# JUR 5630 – 2010
# Lecture 8
# Interlegal aspects of data protection law
# (15th March 2010)

***Lee Bygrave***

## 1. Disposition

- Supplementary comments on monitoring and enforcement mechanisms
  - Self-regulation (e.g., USA)
  - Co-regulation (e.g., Australia)
  - Codes of practice (DPD Art. 27)
- Rules on applicable law
  - Focus on DPD Art. 4
  - Problems in Internet environment
- Rules on transborder data flow (TBDF)
  - Rules in early national laws
  - Rules in early international instruments
  - Rules in DPD
    - Art. 25
    - Art. 26
  - Main policy making bodies
  - Safe Harbor agreement
  - Standard Contractual Clauses
  - Binding Corporate Rules (BCRs)

## 2. Applicable law

- Main rule prior to DPD

  Applicable law = law of State where data file/register located

  Some exceptions, giving national laws considerable extra-territorial scope (e.g., Belgian law)
- Main rule in DPD Art. 4(1)

  Applicable law = law of State where data controller is established (Art. 4(1)(a))
  - Manifests so-called "country of origin" principle (also applied in other EU legislation)
  - Considerable benefits for data controllers, but …
  - What benefits, if any, for data subjects?

  What = established?
  - Establishment "implies effective and real exercise of activity through stable arrangements" (recital 20; cf. Case C-221/89 *Factortame*)
  - legal form not decisive (recital 19)
  - 3 criteria:
    1. exercise of activity
    2. stable organisational infrastructure
    3. relatively lengthy period

  What is situation with, say, multi-national corporation with subsidiaries established in multiple EU member states?
  - Importance of distinguishing between "controller" and "processor"
    - "controller" defined in DPD Art. 2(d); "processor" in DPD Art. 2(e)

- "The rule 'one company, one controller' does not apply" (Kuner) – NB. definition of "controller" permits shared responsibility (DPD Art. 2(d))
- Phrase "in the context of the activities of an establishment of the controller" *arguably* means that law of land of establishment only applies to processing of data that is substantially connected to local company's activity; if data processing by latter occurs exclusively for purposes (or benefit?) of company established elsewhere (even though local company also able to determine purposes and means of processing – i.e., ≠ "processor", as defined in DPD Art. 2(e)), no need to apply "local" law.
  - Precondition is that "foreign" law meets standards of DPD and, possibly, "local" law.
  - Support for this approach in Danish and Austrian law.
  - Still fairly easy to apply "local" law (b/c of ambiguity in provisions, "ordre public" factors etc.)

- Secondary rules in DPD Art. 4(1):

  These apply law of State when data controller not established there – Arts. 4(1)(b) & (c)
  - Art. 4(1)(b): State's law applies "by virtue of international public law"
  - Art. 4(1)(c): State's law applies if data controller (which is not established within EU) uses data-processing "equipment" situated in State (but not for mere transit)
- Many problems with Art. 4 generally:
  1. Interpretative difficulties – e.g., what = "place of establishment" in Internet context? what = "use of equipment" in Internet context?
  2. Conflict of laws because there might be more than one controller, each established in different States
  3. Regulatory overreaching in Internet environment – e.g., use of cookies may invoke rule in Art. 4(1)(c)
  4. How will data subject enforce his/her rights when foreign law applies and controller established in other State? Cf. DPD Arts. 4(2) & 28(6)
  5. Encouragement of "race to the bottom"?

## 3. Regulation of TBDF

- Background:
  - National data protection laws of 1970s
  - fear of "data havens"
  - fear that data protection would hinder TBDF and hence trade
  - (American) assertions that data protection = economic protectionism
    - Assertions refuted subsequently
- International instruments:
  - CoE Convention (1981) Art. 12 – "equivalent" protection
  - OECD Guidelines (1980) para. 17 – "equivalent" protection
  - UN Guidelines (1990) principle 9 – "comparable" / "reciprocal" protection
  - Cf. APEC Privacy Framework (2004/05) Part IV(B) (says nothing directly about personal data exports – either in terms of limitation rules or requirements to allow them)
- DPD:
  1. TBDF within EU/EEA:
     - Art. 1(2) – prohibition on restricting TBDF for privacy protection reasons
  2. TBDF *from* EU/EEA *to* "third countries":
     - Art. 25(1) – TBDF permitted if third country offers "adequate" protection
       - All circumstances to be taken into account

- Exceptions pursuant to Art. 26
  - consent, legal duty, contract with d.s., protect vital interests of d.s., protect important public interests, etc.

- DPD Arts. 25 and 26 –problems of legal interpretation: e.g. …
  1. What = adequate?
  2. What = necessary?
  3. What = legal obligation?
  4. What = transfer?
     - Cf. ECJ decision in *Lindqvist*, Case 101/01, 6.11.2003
- DPD Arts. 25 and 26 – who determines what?
  1. Data controllers
  2. National DPAs
  3. EU Commission (with Art. 31 Committee) (makes binding decisions on adequacy, DPD Art. 25(6))
  4. Article 29 Working Party (advisory power only but has laid down principal criteria for assessing adequacy)
  5. European Parliament (checks whether Commission has used powers properly)
- Relatively few adequacy determinations made; lengthy process (e.g., assessment of Australia) – too cumbersome?
- Note problems with PNR data agreement between EU and USA – first agreement struck down by ECJ for being ultra vires: judgment of 30 May 2006 in Joined Cases C-317/04 and C-318/04, *European Parliament v. Council of the European Union and Commission of the European Communities*.
- Problems identified by Commission (*First report on the implementation of the Data Protection Directive (95/46/EC)*, COM(2003) 265 final, Brussels, 15th May 2003):
  - divergent and inconsistent national implementation of Arts. 25–26
  - much TBDF not subjected to any regulation.
- Conflict with GATS (1994)?
  Exception for privacy in Art XIV(c)(ii)
- Safe Harbor – USA as legitimate "data haven"?
  See article by Bender & Ponemon (class handout – fully referenced below).
  Can one expect similar agreements with other countries?
  Unlikely, cf. potential discrimination concerns
- Other (partial) means of achieving "adequacy"
  1. Standard contractual clauses
     - See Commission decisions 2010/87/EU, 2004/915/EC and 2002/16/EC, all available via <http://ec.europa.eu/justice_home/fsj/privacy/modelcontracts/index_en.htm>
  2. Binding Corporate Rules
     - Only facilitate TBDF within particular corporate group
     - Still developing as legal mechanism
     - Criteria published by Art. 29 Working Party
     - National DPA = main decision-maker
     - Poor uptake to date; largely utilised only by large multinationals
     - Many countries (e.g., Italy, Austria, Netherlands) still require post-BCR approval by national DPA of data transfers; preparation of BCR application is complex

       See further, e.g., Bender & Ponemon, "Binding Corporate Rules for Cross-Border Data Transfer", *Rutgers Journal of Law & Urban Policy*, 2006, vol. 3:2, pp. 154–171, available at

<http://www.rutgerspolicyjournal.org/journal/vol3no2/Bender_Ponemon_Cross_Border_Data.pdf>; Kuner 2007, pp. 218–232; Brooks, "BCR concepts – post-approval requirements and other challenges", *Privacy Laws & Business ( UK Newsletter*), 2010, issue 47, pp. 15–7.