Big Data, privacy and data protection –
An introduction to the challenges of the incoming European legal framework

Dr. Audrey Guinchard (Essex)
Current legal framework

- Started at international level with guidelines as early as 1973 – EU was the last to adopt a framework
- Current at EU level: “data protection” directive 1995/46/CE
  - directive = to be transposed by States who have to adopt their own laws to do so
Future legal framework

- EU Regulation (GDPR):
  - Probably in 2015. Voted in March 2014 by Parliament – Commission cannot amend substantially = only minor differences
  - It is a REGULATION =
    - immediately applicable with no national law to transpose it,
    - and hardly any margin of interpretation
  - NO NATIONAL LAW will be needed
Philosophy – approach to DP

DPD 1995/ DPA 1998
- Privacy = a private good, centered on the individual
- Rights given to individuals
- Very light duties on controllers and processors
- Hardly any sanctions/ penalties

GDPR 2015
- Privacy = a public good, beyond the individual
- More rights given to the individual
- Privacy by Design & by Default
- Huge fines = as big as in fin. markets
- Heavy involvement of controllers and processors

Essex Summer Science School
# Implementation of philosophy

**Justice must be done**

- Legal requirements to ensure compliance

## Consent

## Right to access (but fee)
- Right to rectify
- Right to erase
- Right to object to profiling
- Right to block data if unlawful
- Right to notify third parties

## Purpose:
- Qualified purpose for processing
- Proportionality of purpose (fairness)

## Accuracy of data set

## Proportionality in time

## Unambiguous consent
- No click & wrap
- No pre-ticked boxes
- Difference between Terms & conditions, AND privacy policy

## Right to access (no fee) – as before

## Additional rights:
- Data portability
- To be forgotten
- To object to processing & profiling
- To request human intervention

## Purpose: Privacy BY DEFAULT
- Data MINimisation as qualified purpose
- Proportionality of processing

---

Essex Summer Science School
Implementation of philosophy

Justice must be SEEN to be done

- Legal mechanisms to ensure visibility of compliance

1. DP impact assessment
2. Certification (more constraints than current ICO registration)
3. European Data Seal
4. DP officer = guardian
5. Auditing obligations – periodic review
6. Communications with individuals (art. 12 & 19; reporting & informing breaches)
7. Mandatory cooperation between supervisory authorities
Triggers

- An individual (not a legal person)
- Only if personal data:
  - the person is identified or can be identified
  - => Risks of de-pseudonymisation?
  - => Risks of de-anonymisation?
- Special protection if sensitive personal data
- => FOR EVERY TYPE OF DATA SET YOU COLLECT
- Who? Anybody with core activity (5000 pers.)
- E.g.: epsrc project: digital prosumer
Additional legal frameworks

- EC Directive on metadata (spatial) 12 May 2008
- Directive 2009/136/EC on cookies
- EC Unfair terms directive
- Freedom of information act (UK)
- Future cloud computing legislation

If publicly available electronic communications providers involved:

- Reg 611/2013 on Data Breach notification
- Data retention directive 2006/24 declared illegal in 2014