makes it clear that:

- Privacy Shield is invalidated with immediate effect;
- Whilst SCCs and/or BCRs may still continue to be used for transfers to the US, data exporters must conduct an assessment of each case, taking into account the circumstances of the transfers, and supplementary measures which could be put in place. Such supplementary measures along with SCCs, following a case-by-case analysis of the circumstances surrounding the transfer, would have to ensure that US law does not impinge on the adequate level of protection they guarantee. If they cannot ensure such impingement, transfers may have to be suspended or ended.
- The same assessment would need to be undertaken for all transfers to a third country based on SCCs and/or BCRs.
- There will be further guidance on what "assessment" means in practice.

Both the Jersey Office of the information Commissioner (JOIC) and Guernsey's Office of the Data Protection Authority (ODPA) have published their initial views of *Schrems II*. Broadly, both

regulators echo each other, recommending that controllers and processors should consider:

- The extent to which they are reliant upon Privacy Shield;
- The availability of alternatives to Privacy Shield;
- Where reliance is placed on SCCs and or BCRs, a review should be undertaken to consider any risks and any appropriate safeguards to address such risks.

The Jersey regulator arguably went significantly further, however:

> *"...any Jersey-based business using SCCs as a transfer mechanism to another Third country will need to ensure that the receiving jurisdiction can provide the same standard of protection as required by the DPJL. The receiving data importer will be expected to identify any areas or factors that may prevent them from complying with those standards. If that happens, the expectation will be that the Jersey-based company must suspend the transfer until such issues are resolved and the appropriate standards of protection can be afforded in the receiving jurisdiction."*

Read literally, this would appear to suggest that (for example) transfers to the USA should be suspended, as should transfers to any other non-adequate jurisdiction where there are significant concerns relating to State or national security access to personal data. However, the balance of the publication by JOIC would not appear to suggest that is what is expected. Instead, Jersey organisations should ensure that they have reviewed their data transfers and have taken steps to address any risks.

It is also notable that should the UK not have obtained an adequacy finding from the European Commission following the end of the Brexit transition period, then the *Schrems II* decision could potentially impact transfers to the UK (which has in the past been criticised for the scope of the powers which it gives to its security services to access personal data).

What to do next

We would recommend that controllers and processors in the Channel Islands should consider the following:

- **Make sure that senior management are aware that this is important:** you should ensure that senior management are aware of the *Schrems II* decision and its implications – there are likely to be a range of impacts from cost to legal to practical.
- **Review your current transfers:** there has been a presumption in the past that SCCs could be used for transfers to any jurisdiction. This will not be the case going forward and it is accordingly imperative to understand:
  a. Which personal data is being transferred to which jurisdiction (or accessed from – this includes remote access via such platforms as Citrix);
  b. What the sensitivity of the personal data being transferred is (e.g. is it special category? Or otherwise sensitive for another reason?);
  c. What technical and/or practical safeguards are already in place? For example, encryption and/or tokenisation may already be in place, as may remote access which may easily be withdrawn;
  d. Which basis is being relied upon for the relevant transfer? The obvious ones are:
     1. Adequacy;
     2. Privacy shield (for US transfers);
     3. SCCs; or
     4. BCRs.
  e. Whether any existing or proposed transfers need to be suspended (or at least paused).
- **Review your outsourcing agreements and risk assessments:** the *Schrems II* decision will likely affect a number of outsourcing arrangements and may have a material impact, particularly where outsourcing is taking place under the JFSC Outsourcing Policy or its GFSC equivalent. Controllers and processors should consider at an early stage whether:
  a. Outsourced functions should be reviewed;
  b. Whether risk assessments need to be amended;
  c. Whether *Schrems II* may make outsourcing less attractive as a proposition;
  d. Whether regulators need to be engaged with; and/or
  e. Whether transactions involving the export of personal data to non-adequate jurisdictions should be delayed (or cancelled).
- **Consider whether localisation is practicable or appropriate (or whether it might be a selling point).** Obviously, one of the lowest risk approaches to international data transfer is simply not to undertake it and instead to keep data within Jersey or Guernsey (so-called data "localisation"). Whilst in many businesses data localisation will not be practicable, it may be possible to localise more sensitive data (or client data) and only export tokenised/pseudoanonymised data. Additionally, the offer of data localisation may be a selling point for many clients, particularly those for whom privacy is a priority.
- **If you are relying on Privacy Shield, identify an alternative.** As the EDPB makes clear, Privacy Shield is invalid with immediate effect. If you currently utilise it, you will need to put in place an alternative (e.g. SCCs or BCRs) or suspend transfers. SCCs are probably the practicable alternative. BCRs are more complex and may take anything up to 18-24 months to achieve approval. This, of course, may change as we gain further understanding of what additional safeguards may be required of controllers and processors.
- **Monitor guidance.** Neither the *Schrems II* judgment nor the EDPB guidance are clear as to how compliance can be achieved in relation to SCCs and/or BCRs, nor do the ODPA or JOIC provide any guidance on this issue (at this stage). Further guidance will be crucial in determining what (if any) measures will be sufficient.
- **Focus on the US but don't forget other countries.** The US is the only country that the ECJ has actually ruled on in *Schrems II*. However, the EDPB FAQ document makes it clear that the assessment obligation on data exporters and

importers applies to data transfers to any third country. Therefore, whilst the US should be the immediate priority, you should be considering international data transfers across the piece.

- **Start thinking about the "assessment" required when using the SCCs/BCRs:** whilst no definitive guidance currently exists, you should consider whether any of the jurisdictions to which you export (or intend to export) personal data may be problematic either from the viewpoint of State access to personal data or from serious gaps in local laws protecting personal data. You should then consider what measures could be put in place to address any risks which have been identified, such measures might include, for example:
  a. Technical measures, such as:
     1. Encrypting and/or tokenising data; and
     2. Greater use of remote access (which can be throttled or completely deactivated).
  b. Contractual measures to ensure that any legal or regulatory demands for access are communicated (where possible) to data exporters and are subject to appropriate scrutiny and (where necessary) challenge.
  c. Practical measures such as data minimisation and/or greater localisation.

Subscribe for more

FIND US

Carey Olsen (Guernsey) LLP
PO Box 98
Carey House
Les Banques
St Peter Port
Guernsey GY1 4BZ
Channel Islands

T +44 (0)1481 727272
E guernsey@careyolsen.com

Carey Olsen Jersey LLP
47 Esplanade
St Helier
Jersey JE1 0BD
Channel Islands

T +44 (0)1534 888900
E jerseyco@careyolsen.com

FOLLOW US

Subscribe for more

Visit our cybersecurity and data protection team at careyolsen.com

PLEASE NOTE