UiO : Institutt for privatrett
Det juridiske fakultet

Lee A. Bygrave, Senter for rettsinformatikk

Person(opplsynings)vernforordningens bestemmelser om innebygget person(opplysnings)vern

Personvernkonferansen 02.12.2016

‘The answer to the machine is in the machine’ (Clarke)

- ECMS ► DRMS ► PETs
- ‘Lex informatica’ (Reidenberg) og ‘Code’ (Lessig)
- ‘Ex post’ ► ‘ex ante’ anvendelse av rettsregler
- Bruk av jussen til å understøtte ‘hardwiring’ – sml. opphavsrett med pov-rett

PVF art. 25(1): pv gjennom design

Art. 25(1): ‘Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.’

PVF art. 25(2): pv gjennom standardinnstillinger (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.'

PVF art. 25(3): sertifisering

Art. 25(3): ‘An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Articles.’

PVF art. 25: kontekst

- PETs ► PBD
- Kryptering ► bredere funksjoner (eks., innsyn, forståelighet og styrbarhet av informasjonssystemer)
- Teknologiske ► organisatoriske tiltak

Privacy by design (PBD): definisjon(er)

‘practical measures, in the form of technological and/or design-based solutions, aimed at bolstering privacy/data protection laws, better ensuring or almost guaranteeing compliance, and minimizing the privacy-intrusive capabilities of the technologies (i.e. PITs) concerned’

-- Demetrius Klitou

PBD: prinsipper

- ‘Proactive not Reactive; Preventative not Remedial
- Privacy as the Default
- Privacy Embedded into Design
- Full Functionality: Positive-Sum, not Zero-Sum
- End-to-End Lifecycle Protection
- Visibility and Transparency
- Respect for User Privacy.’

-- Ann Cavoukian

PBD: problemer (1)

- Hvordan iverksetter vi PBD-prinsippene?
- Hvordan måler vi ulike grader av person(opplysnings)vern?
  - Eks. Cavoukian: '*Privacy by design* seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any IT system or business practice.'
  - Hva menes med 'maximum degree of privacy'?

PBD: problemer (2)

- Hvor 'hard' må 'hardwiring' være?
  - Sml. debatt mellom Lessig og andre over P3Ps status
  - Sml. Klitous definisjon av PBD ('better ensuring or almost guaranteeing compliance …')
- I hvilken grad skal PBD/PET-funksjoner overgå rettslige krav?
  - Sml. Cavoukians synspunkt med EU instrumenter
- I hvilken grad er PBD = DPBD?

PBD/iPOV: rettslige utfordringer (1)

- Nåværende regler om pov er ikke konstruert for å være 'automatiseringsvennlige'
  - Sml. Schartums forslag
- P(O)V-rett fokuserer på behandlingsansvarlige ('controllers'), ikke utviklere av informasjonssystemer eller -standarder

PBD/iPoV: rettslige utfordringer (2)

- Dårlig støtte i PVD
  - Jf. art. 17 (men sml. fortalens avsnitt 45!)
  - Sml. EPD (2002/58/EF) art. 14(3) og tysk rett

PBD/iPOV: støtte i domstolen(e)

- EMD i *I v Finland* (2008) – iverksetting av teknologiske tiltak for å sikre konfidensialitet av pasientdata = positiv forpliktelse ihht. EMK art. 8
- EU-domstolen i Sak C-131/12, *Google Spain* – søkemotorer
- EU-domstolen stoppet 'PIT' (i form av DPI) i *SABAM* sakene fra 2011 og 2012.

PVF art. 25(1): kvalifikasjoner

Art. 25(1): 'Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.'

PVF art. 25(1): ansvar

Art. 25(1): 'Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.'

PVF art. 25(1): tiltak

Art. 25(1): 'Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.'

PVF art. 25(2): pv gjennom standardinnstillinger (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.'

PVF art. 25: svakheter (1)

- Fokus på ‘controllers’
- Formulerer ‘design’-trinn som tidspunkt da ‘controller’ blir ‘controller’
  - Sml. fortalens avnsitt 78 som nevner ‘producers’, men disse underlegges mindre strengere krav
- ‘Processors’ fanget indirekte av art. 28(1)
  - Se også fortalens avsnitt 81
- Krav i art. 25 er vage; lite veiledning om tolkning

PVF art. 25: svakheter (2)

- Mangel på 'hardwiring'-insentiver (unntatt sanskjoner)
- Lite sannsynlig at strenge sanksjoner anvendes
- Dårlig 'regulatory conversation' (Black) med IKT-ingeniører o.l.