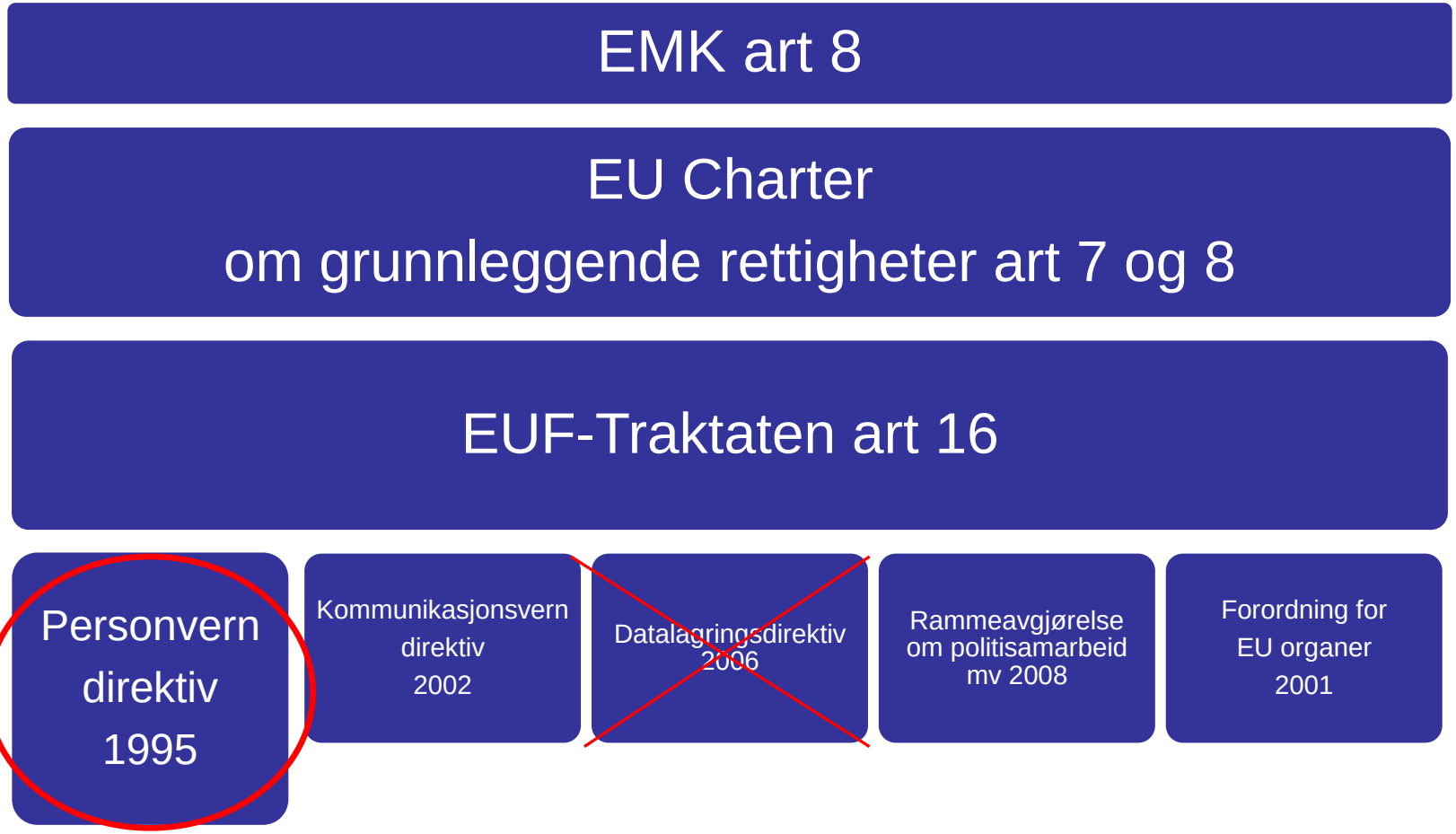
UiO : Institutt for privatrett
Det juridiske fakultet

Lee A. Bygrave, Senter for rettsinformatikk

EUs forordning om personopplysningsvern: Historikk, kontekst og hovedtrekk

Partnerforum seminar, Oslo 27. mars 2017

Rettslig kontekst



Historikk

- 1995: Direktiv 95/46/EF
- 2002: Direktiv 2002/58/EF
- 2009: Charter art. 7 og 8 ble rettslig bindende
- 2012: Første forslag til forordning
- 2016: Forordning vedtatt (i kraft 2018)

Siktemål

- Harmonisering
  - Videreføring av grunnprinsipper
- Modernisering
  - «Putting the data subject in control»
- Forenkling
  - Stimulerer til økonomisk vekst
  - Realiserer «Digital Single Mkt»

Harmonisering?

- (T)ja, men medlemsstater får fremdeles spillerom, f.eks ifht:
  - Lovlighet av behandling (art. 6(2a))
  - Behandling av genetiske, biometriske og helseopplysninger (art. 9(4))
  - Generelle unntak (art. 23)
  - Behandling av opplysninger om arbeidstakere (art. 88)
  - Bøtelegging av offentlige myndigheter (art. 83(7))

Forenkling? (1)

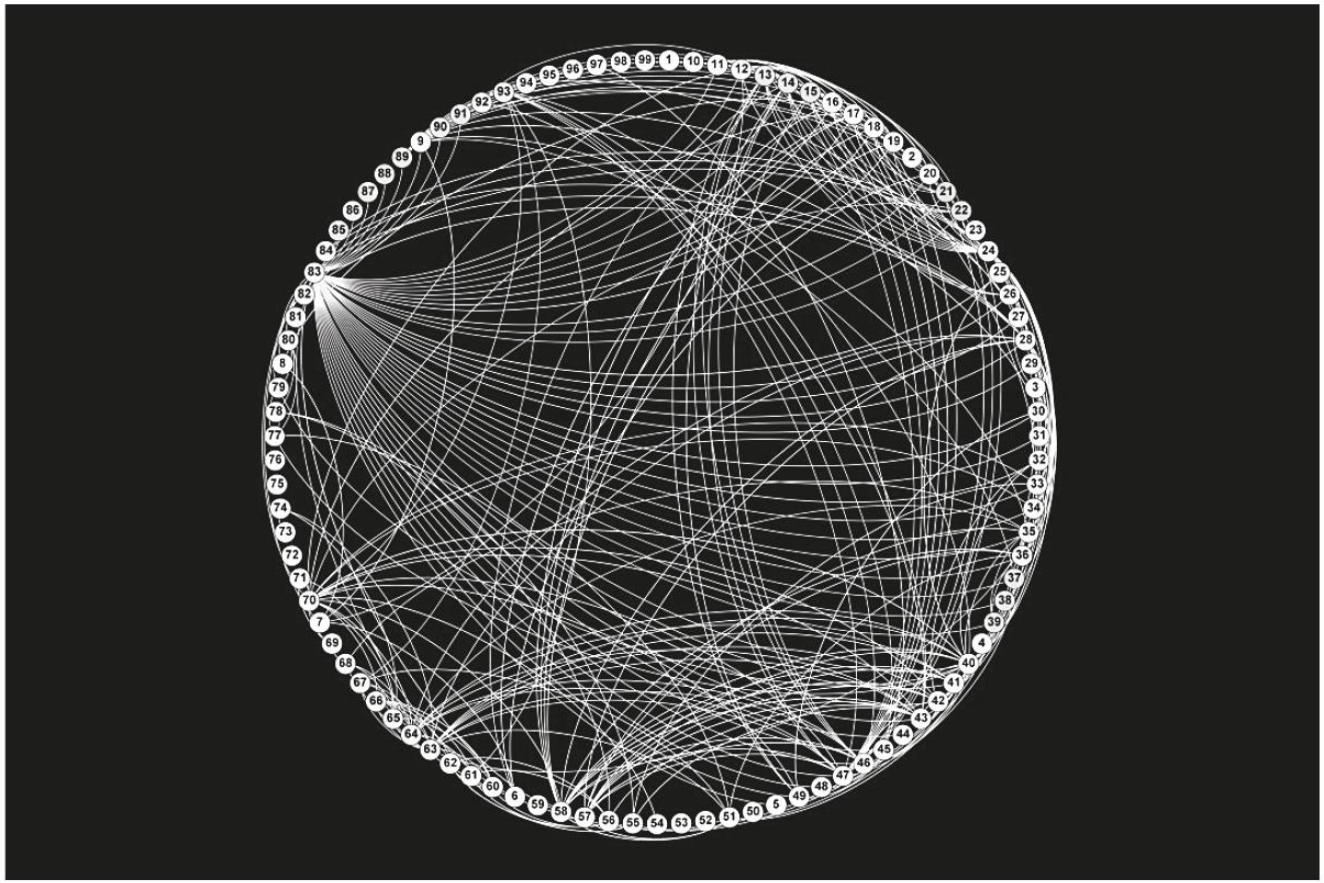
- (T)ja …
  - eks. «one-stop shop» (jf. art. 56)
  - «consistency mechanism» (art. 63flg)
  - redusert meldeplikt
  - klargjøring av noen kriterier i PVD

Et hårete beist

Forenkling? (2)

- Nei …
  - mange rettstekniske vanskeligheter …
    - nesten 100 artikler (mange med flere lange avsnitt)
    - fortale med 173 avsnitt
    - hyppig bruk av kryssreferanser
    - lite veiledning
  - nye dokumentasjonskrav

Forenkling? (3)



- Sushant Agarwal, Institute for Management Information Systems, 2016

Eks. på klargjøring (1): samtykke

- «… any freely given, specific, informed and unambiguous indication of … wishes [by which the data subject] by a statement or by a clear affirmative action, signifies agreement …» (art. 4(11))

  [NB: Mye debatt rundt tidligere krav om uttrykkelighet og om passiv samtykke er gyldig]

Eks. på klargjøring (2): erstatning (oppreisning)

- «any person who has suffered material or non-material damage … shall have the right to receive compensation» (art. 82(1))

Viktige forskjeller (1)

- Ny tilsynsordning
  - European Data Protection Board (art. 68flg)
- Økt makt til kommisjonen?
  - I liten grad
- Kraftigere sanksjonsmuligheter (art. 83)
  - Opp til 20 M Euro / 4 % av årlig omsetning

Viktige forskjeller (2)

- Nye kriterier for lovanvendelse (art. 3)

Lovanvendelse ved etablering i EU

Art. 3(1): «This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union***, regardless of whether the processing takes place in the Union or not***».

Lovanvendelse utenfor EU

Art. 3(2)): «This Regulation applies to the processing of personal data … by a controller ***or processor*** not established in the Union, where the processing activities are related to:

(a) the offering of goods or services***, irrespective of whether a payment of the data subject is required***, to such data subjects in the Union; or

(b) the ***monitoring*** of their behaviour as far as their behaviour takes place within the Union».

Viktige forskjeller (3)

- Flere dokumentasjonskrav (art. 30, 31(4))
  - Men kvalifisert unntak for organisasjoner < 250 ansatte (art. 30(5))
- Meldeplikt vedr. sikkerhetsbrudd (art. 33, 34)
- Økt krav til risikovurdering («data protection impact assessment») (art. 35)
- Nye krav til innebygd personopplysningsvern («data prot. by design and default» (art. 25))

Viktige forskjeller (4)

- Nye eller forsterkede rettigheter/plikter
  - samtykke
  - retten til dataportabilitet (art. 20)
  - retten til å motsette seg «profiling» (art.22)
  - krav til innebygd personopplysningsvern (art.25)

Viktige forskjeller (5)

- Krav til «data prot. officers» (art. 37flg)
  - Gjelder alle offentlige etater
  - Gjelder alle private aktører som har storskala systematisk «monitoring» som kjerneaktivitet eller som gjør storskala bruk av sensitive data som kjerneaktivitet

Viktige forskjeller (6)

- Behandlere («processors») får økt ansvar
  - Se f.eks. art. 30, 33 og 37, men ikke 35(!))
  - Behandlere får erstatningsansvar dersom
    - De har brutt forpliktelser som spesifikt gjelder dem, eller
    - De har handlet utover eller i strid med lovlige instrukser fra behandlingsansvarlige (controller) (jf. art. 82(2))

[Ikke så?] viktige forskjeller (7)

- Nye (eller modifiserte) grunnprinsipper, f.eks.
  - «accountability»: «The controller shall be responsible for and be able to demonstrate compliance with paragraph 1» (art. 5(2))
  - «minimalisation»: p.o. skal være «adequate, relevant and limited to what is necessary …» (art. 5(1)(c))
    - Sml. «ikke for omfattende» («not excessive») i PVD

Samtykke (1)

- Samtykke får ikke fortrinn over andre rettslige grunnlag for databehandling
- En kan ikke avtale bort grunnleggende pv-krav

Samtykke (2)

- Krav til dokumentasjon (art. 7(1))
- Krav til klarhet (art. 7(2))
  - «If … consent is … given in the context of a written declaration which also concerns other matters, the request for consent must be presented in a manner which is clearly distinguishable from the other matters»

Samtykke (3)

- Krav til formålsbestemthet (art. 6(1)(a))
  - «consent … for one or more specific purposes»
- Nye krav til samtykke fra barn (art. 8)
- Kan trekke samtykke tilbake når som helst (art. 7(3))

Samtykke (4)

- Uklar bestemmelse om maktmisbruk og ubalanse i art. 7(4)); sml. fortalen avsnitt 43:
  - « … consent should not provide a valid legal ground for the processing of personal data … where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation. Consent is presumed not to be freely given, if it does not allow separate consent to be given to different data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service is dependent on the consent despite such consent not being necessary for such performance».

    [Samtykke kan ikke være betingelse for bruk av tjeneste]

Sensitive opplysninger (1)

- Nye kategorier av sensitive opplysninger
  - Genetiske data og biometriske data brukt til identifiseringsformål (men ikke autentisering?)
- Flere nye behandlingsgrunnlag
  - Eks. for arkiv-virksomhet

Sensitive opplysninger (2)

- Merk skjønnsmargin for medlemsland ifht. genetiske, biometriske og helsedata (jf. art. 9(4))
  - «Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health».
  - Se også art. 87 om bruk av nasjonale identifikasjonsnumre «or any other identifier of general application»

Krav til innebygd pov

- Forordningen art. 25 (ny!)
- Deles opp i to aspekter:
  - 1. «by design»
  - 2. «by default»
- Sml. «Privacy by design»

Mer reform på vei

- Reform av direktivet om kommunikasjonsvern (2002/58/EF)
  - Forslag til ny forordning om «privacy and electronic communications» publisert 10.01.2017
- Nytt direktiv om personopplysningsvern i politi og justissektor (2016/680)
  - Skal i hovedsak implementeres innen 6. mai 2018
- Diskusjon ifm. realisering av Digital Single Market

EU-domstolen: garantist for sterk pv?