International Data Transfers GDPR & beyond

Jan Tomíšek

Institute of Law and Technology

ROWAN LEGAL

Why do we deal with it

- Different regimes in different countries – different levels of protection
- Possible loophole – exported data might not be protected
- Data Transfers Rules – ensuring data are protected even when transferred abroad

- Conflict: adequate protection x free flow of data (one of the origins data protection law)

- Data sovereignty?

Sources

- OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data
- Convention 108 (updated)
- GDPR
- Other frameworks – APEC

Approaches

- Territorial – example: adequacy decisions
- Organizational – example: binding corporate rules

- Transfers x scope of application (extrateritoriality)

Data transfers under GDPR

- Free flows in the EU/EEA

- Transfers to „third countries“
  - Adequacy
  - Appropriate safeguards
  - Derogations

Adequacy

- Decision of European Commission on adequate level of protection in particular country/sector in country/international organization
- Current example: **Japan** (based on Framework for Mutual and Smooth Transfer of Personal Data between Japan and the EU effective on 23 January 2019)
- Assessment of
  - rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data,
  - the existence and effective functioning of one or more independent supervisory authorities
  - the international commitments the third country or international organisation concerned
- Monitoring, amendment, repeal or suspension
- Adequacy decision - Japan

Adequacy

- States providing adequate protection (as recognized by EC decisions)
  - Andorra
  - Argentina
  - Canada (commercial organizations)
  - Israel
  - Japan
  - New Zealand
  - Switzerland
  - Uruguay
  - USA (limited to Privacy Shield)
  - + smaller territories (Faroe Islands, Guernsey, Isle of Man, Jersey)

Safe Harbor

- Adequacy decision for US
- Not whole country, only certified companies
  - „Self-assessment“
- Enforcement by Federal Trade Commission – fraudulent representation if not committed to the principles

- Edward Snowden and PRISM affair

Schrems Ruling C-362/14

- Safe Harbor adequacy decision invalidated
- Individual data protection authorities entitled to review adequate level of protection in particular case, even despite adequacy decision

- adequate level of protection' must be understood as requiring the third country in fact to ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental rights and freedoms that is *essentially equivalent* to that guaranteed within the European Union by virtue of Directive 95/46 read in the light of the Charter (para 73)
- legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter (para 94)

Privacy Shield

- New „Safe Harbor“
- Around 5000 participating companies

- Principles
- Ombudsperson
- Dispute resolution
- Regular review
- Judicial redress for foreigners (Judicial Redress Act)

- Kuner, C. Reality and Illusion in EU Data Transfer Regulation Post Schrems, 18 German Law Journal 881 (2017) [full text]

Privacy Shield currently

- Privacy Shield is annually review and improved
- Third review took place recently (October 2019)
  - „*Enforcement action has improved with the Federal Trade Commission taking enforcement action related to the Privacy Shield in seven cases*.“
  - EC suggests strengthening the (re)certification process for companies who want to participate by shortening the time of the (re)certification process, expanding compliance checks etc.

- Pending case C-311/18 (*Schrems II*) before CJEU (not yet decided)
  - Full decision expected by early 2020
  - EC will assess consequences for the Privacy Shield

Appropriate safeguards

- Legally binding and enforceable instrument between public authorities or bodies
- Binding Corporate Rules
- Standard Contractual Clauses
- Codes of Conduct
- Certifications

- Subject to specific approval
  - Ad hoc contractual clauses
  - Provisions to be inserted into administrative arrangements

Binding Corporate Rules (BCRs)

- Intended for multinational corporations / groups of companies (currently +- 130 companies)
- Commitment to common policy through a legal act
- Policy meeting standards set by GDPR
- Serves for intragroup transfers but also receipt of data by the corporation

- Recommendation on the approval of the Processor Binding Corporate Rules form (wp265)
- Recommendation on the approval of the Controller Binding Corporate Rules form (wp264)
- Working Document on the approval procedure of the Binding Corporate Rules for controllers and processors (wp263rev.01)
- Working Document on Binding Corporate Rules for Processors (wp257rev.01)
- Working Document on Binding Corporate Rules for Controllers (wp256rev.01)

Codes of Conduct

- To be issued by professional organizations
- Detailing the provisions of GDPR for particular sector / association
- Independent monitoring body has to be specified
- To be approved by DPA / EDPB
  - **EDPB Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679**
- Organization commits to the code – compliance has to be certified by the monitoring body
- E.g.: Code of conduct for credit reporting systems operated by private entities regarding consumer credit, creditworthiness and punctuality in payments (not yet approved by EDPB)

Certification Schemes

- May be proposed by anybody
- To be approved by DPA / EDPB
- Certification by
  - DPA
  - Independent third party accredited by (upon choice of member state)
    - DPA
    - accreditation body
- **EDPB Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679**
- **EDPB Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679)**

Standard/Model Contractual Clauses

- Standard contract to be entered between data exporter (in the EU) and data importer (in the third country)
  - Controller to Controller
  - Controller to Processor
- Issued by the European Commission
- Other provisions may be agreed (typically MCC are signed in parallel with a data processing agreement), but must not be conflicting
- To be reviewed by CJEU in case C-311/18 (*Schrems II*)

Derogations

- Explicit consent, „after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards“
- Performance of a contract
  - between the data subject and the controller
  - concluded in the interest of the data subject between the controller and another natural or legal person
- Important reasons of public interest
- Establishment, exercise or defence of legal claims
- Vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent
- Transfer is made from a register which according to Union or Member State law is intended to provide information to the public
- **Escape clasue**: necessary for the purposes of compelling legitimate interests – only if transfer is not repetitive, concerns only a limited number of data subjects
  - The controller shall inform the supervisory authority and the data subject of the transfer.
- **EDPB Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679**

Open point – article 48

- Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognized or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, *without prejudice to other grounds for transfer pursuant to this Chapter*.

Challenges for future

- Privacy Shield Reviews
- Standard Contractual Clauses before CJEU (Schrems II case)
- US Cloud Act – European Commission engaged in negotiations with the US of an international agreement dealing with cross-border access requests to electronic evidence
  - According to EDPB such international agreement must contain sufficient adequate data protection safeguards

Summary

- Cornerstone of data protection laws
- Territorial and organizational approach
- Adequacy, appropriate safeguards, derogations
- In practice
  - Adequacy, including Privacy Shield
  - Model Contractual Clauses

Questions?

tomisek@rowan.legal