

# Promising Themes for Reform

**Richard Thomas**

**UK Information Commissioner**

**European Privacy and Data Protection  
Commissioners' conference**

**Edinburgh – 24 April 2009**

# Strengths of the EU approach

- Sets out basic framework of protection, drawing on OECD and Council of Europe approaches
- “High” standards, with Human Rights resonance
- Flexible, robust Principles
- Important and usable access and other rights
- Technology neutral
- Significant success in harmonising DP rules and promoting an internal market
- Reference model for good practice
- Some international success – e.g. SWIFT, Search Engines.

# General weaknesses of the EU approach

- Outdated – in terms of technology and modern regulatory approaches (“Mainframe Directive”)
- Unclear objectives
- Insufficient focus on detriment, risk and (especially) ***application in practice***
- Not enough choice and control for people
- Excessively bureaucratic and burdensome
- Too prescriptive – (“How?” not “What?”)
- Captured by “experts”: Too remote from citizens
- “Words, not Actions”
- Overall, not sufficiently Effective in practice

# Specific weaknesses of the EU approach

- Notification = burdensome and poor transparency tool
- Prior authorisation/approval = old-fashioned and unrealistic regulatory tool
- Detailed conditions for processing = excessively rigid control mechanism
- Static concepts and definitions (e.g. controller / processor; scope)
- Need integrated approach for 1<sup>st</sup> and 3<sup>rd</sup> Pillars
- Outmoded, and unrealistic data export rules

# Global context

- Reality of Globalisation – economic, technological, social
- 21st Century themes for regulating the privacy and integrity of personal information:
  - Trust, confidence, transparency, governance and accountability
  - Privacy as reputational issue for businesses and governments
- Pressures and changes inside China, India, USA
- and elsewhere
- APEC Privacy Framework = source of new thinking, not competitive “threat”

# Eight promising avenues for new EU approach

1. Explicit focus on outcomes - reducing risks of adverse effects to (a) Individuals and (b) Society
2. Clear Standards which organisations must achieve
3. Hold organisations to account for failure to achieve Standards in practice
4. Genuine transparency
5. Convert Notification to Registration
6. Greater clarity for Commissioner role
7. Improved Enforcement
8. Modernise export rules

# 1(a). Outcomes: Risks of adverse effects to individuals

- Risks to fundamental rights and freedoms
- Harm because personal information is:
  - inaccurate, insufficient, or out of date
  - excessive or irrelevant
  - kept too long
  - disclosed to wrong people
  - used in unacceptable or unexpected ways
  - not kept securely

# 1(b) Outcomes: Risks of adverse effects to Society

- Risks to fundamental rights and freedoms
- Harm to society where improper use of personal information results in:
  - excessive intrusion into private lives
  - loss of personal autonomy or dignity
  - arbitrary decision-making, stigmatisation or exclusion
  - excessive governmental or organisational power
  - climate of fear, suspicion or lack of trust

# 2. Internationally accepted Standards

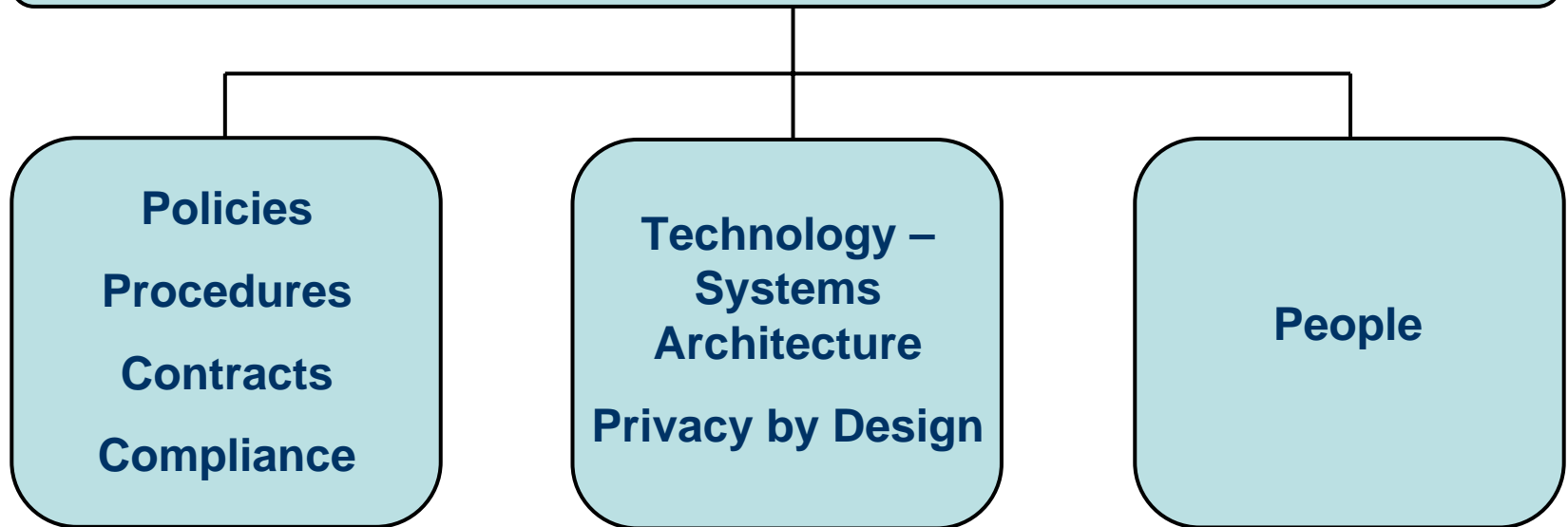
- Collection, use or disclosure based on genuine consent, legal requirement or reasonable expectations
- Duty of care for integrity of personal information
- Purpose limitation / data minimisation / proportionality
- Transparency of processing
- Limitations on retention and onward disclosure
- Accuracy
- Security
- User-friendly access to own information
- Effective arrangements for compliance, complaint and redress

# 3. Holding organisations to account

- Organisations held to account for fulfilling privacy policies, which meet legal requirements, but in ways best-suited to the organisation
- Primary responsibility on organisations and their senior leaders
- DP = top-level Governance issue

# Reputation and Regulation matters for the Board

## Governance and Accountability



## 4. Genuine Transparency

- Privacy by Design / Privacy Impact Assessments
- Privacy Policies
- 3<sup>rd</sup> party Certification
- Self-Certification?
- Right Notice to right people at right time

# 5. From Notification to Registration

- Basic corporate details
  - to identify entity for efficient and effective enforcement
  - to provide electronic and other communication channels for Commissioner advice and messages
- Fee
  - to increase Commissioner funding
  - to improve Commissioner independence

# 6+7. Strategic Commissioners and improved enforcement

- Selective as Teacher, Ombudsman & Policeman
  - Improved Enforcement
    - Commissioner monitoring, challenge and meaningful sanctions
    - especially for deliberate or reckless failure
- + direct liability and group actions

## 8. Modernise export rules

- Genuine Adequacy (not Equivalence) test
- Focus on corporate practice, not theoretical rules – e.g. real redress for individuals
- Certified Binding Corporate Rules
- Full responsibility on data exporters



**Information Commissioner's Office**

[www.ico.gov.uk](http://www.ico.gov.uk)