2020 Hindsight: Clouds and the New Normal

Andrew Cormack, Chief Regulatory Adviser (@Janet_LegReg)

Topics/What changed?

- Schrems II case
  - How to export personal data
- EDPS Microsoft report
  - Looking at Cloud contracts
- COVID-19
  - Emergency and opportunity?

Jisc

Schrems II

C-311/18: DPC (Ireland) v Facebook Ireland & Max Schrems

How to export personal data from EU

Schrems II: European Court of Justice (ECJ)

- Question about Facebook exporting data IE => US
  - Covered by Standard Contractual Clauses (EU-approved: SCCs)
  - According to GDPR, satisfying exporter's responsibility to ensure adequate protection
- Court's response also considered Privacy Shield
- Fundamental issue
  - US law can override any contract with US data importer
  - National Security laws let US Gov't access data on cables and in some US data centres
  - Those laws do not provide adequate protection for EU data subjects
- NB this only affects data physically transferred outside European Economic Area (EEA)
  - …including, after 31st Dec, to UK

Jisc

Schrems II: Privacy Shield

- Bilateral EU/US Government agreement (2016)
- Replaced Safe Harbor (2000), declared invalid in *Schrems I*
  - Parallel sequence of Switzerland/US agreements
- Repeated doubts about adequacy of protection
  - Article 29 Working Party, European Parliament both have unsatisfactory periodic reviews
  - Exporters recommended not to rely on it
- ECJ not asked to rule on it, but does anyway:
  - Privacy Shield does not ensure adequate protection for exports
  - Invalid with immediate effect
- Commission immediately announces work on Mark III…

Jisc

Schrems II: Standard Contract Clauses (SCCs)

- Approved terms in contracts between data exporter and importer
  - Applies to any receiving country, not just US
- No formal doubts till ECJ gave broad analysis in Schrems I
  - Hint that receiving state legal system (if non-EEA) might be an issue
  - Many US exports moved to SCCs when Safe Harbor invalidated
    - Last option standing…
- ECJ ruling
  - SCCs *do* provide adequate protection from importer
  - Exporter/Regulator must decide if more is needed to protect from Gov't

Jisc

Schrems II: SCCs plus…What?

If needed, what might that protection be?

- Not contract, since that doesn't bind Government
- Maybe: Technology, e.g. encryption
- Maybe: Law of Importing state, e.g. FERPA?
- Or: Don't export!
- Back to DP Directive-style self-assessment of adequacy?
  - ht Chris Pounder/Amberhawk

Jisc

European Data Protection Supervisor:Microsoft contract report

Issues with cloud contracts

Review of Commission contract with Microsoft

NB Issues may be specific to that contract

- Does claimed status match functional relationship?
  - Does “Data Processor” claim rights that belong to a Controller?
- Check *all* data flows
  - Have you specified storage/processing locations?
  - Telemetry data mentioned in several reviews
- Ask about…
  - Technical controls (or 3rd party audit)
  - Transparency measures
- Don’t assume all contracts are same
- Don’t assume all providers are different

Jisc

COVID-19

Emergency and Opportunity?

Emergency Remote Teaching…

Short/medium/long-term response to COVID-19

- KluwerLaw blogs (short term)
  - Rapid adoption of new (cloud) services
  - Many with sub-optimal Data Protection and Intellectual Property clauses
  - But we couldn't have stayed open without them
  - Which risk is worse?
- Gartner idea (EUNIS 2020 conference): decide…
  - Which approaches/technologies we want to keep/improve (long term)
    - Future arrived 57 months early…
  - Which we want to revert/retire (medium term)
    - Conscious decision not to go that way
  - Define appropriate timescale, process, resources for each set…

Jisc

Summary

Things to look out for…

- (local) Regulator responses to Schrems II
  - How long to move off Privacy Shield?
  - How to assess additional measures needed for SCCs?
  - Is “export” law binary? Or risk-based?
- Cloud contracts – use EDPS report as a checklist
  - For internal discussion: which risks are greater than walking away?
  - For supplier discussion: how do you address EDPS requirements?
- Cloud procurements – be realistic
  - “Compliant” is too ill-defined to aim for (GDPR Art.28 is necessary but not sufficient)
  - Risk assessment/management is a realistic aim
  - Compare risks of in-house vs cloudA vs cloudB options

Jisc

References

- Schrems II
  - http://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=11527256
  - https://regulatorydevelopments.jiscinvolve.org/wp/2020/07/17/ecj-invalidates-privacy-shield-model-clauses-valid-but-may-not-be-sufficient/
  - https://regulatorydevelopments.jiscinvolve.org/wp/2020/07/29/schrems-ii-sccs-plus-what/
- EDPS Microsoft report
  - https://edps.europa.eu/sites/edp/files/publication/20-07-02_edps_paper_euis_microsoft_contract_investigation_en.pdf
- Kluwer Law on Emergency Remote Teaching
  - http://copyrightblog.kluweriplaw.com/2020/05/27/emergency-remote-teaching-a-study-of-copyright-and-data-protection-terms-of-popular-online-services-part-i/
  - http://copyrightblog.kluweriplaw.com/2020/06/04/emergency-remote-teaching-a-study-of-copyright-and-data-protection-policies-of-popular-online-services-part-ii/

Jisc

Andrew Cormack

Lumen House, Library Ave, Didcot OX11 0SG

01235 822200

Andrew.Cormack@jisc.ac.uk

jisc.ac.uk