Brexit and Data Privacy

Barry Fishley, Briony Pollard & George Mole

16 December 2020

Enforcement Landscape – Europe

- Broadly still a complaints-driven regime but…
- Enforcement approach varies amongst Member States
- In the UK, it's not all fines:
  - 11.2% of investigations result in regulatory enforcement action
  - 0.7% of investigations result in a fine

Level of Fines I – Europe (Calculation)

- One of a number of measures including:
  - Enforcement notices requiring corrective action (or prevention is required) where there is a breach of GDPR principles e.g. consent
  - Information notices

- Serious breaches:
  - €20m or 4% of worldwide annual revenue
  - ICO fines should be effective, proportionate and dissuasive

- Factors include:
  - Nature, gravity and duration of failure
  - Intentional or negligent character of infringement

Level of Fines II – Europe (Examples)

- Google (and Amazon)
  - Fines: €100m (and €35m) (France, CNIL)
  - Issue: (i) cookies without consent, and (ii) insufficient information provided
  - Affected: 50m users of Google Search services for financial gain

- British Airways
  - Fine: £20m (UK, ICO)
  - Issue: Data breach caused by security failures
  - Affected: 30,000 customers

- Marriott International
  - Fine: £18.4m (UK, ICO)
  - Issue: Data breach caused by security failures
  - Affected: 30m customers

- Fines reduced from £183m and £99m, but why?

Level of Fines III – Europe (Lessons)

- Act quickly to mitigate impact on data subjects
- Robust legal and technical response
- Cooperation with the supervisory authority
- Building a relationship with the supervisory authority
- Median average ICO fine since November 2018: **£95,000**

Civil Claims Landscape – Europe

- Increased awareness will lead to increased civil claims

- Individuals can claim for financial and non-financial damages e.g. reputational damage, embarrassment, distress, inconvenience or anxiety

- There is an early growing trend in Europe for class-actions… British Airways, Cathay Pacific, EasyJet, Marriott

Use of Standard Contractual Clauses ("SCCs")

- *Schrems II* decision - Privacy Shield invalid
- SCCs valid but exporter must undertake case by case analysis of adequate level of protection
- EDPB adopted recommendations on Essential Guarantees and Supplementary Measures
  - Aim to assist data exporters with ensuring an equivalent level of protection
  - Consultation ends 21/12/20

Recommendations: Six Steps

1. Data Mapping – including onward transfers
2. Identify the transfer ‘tools’ for each transfer
    - Art. 45 - adequacy decision e.g. Andorra, Argentina, Canada, Guernsey, Isle of Man, Israel, Japan, Jersey, New Zealand, Switzerland and Uruguay
    - Art. 49 – explicit consent, contractual necessity, necessary in relation to legal claims
    - If 45 or 49 apply then no additional steps are required
    - ICO and EDPB - Art. 49 must be interpreted restrictively and may only relate to processing activities that are occasional and non-repetitive

Recommendations: Six Steps (Continued)

3. Art. 46 transfer tool e.g. SCCs or BCRs – is the protection essentially equivalent?
   - Must include an assessment of onward transfer
   - Assess the legal system in each third country in particular access by public authorities to EU data – use Essential Guarantees
   - Review by exporter must be assisted by importer and publicly available sources
   - *Schrems II* determined that US does not provide essentially equivalent protection therefore supplementary measures are required for US transfers

Recommendations: Six Steps (Continued)

4. Consider whether supplementary measures are required
   - unclear whether risk based approach can be taken but see ICO's statement - stipulates risk based approach to enforcement
   - additional contractual measures - e.g. obligation to notify of access request
   - technical measures – e.g. encryption
   - organisational measures e.g. data segregation

   - EDPB's view is that access to unencrypted data by cloud providers and remote access for business purposes by importers will always mean that data is not "essentially equivalently protection" – suspension/termination?

5. Take any formal procedural steps e.g. if seeking to amend SCCs need DPA approval
6. Re-evaluations at appropriate intervals
   - Exporters must monitor on an ongoing basis any development that could affect the initial assessment

New SCCs

- EC Commission issued draft SCCs in November 2020
- Consultation ended 10 December
- Aims
  - deal with different scenarios e.g. EEA processor to non-EEA controller
  - incorporate *Schrems II* supplementary measures e.g. transfer assessment in Clause 2
- Formal adoption of new SCCs requires an opinion of EDPB and positive vote by European Parliament
- Approval not expected before early 2021
- Likely UK will adopt broadly similar clauses particularly if UK receives an EC Commission adequacy decision

New SCCs (Continued)

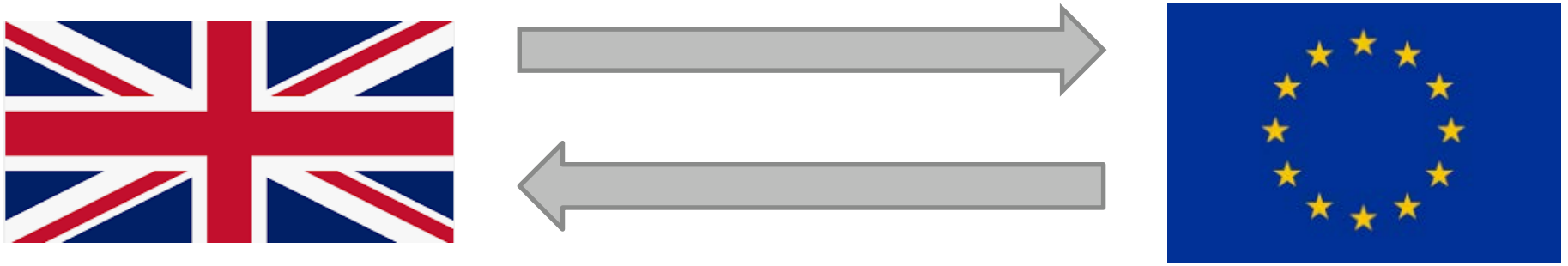
- Once adopted existing SCCs need to be replaced within 12 months – long enough?
- New SCCs:
  - modular approach e.g. C2C, C2P, P2P, P2C
  - may not be amended (directly or indirectly) – uncertainty?
  - C2C – non-EEA based importer – notify exporter and SA of data breach likely to result in significant adverse effects
  - obligations on non-EEA sub-processors to notify controllers – practical?
  - both importer and exporter need to undertake transfer impact assessment and an obligation on exporter to consult with SA
  - obligations to replicate protections on onwards transfer to other third country

Where does this leave us?

- Data mapping now! – which transfers are necessary?
- Review SCCs – prioritise key transfers
- Risk based assessment
  - types of data – client, customers, financials, special category
  - key vendors Q&A – can data be held in EEA? Additional measures?
- More diligence needed
- Re-visit derogations e.g. consent etc.
- EDPB is guidance
- ICO has not opined yet

No Deal Brexit – Impact on data transfers

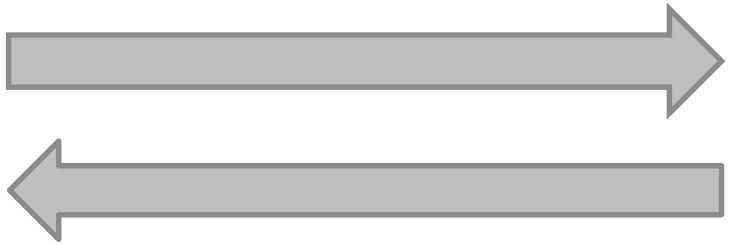
- Transfers from UK to EEA
  - Transitional adequacy decision in place



- Transfers from EEA to UK
  - No adequacy decision
  - Exception/derogation e.g. consent – only for occasional and non-repetitive transfers
  - Binding Corporate Rules
  - EU Model Clauses (SCCs) – consider *Schrems II*

No Deal Brexit – Impact on data transfers

- Transfers from UK to ROW (other than EEA)
  - Rely on the same mechanisms as under the GDPR i.e. adequacy, appropriate safeguards and exceptions
  - Consider *Schrems II*
  - Holders of EU BCRs where ICO not lead authority – eligible for UK BCR



- Transfers from ROW (non-EEA) to UK
  - Sender to ensure they are complying with rules that apply in their jurisdiction
  - UK entity to comply with data protections rules in UK

What happens if there is a deal?

- Anticipate that negotiations will go down to the wire, potentially until 31 December 2020
- No deal highly likely
- Possible outcomes:
  - EU may deem the UK an ‘adequate’ country meaning that transfers of personal data from the EEA to UK will be permitted without the need to rely on an exemption or additional safeguards; OR
  - No adequacy decision. EU deems SCCs sufficient provided the *Schrems II* risk assessment is conducted, as with other international transfers

What do I need to do?

- Privacy Policies and Notices
  - Update to reflect the revised position in relation to international transfers of data
- Review agreements with third party vendors
  - Update to ensure data is being transferred legally
- Consider whether to designate an EU representative
  - Required when offering goods and services to EEA and/or monitoring behaviour and no branch, office or establishment in the EEA. Not required if processing is occasional or low risk
- Identify lead supervisory authority - participate in the One Stop Shop
  - Established in UK and one EEA state – action could be taken by ICO and the EEA authority
  - Established in UK and two or more EEA states – EEA state with larger customer base would act as the lead authority; action could be taken by the EEA lead supervisory authority and ICO
  - No establishment in the EEA, but offer goods and services to EEA data subjects – no lead supervisory authority; action could be taken by all supervisory authorities where data subjects have been affected

Any questions/special topics?