The once-only principle
Privacy, data protection and trust

Jesper Lund
jesper@itpol.dk

IT-Political Association of Denmark
(member of EDRi)

SCOOP4C Workshop
Brussels, 26 April 2018

IT-Political Association

- Danish digital rights NGO
- Member of European Digital Rights (EDRi)
  - EDRi is an association of 39 civil and human rights organisations in Europe
- IT-Pol and EDRi work on
  - Data protection (GDPR and ePrivacy)
  - Surveillance and security
  - Once-only (in 2015 EDRi analysis of DSM)

The once-only principle

- EU eGovernment Action Plan 2016-2020
  - *Public administrations **should ensure that citizens and businesses supply the same information only once** to a public administration. Public administration offices take action if permitted to **internally re-use this data, in due respect of data protection rules.***
- Reduce burden for citizens and businesses
- More efficient (cheaper) public administration

Implementation of once-only

- The public sector as one controller?
  - All personal data about citizens stored in the same public-sector system
  - Purpose limitation and data minimisation
- Linkages between different systems
  - At citizen's request, personal data can be transferred from public service A to B
  - One way to facilitate this: **single citizen ID** used in all public-sector systems (like Denmark)

Once-only and data protection

- Centralised data sharing with the citizen's consent can also be done without consent
- In due respect for data protection rules..
  - Legal basis for processing in the public sector is generally national law, not consent
- Data protection risks
  - Personal data may processed for new purposes or shared with other controllers (public services)
  - Once-only will make this easier and inevitably more tempting for the public sector

Motivation for the public sector

- Profiling citizens
  - Fight against tax evasion or welfare fraud
  - Predictive social services or health care that use all available information about the citizen or family
- AI and automated decision making
- Data-driven new technologies (“big data”)
- Reduce public expenditure

The transparent citizen

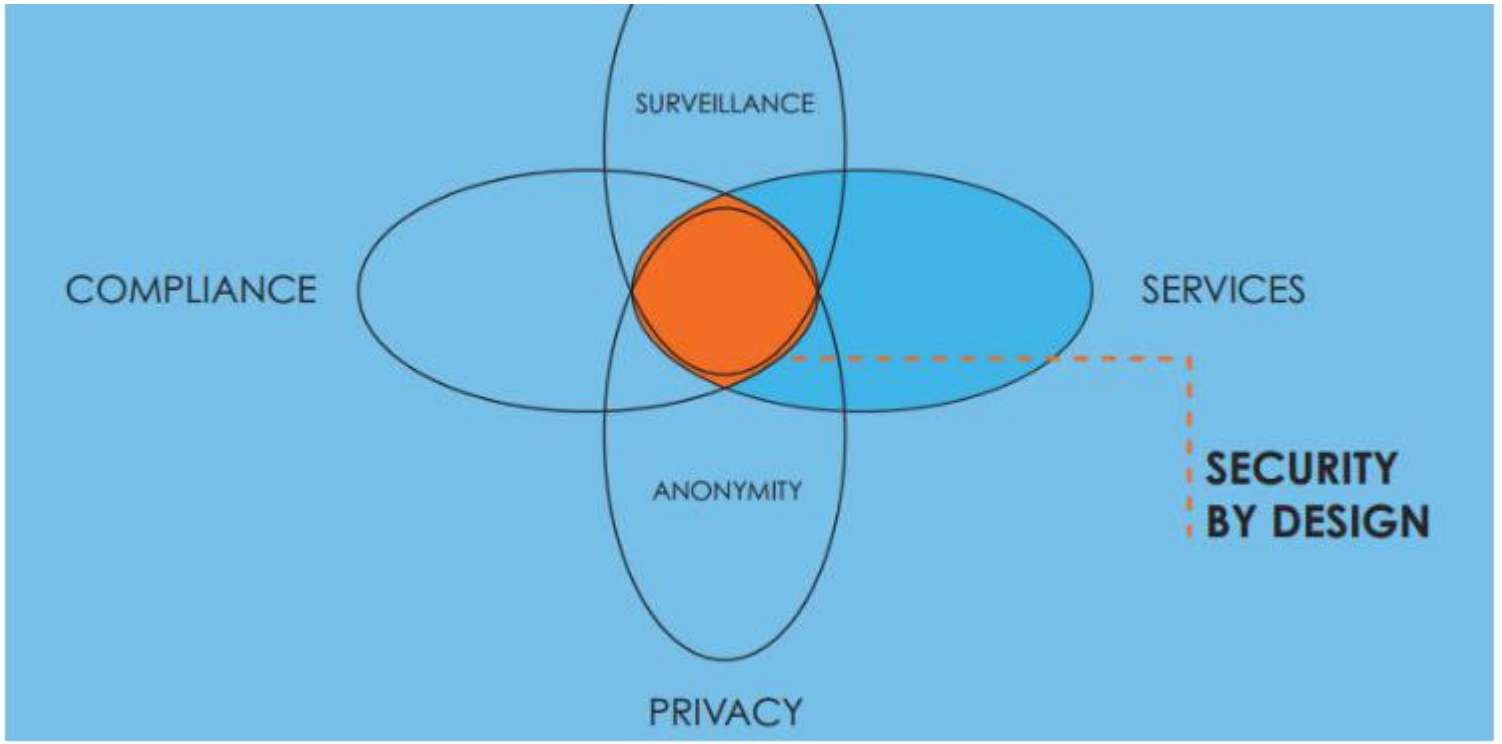
- What will citizens think about this?
  - Feeling of being under constant surveillance
  - No control over which public authorities process their personal data and for what purposes
  - The public sector makes decisions about citizens (profiling) rather than offering services to them
- Reduced trust in the public sector
  - Citizens could become less willing to contribute data, e.g. for surveys, when they have a choice

Once-only and information security

- Data breaches become more dangerous
  - Centralised database: single point of failure
  - Single citizen ID: information from different data breaches can be linked to create a profile
- Massive breach in South Korea (2014)
- Data protection by design (GDPR Article 25)
  - State of the art technology to implement e.g. **data minimisation** is now a legal requirement
  - Once-only database linkages could make this more difficult

Citizen-centric once-only

- Objectives
  - Allow citizens to re-use their own information between public services (”data portability”)
  - Ensure that **only the citizen can do this** to prevent ”abuse” (uncontrolled data use)
- How?
  - Virtual identities (validated) for public services
  - eID with pseudonyms [eIDAS Article 5(2)]
- CitizenKey project in Denmark (trial)



Announcing CitizenKey® providing Small Data, eIDAS 5.2 Id & Citizen-Centric OnceOnly in Denmark

Udgivet den 30. december 2017

Stephan Engberg | Følg
I make Trustworthy Identity Services to prevent markets and de…