JUS5630 – 2013
Lecture 4 & 5
Regulatory logic of data protection laws (I–II)
(28th February & 7th March)

Lee Bygrave

1. Disposition

- Core principles of data protection laws
  - Fair and lawful processing
  - Proportionality
  - Minimality
  - Purpose specification and limitation
  - Information quality
  - Data subject participation and control
  - Disclosure limitation
  - Information security
  - Sensitivity
  - Other principles?

2. Nature of "principles"

- Abstractions denoting pith of legal rules, but …
- have normative force of their own:
  1. express incorporation as rules
  2. guiding standards in interest-balancing processes
  3. shape drafting of legislation

3. Fair and lawful processing

- Primary principle (DPD Art. 6(1)(a))
- "Fairness" is difficult to define in abstract but probably implies
  1. Balance
  2. Proportionality
  3. Transparency (cf. pDPR Art. 5(a))
  4. Direct collection
  5. Account of data subjects' reasonable expectations
     - Cf. British Gas Trading case
  6. Protection from undue pressure / abuse of monopoly
- Account only of data subjects' interests?

4. Proportionality

- In EU law, proportionality principle (PP) is generally recognized as having three prongs: (i) suitability – is measure concerned suitable or relevant to realizing goals it is aimed at meeting?; (ii) necessity – is measure concerned necessary (indispensable) to realizing goals it is aimed at meeting?; and (iii) non-excessiveness (proportionality *stricto sensu*) – does measure go further than is necessary to realize goals it is aimed at meeting?
- DPD Articles 6(c) ("relevance", "not excessive"), 7, 8 & 13 ("necessary") manifest PP – recognized too by CJEU in *Rechnungshof* decision (particularly para. 91)PP increasingly recognized as core data protection principle in its own right.
- For recent examples of PP operationalized in CJEU caselaw, see decision of 9.11.2010 in Joined Cases C-92/09 (*Volker und Markus Schecke GbR*) and C-93/09 (*Hartmut Eifert*). See too decision of 24.11.2011 in Case C-70/10 (*Scarlet Extended v SABAM*), and decision of

16.2.2012 in Case C-360/10 (*SABAM v Netlog*).
- For general analysis, see Bagger Tranberg 2011.

5. Minimality

- Manifest in DPD Arts. 6(1)(c), 6(1)(e),7, 8 (cf. pDPR Art. 5(c) and (e), Art. 23)
- Hinges largely on "necessity" criterion, which is not defined in DPD. Bygrave (2002) argues that criterion may be construed according to case law on ECHR Art 8(2):
    1. Pressing social, political or commercial need; AND
    2. Proportionality / non-excessiveness

  However, CJEU in Case C-524/06 *Heinz Huber v. FRG* [2008] ECR I-9705 held that "necessary" in DPD Article 7(e) "is a concept which has its own independent meaning in Community law and which must be interpreted in a manner which fully reflects the objective of that directive, as laid down in Article 1(1) thereof" (para. 52). Further, the necessity criterion in Article 7(e) is met if the processing leads to enhanced effectiveness – i.e., "necessary" ≠ indispensable: "with respect to the necessity that a centralised register such as the AZR [Ausländerzentralregister] be available in order to meet the requirements of the authorities responsible for the application of the legislation relating to the right of residence, even if it were to be assumed that decentralised registers such as the district population registers contain all the data which are relevant for the purposes of allowing the authorities to undertake their duties, the centralisation of those data could be necessary, within the meaning of Article 7(e) …, if it contributes to the more effective application of that legislation as regards the right of residence of Union citizens who wish to reside in a Member State of which they are not nationals" (para. 62; see too para. 66).
- May give rise to principle of anonymity / pseudonymity
    - Not prominent in DPD
    - Cf. DPEC, preamble, recital 30: "Systems for the provision of electronic communications networks and services should be designed to limit the amount of personal data necessary to a strict minimum" (cf. pDPR Art. 23)
    - Cf. Germany's *Bundesdatenschutzgesetz* § 3a
    - Cf. Australia's *Privacy Act 1988* (Cth) NPP 8
    - PET usage?

6. Purpose specification and limitation ("finality")

- Manifest in DPD Art 6(1)(b)
- 3 separate principles:
    1. need to define purposes for processing in specific way (cf. pDPR Art. 5(b) – adds "explicit")
    2. purposes must be lawful/*legitimate*
        - Does this embrace *social justification* principle?
        - If so, is justification to be defined in basically procedural terms or also substantive?
    3. secondary purposes must not be incompatible with primary purposes
        - Does "not incompatible" = less stringent standard than "compatible"?
        - Account to be taken of data subjects' reasonable expectations?

7. Information quality

- See, e.g., DPD Art. 6(1)(c), 6(1)(d))(cf. pDPR Art. 5(c) and (d))
- Multifaceted; variation in terminology
- key criteria: validity, relevance, completeness
- variation in terms of stringency of monitoring requirements
- insufficient focus on quality of *information systems*?

8. Data subject participation and control

- duties of information/orientation (DPD Art. 10-11)
  NB. special rule in Norwegian and Icelandic laws with respect to profile use and video surveillance
- duties to collect data directly from data subject
- duties of consent (DPD Art. 7 & 8)
  NB. issue of normative primacy of consent
- opt-in vs. opt-out issue; explicit vs. implicit consent
- access and rectification rights (DPD Art. 12)
  NB. access to logic in automated decisions
- rights to object to direct marketing and automated decision making (DPD Art. 14 & 15)

9. Disclosure limitation

- Minimum rule: data should not be disclosed except with consent of data subject or by authority of law
- Not separate principle in DPD but o/wise important (see, e.g., OECD Guidelines – "use limitation" principle)

10. Information security

- See, e.g., DPD Art. 17
- Does Art. 17 encourage usage of PETs?
- Cf. special rule on wartime planning in Danish law

11. Sensitivity

- See, e.g., DPD Art. 8 and CoE Convention Art. 6
- A principle in its own right?
- A practicable principle?
- Not strongly manifested in all jurisdictions, particularly those o/side Europe (but this is changing a little)

12. Other principles?

- Anonymity?
  - Arguably yes in DPD; more definitely in German and Australian laws on point
- Privacy by design?
  - Not much in DPD; more in German laws («Systemdatenschutz»)(cf. pDPR Art. 23)
- Automated decision making?
  - Arguably yes in DPD (*viz*. Art. 15(1))(see also pDPR Art. 20)
- "Openness" (OECD Guidelines); "Transparency" (pDPR Art. 11)
- "Preventing Harm Principle" (APEC Privacy Framework)
- "Accountability" (OECD Guidelines; pDPR Art. 5(f), chapt. IV)