UiO : Institutt for privatrett
Det juridiske fakultet

Lee A. Bygrave, Norwegian Research Center for Computers and Law

# The EU General Data Protection Regulation as Security Instrument: Strengths and Shortcomings

[SIGNAL Symposium 2017]

# Enter the hairy beast!

# Basic regulatory approach

- Risk-oriented
- Preventative focus
- Emphasis on accountability
  - Not just controllers but also processors

# Main security requirements

- Primary obligations in Art. 32
  - more prescriptive; less discretionary than DPD
  - but note contextual qualifications in Art. 32(1)!
  - embrace not just classic CIA criteria but also *resilience* (Art. 32(1)(b))
- Note requirement for regular testing and evaluation of security (Art. 32(1)(d))
- Note too role envisaged for codes of conduct and certification

# Data breach notification

- Mandatory notification of ‘personal data breaches’ (defined in Art. 4(12)) (new!)
- Two aspects:
  - 1) notification to DPAs (Art. 33)
    - 72-hour (!) deadline for reporting (‘where feasible’ and likelihood of risk to rights and freedoms of data subjects)
  - 2) notification to data subjects (Art. 34)
    - only when likelihood of ‘high risk’ to data subject rights and freedoms
    - note also derogations – e.g., disproportionate effort; technical/organisational measures applied (encryption); more general derogations under Art. 23

# New(ish) roles and liabilities

- Joint controllers (Art. 26)
- Full liability for each joint controller (Art. 82(4); cf. Art. 82(5))
- Liabilities for processors (Art. 82)(new!)
- Potentially stringent sanctions
  - Article 83(4): up to EUR 10 million or 2 % annual turnover (new!) (not highest level of sanctions, but still high; uncertainty as to what = ‘undertaking’; recital 150 suggests application of competition law criteria for assessing fines)

# Data protection by design and default

- GDPR Art. 25 (new!)
  - Two aspects:
    - 1. 'by design'
    - 2. 'by default'
  - Cp. 'Privacy by design'
  - Cp. 'data prot. impact assessment' (Art. 35)(new!)
  - Note too similar req.s in Art. 89(1) for 'scientific research'
- Security dimension espec. in Art. 25(2)!

# GDPR Art. 25(2): dp by default

Art. 25(2): 'The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.'

# Don’t forget the judiciary!

# Judicially imposed security

- *I v Finland* (2008) – ECtHR
  - implementing technological measures to ensure confidentiality of pasient data is positive obligation under ECHR Art. 8
- *Digital Rights Ireland* (2014) – CJEU
  - implies that ‘essence’ of right in EUCFR Art. 8 requires adoption of ‘ technical and organisational measures’ to ensure ‘effective protection against ‘risk of abuse and against any unlawful access and use’