BECH-BRUUN

Den nye persondataforordning

Advokat Marie Albæk Jacobsen

DEIC-konference, den 6. oktober 2015

Den kommende forordning

Kommissionens forslag til en persondataforordning, KOM(2012)11 af 25. januar 2012

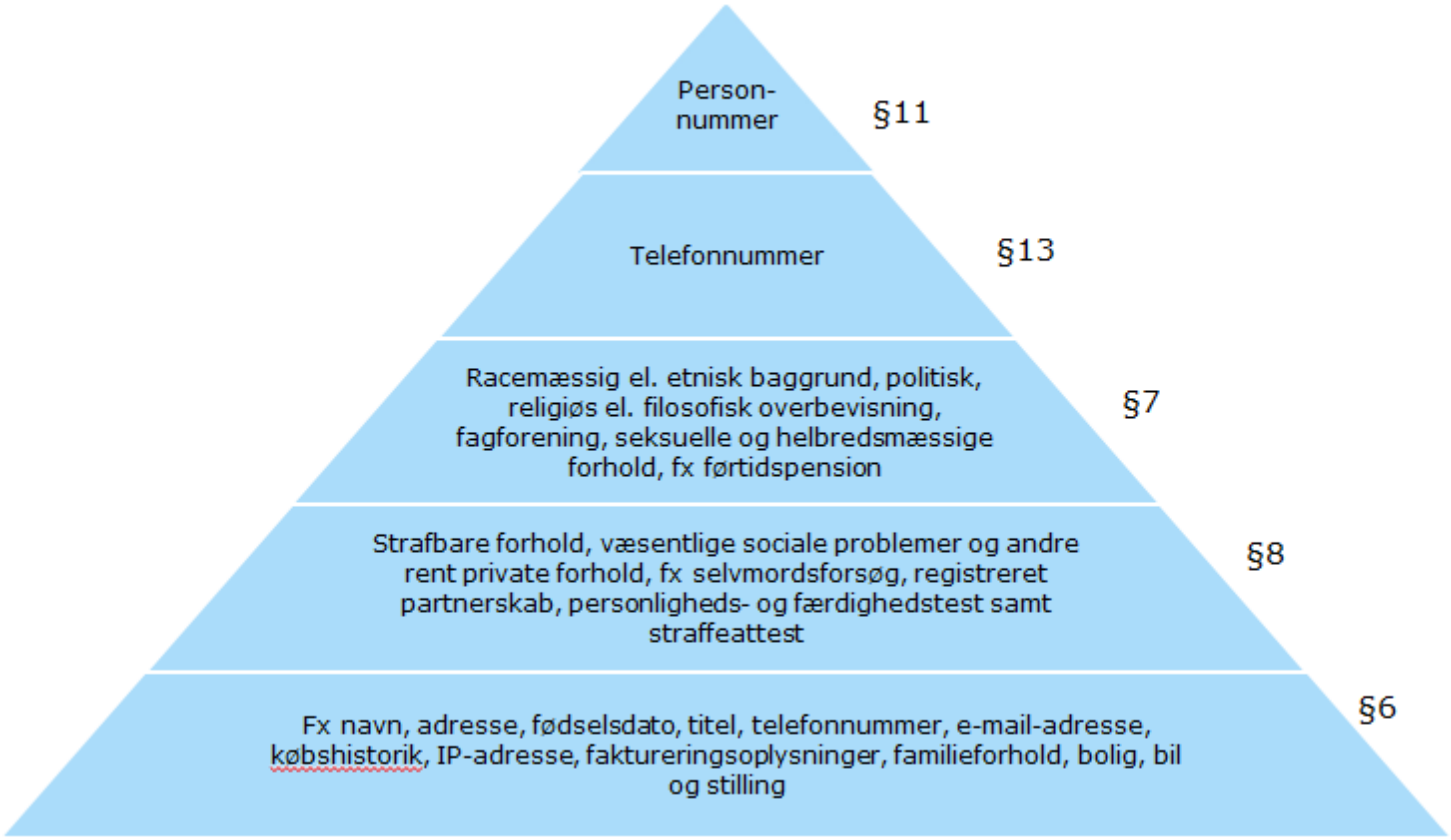
- Formål
  - Ensartet regulering i EU
  - Færre administrative byrder for virksomhederne
- Form
  - Forordning vs direktiv
  - Mulighed for national regulering?
- Status
  - Oprindeligt Q2 2014
  - Nu Q4 2015/Q1 2016
  - 2-årig implementeringsperiode

Hvad er personoplysninger?

Cpr-nr.
Køn
Navn
Race
Adresse
E-mail-adresse
Seksuel overbevisning
Foto
Fødselsdato
Kreditkortnummer
Adgangskontrol
Helbredsoplysninger
Nummerplade
Genetisk information
Interesser
Familiemæssige oplysninger
MedarbejderID
Politisk overbevisning

Væsentlige sociale problemer
Uddannelse (karakterer)
Personlighedstest
Telefonnummer
Religion
Personlige produktionstal
IP-adresse
Elektroniske spor
Videoovervågning
Pasnr.
GPS-oplysninger
Logning i IT-systemer
Initialer/Loginnavn
Fagforeningsmæssige tilhørsforhold
Biometriske oplysninger
Straffeattest
Stilling
Størrelse på tøj og sko
Rejseoplysninger
Løn

Oplysningskategorier



Den kommende forordning

- Systematik svarer nogenlunde til persondataloven

- Generelle databehandlingsprincipper gælder fortsat
  - Saglighed, proportionalitet, sletning, mv.

- Behandlingshjemmel (hvornår må man behandle personoplysninger) er mere eller mindre de samme:
  - Samtykke
  - Sker som led i opfyldelse af aftale
  - Interesseafvejning (det offentlige?)

Væsentlige ændringer

- Væsentligste ændringer:
  - Øgede dokumentationskrav
  - Privacy Impact Assessment (konsekvensanalyse)
  - Data protection by design/Data protection by default
  - Krav om udpegning af DPO
  - Notifikationsforpligtelse
  - Databehandleren får selvstændige forpligtelser
  - Sanktioner skærpes

Øgede dokumentationskrav

- Dokumentation af datastrømme
  - Kortlægning af data flows
    - Typer af data
    - Formål
  - Internt vs eksternt

- Grundlaget for overførsler
  - Databehandleraftaler
  - Tredjelandsoverførsler
    - EU Model Clauses
    - Binding Corporate Rules

- Interne procedurer
  - Indsigtsanmodninger, mv.

Privacy Impact Assessment

- Privacy Impact Assessment skal udarbejdes, hvis behandlingen af personoplysninger involverer store risici i relation til datasubjektets rettigheder og friheder, fx:
  - Behandling af oplysninger om mere end 5000 personer årligt
  - Systematiske profileringsaktiviteter
  - Behandling af følsomme oplysninger
  - Omfattende videoovervågning af offentlige arealer
  - Behandling af oplysninger om børn, biometriske data, genetisk data i omfattende systemer

- Indhold
  - Beskrivelse af behandlingsaktiviteterne
  - Risici i relation til datasubjektet
  - Beskrivelse af sikkerhedsforanstaltninger

Data protection by design/by default

- Krav til implementering af passende tekniske og organisatoriske foranstaltninger og procedurer til sikring af, at forordningen overholdes

- Systemer skal understøtte beskyttelse af privatlivets fred
  - fx at oplysninger ikke behandles til andre formål eller længere end nødvendigt
  - Fx at oplysninger ikke er tilgængelige for et ubegrænset antal personer

Data Protection Officer

- Der skal udpeges en DPO:
  - i virksomheder/organisationer med mere end 250 ansatte *ELLER*
  - hvis der behandles oplysninger om mere end 5000 datasubjekter i en sammenhængende periode på 12 måneder

- Krav til DPO'en
  - DPO'en skal være en uafhængig person, der rapporterer direkte til ledelsen hos den dataansvarlige eller databehandleren
    - DPO'en skal have ekspertise på området for databeskyttelseslovgivning og –praksis
    - DPO'en skal udpeges for en periode på mindst to år

Notifikationspligt

- Til Datatilsynet:
  - "without undue delay" og som udgangspunkt inden for 24/72 timer
    - Hvad er der sket, kategorier og antal
    - Anbefalede foranstaltninger til afhjælpning skadevirkninger
    - Beskrivelse af konsekvenser af bruddet
    - Beskrivelse af foreslåede eller iværksatte foranstaltninger ifm. bruddet

- Til datasubjektet:
  - "without undue delay" efter meddelelsen til datatilsynet, hvis risiko for at sikkerhedsbruddet vil påvirke beskyttelsen af datasubjektets personoplysninger, eller rettigheder/friheder berøves

Databehandler

Databehandleren pålægges selvstændige forpligtelser, herunder:

- Dokumentation for enhver behandling af personoplysninger i virksomheden (datastrømsanalyse)
- Intern og ekstern persondatapolitik
- DPO
- Indretning af systemer og tekniske hjælpemidler samt kontrol heraf (audits)
- Brug af underdatabehandlere
  - Databehandleraftale
  - Procedure, der sikrer at ej underdatabehandlere uden den dataansvarliges instruks
- Proces for håndtering af underretning af de dataansvarlige i forbindelse med sikkerhedsbrud

Sanktioner

Bøde op til 2% (5%) af den globale omsætning eller op til 1 mio. EUR

Overtrædelsestype:	Bødeniveau:
• Ingen fastlæggelse af ordninger for registreredes anmodninger • Ej rettidig besvarelse heraf	Op til 0,5% af den årlige globale omsætning/ 250.000 EUR
• Ikke giver relevante oplysninger ved indsigtsanmodning • Ikke sletter oplysninger • Manglende ajourføring af dokumentation	Op til 1% af den årlige globale omsætning/ 500.000 EUR
• Behandler oplysninger uden hjemmel • Ikke respekterer en indsigelse • Ikke varsler tilsynet om brud på sikkerheden • Ikke gennemfører konsekvensanalyser • Ikke udpeger en DPO • Overfører oplysninger til tredjelande uden hjemmel	Op til 2% af den årlige globale omsætning/ 1 mio. EUR

Hvordan bør man forberede sig?

- Overblik over datastrømme i virksomheden/organisationen (vigtigt!)
- Overblik over databehandleraftaler
- Overvejelser omkring udpegning af DPO
- Mulighed for at afprøve kommende krav, fx Privacy Impact Assessment
- Ledelsesforankring!
- Persondataretlig Pre-audit /Compliance Projekt

Kontakt

Marie Albæk Jacobsen

Advokat · Aarhus

Intellectual Property & Technology

T +45 72 27 33 49
M +45 25 26 33 49
E maja@bechbruun.com