30/09/2015

Information Security and the (draft) Data Protection Regulation

Andrew Cormack, Chief Regulatory Adviser, @Janet_LegReg

Where are we?

- 1995 Data Protection Directive needs replacing
- Currently three drafts from different EU bodies
  - COM: European Commission (2012)
  - PAR: European Parliament (2014)
  - COU: Council of Ministers (2015)
- Each ~200 pages; 90+ articles (1995 Directive has 34)
- Trilogue process to agree a single text (by end 2015?)
- In force across EU ~18 months thereafter

Caveat

- Following is based on *drafts*
- Many significant differences between them
- Possible to pick out themes
  - From uncontentious areas
  - And those where there is disagreement

Good News (mostly) for InfoSec

Privacy Assessment/Design

- Privacy Impact Assessments (for some systems) (Art.33)
  - Assess/mitigate risks to individuals' rights and freedoms
  - Consult with them (for high-risk processing)
- Data Protection by Design & Default (Art.23: COM/PAR)
  - Plan compliance/InfoSec when designing systems
  - Minimise data & storage; access control; etc.
- Both require early InfoSec thinking

Incident Response

- Regulation recognises it's a "legitimate interest" (Rec.39)
  - Extends supportive wording in Telecoms Directive
  - LegInt requirements support CSIRT good practice
  - See references for details
- Security breach notification (at least to regulator) (Art.31)
  - Fixed time limits (24-72 hours COM/COU) unhelpful
  - But does support you having a detect/respond process

Bad News for InfoSec

Increased Harmonisation?

- Supposed effect of a Regulation versus a Directive
- But "One law for Europe" seems unlikely
  - Current variants (e.g. on basis for exports) still there
  - COU draft is 1/3rd derogations
- One-stop-(local)-shop promise
  - For both data subjects and data controllers…

Internet aware?

- Many internet issues not addressed
  - "IP address is personal data"
    - Trend towards: anything where one record = one person
    - But implications of that not recognised (e.g. SAR, DBN, export)
    - COU draft does try (clumsily) to encourage indirect identifiers
  - Physical location of data (not sysadmin) still king
- Little change to 1995 treatment of cloud etc.
  - Unless service directly provided to consumer
  - IaaS (if data processor) has direct security responsibilities

Compliance?

- Trilogue may well introduce further inconsistencies
  - Many paradoxical requirements already
  - Particularly where Internet concerned
- Probably aim to "manage risk" not "comply" ☹
  - "How can X comply?" will often have no answer

Next steps

Things to do

- Review/improve current practice
  - ICO says existing compliance will be a good start
- Look for (UK) regulator guidance/enforcement
  - ICO pretty clueful about internet issues
- I'll try to blog/tweet things of interest

Find out more…

Andrew Cormack
Chief Regulatory Adviser

Andrew.Cormack@jisc.ac.uk
jisc.ac.uk
@Janet_LegReg

Blog posts

Latest drafts (25/6/15): https://community.jisc.ac.uk/blogs/regulatory-developments/article/data-protection-regulation-now-there-are-three

DP and incident response (19/6/15): https://community.jisc.ac.uk/blogs/regulatory-developments/article/protecting-privacy-through-incident-response

IR as legitimate interest (6/6/12): https://community.jisc.ac.uk/blogs/regulatory-developments/article/privacy-and-incident-response

Feasibility of compliance (18/5/15): https://community.jisc.ac.uk/blogs/regulatory-developments/article/data-protection-developments-how-cope

Updates on DPR (ongoing): https://community.jisc.ac.uk/blogs/regulatory-developments/tags/Data-Protection-Regulation