

JUS5630 – 2013
Lecture 6
Regulatory logic of data protection laws (III)
(14th March 2013)

Lee Bygrave

1. Disposition

- Data Protection Authorities
- Other regulatory agencies
- Licensing / notification schemes
- Courts

2. Data Protection Authorities (DPAs)

- Main requirements of DPAs (see DPD Art. 28; CoE Convention Additional Protocol Art. 1):
 1. complete functional independence
 - See CJEU decision of 09.03.2010 in Case C-581/07, *Commission v FRG* ((holding that supervisory authority does not have requisite independence for purposes of Article 28(1) when it is subject to State scrutiny; a supervisory authority must have “complete independence” which implies “a decision-making power independent of any direct or indirect external influence on the supervisory authority” (para. 19), and “the mere risk that the scrutinising authorities could exercise a political influence over the decisions of the supervisory authorities is enough to hinder the latter authorities’ independent performance of their tasks” (para. 36); DPAs in German *Länder* found not to be completely independent as required by DPD Article 28(1) b/c they were subject to state scrutiny); cf. Opinion of Advocate General Mazák of 22.10.2009.
 - See too CJEU decision of 16.10.2012 in Case C-614/10 *Commission v Austria* (organisational overlap between Datenschutzkommission (DSK) and Federal Chancellery meant breach of DPD Art 28(1)).
 - The CJEU case law is reflected in pDPR Art 47.
 2. variety of tasks with broad discretionary powers
 - reporting, monitoring, complaints handling, rule development, enforcement; intervention
 - must be more than mere ombudsmen (?)
 - what = “effective powers of intervention”?
 - increasing need for cross-jurisdictional expertise (DPD Art. 28(6))
- Existence of “independent” DPA = part of “new” right of data protection in EU system – see EU Charter of Fundamental Rights (2000) Art. 8(3) (cf. TEU Art. 6(1)); TFEU Art. 16(2)
- DPAs at different levels and with different competences
 1. National (e.g., Norwegian Data Inspectorate (Datatilsynet), UK Information Commissioner (covering also FOI)
 - Note special relationship between data protection and FOI
 2. Sub-national (e.g. in federal systems, such as FRG and Australia)
 3. Regional (e.g., Art. 29 Data Protection Working Party (advisory competence only))
 4. EU (European Data Protection Supervisor (controls EU institutions only; see further Regulation (EC) 45/2001 of 18.12.2000 on the protection of individuals with regard to the processing of personal data by the institutions and bodies of the Community

and on the free movement of such data (OJ L 8, 12.1.2001, p. 1 *et seq.*); gives effect to TFEU Art. 16(2). NB. EDPS can issue legally binding orders; these can be appealed to ECJ: see further H. Hijmans, “The European Data Protection Supervisor: The Institutions of the EC Controlled by an Independent Authority”, *Common Market Law Review*, 2006, vol. 43, pp. 1313–1342)

- Growing “internationalisation” of DPA activity – e.g., ...
 - DPD Article 28(6) (European national DPAs to cooperate with each other); see too pDPR Arts 55–56 on ‘mutual assistance’ and ‘joint operations’, plus Art 57ff on ‘consistency mechanism’
 - Art. 29 Data Protection Working Party, http://ec.europa.eu/justice/data-protection/article-29/index_en.htm
 - See further, e.g., Y. Poullet & S. Gutwirth, “The Contribution of the Article 29 Working Party to the Construction of a Harmonised European Data Protection System: An Illustration of ‘Reflexive Governance’?”, in Maria Verónica Pérez, Asinari and Palazzi, Pablo (eds.), *Défis du droit à la protection de la vie privée / Challenges of privacy and data protection law* (Brussels: Bruylant, 2008), pp. 569–609.
 - pDPR Art 64 replaces A29WP with ‘European Data Protection Board’, though latter has much the same competence as former
 - International Working Group on Data Protection and Telecommunications, <http://www.datenschutz-berlin.de/content/europa-international/international-working-group-on-data-protection-in-telecommunications-iwgdpt>
 - Asia-Pacific Privacy Authorities (APPA), <http://www.privacy.gov.au/international/appa/>
 - OECD’s Recommendation on Cross-Border Co-operation in the Enforcement of Laws Protecting Privacy (adopted 12 June 2007)

3. Other regulatory agencies

- Other bodies can have relevant role: e.g., ...
 1. Federal Trade Commission (USA) – with respect to deceptive trade practices and Safe Harbor scheme
 2. European Parliament (EU) – increased powers pursuant to Lisbon Treaty
 3. Financial Services Authority (UK)
 4. Post- and Telecommunications Authority (Post- og teletilsynet, Norway) – with respect to electronic communications
 5. Internal privacy/data protection officers (not really “regulatory agency”) – compulsory under German and NZ dp law; also under pDPR Art 35 for public authorities, private enterprises with more than 250 employees, or bodies engaged in ‘regular and systematic monitoring of data subjects’.

4. Licensing / notification schemes

- Licensing = prior approval req’d from DPA
- Notification = prior notification of DPA req’d
 - Rationales: (i) Ex ante control; (ii) Transparency; (iii) Contact between controllers and DPAs; (iv) Learning / sensory mechanisms
- Balance under DPD (Arts. 18-20): notification = main rule; licensing = exception (recital 54); cf. earlier regimes (e.g., Norway, Sweden, France)
- Exemption from notification if internal data protection officer appointed (Art. 18(2))
- Problems with licensing:
 - Overly bureaucratic
 - Divergence in EU/EEA (e.g., Norway vs. Sweden)
 - But some advantages ...

5. Courts

- Role of judiciary and quasi-judicial bodies?

In many jurisdictions, role has been relatively marginal (see further L.A. Bygrave, “Where have all the judges gone? Reflections on judicial involvement in developing data protection law”, in P. Wahlgren (ed.), *IT och juristutbildning. Nordisk årsbok i rättsinformatik 2000* (Stockholm: Jure AB, 2001), pp. 113–125).

What consequences does this entail?

Note, though, increasing jurisprudence of CJEU; and Norwegian Supreme Court has recently issued judgment dealing directly with PSP in popplyl § 11: HR-2013-00234-A (sak nr. 2012/1334).

6. Supplementary comments on monitoring and enforcement mechanisms

- Self-regulation (e.g., USA)
- Co-regulation (e.g., Australia)
- Codes of practice (DPD Art 27; pDPR Art 38)