Henning Mortensen 15. sep. 17

Persondataforordningen

- Et overblik

Den politiske baggrund

Menneskerettigheder m.v.

- No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, Verdenserklæringen om mtighederne, 1948, Ditto EMRK, GRL, OECDs guidelines, Europarådets konvension
- Privacy er et konstituerende menneskeligt træk, med stor historisk betydning og geografisk betydning. Alternativet er ændring af adfærd, udfordring af det reelle frie valg, hvis uerkendte "afslørende præferencer" udnyttes
- Ro til refleksion m.v.

Teknologisk udvikling

- Biometri og væv: Man kan spore DNA og fingeraftryk – men også gangart og ansigtsgenkendelse (face detection vs. recognition – f.eks. DeepFace med 97,35% succesrate)
- Søgning, surveys, likeknapper og cookies: alle brugernes aktiviteter kan opsamles i en profil.
- Man kan spore udstyr: Devicefingerprinting
- Location based services og trafikanalyser: Vi ved altid hvor brugerne er
- Forensic linguistics: Man kan fastslå, hvem der har forfattet et stykke tekst af en vis længde (f.eks. J.Krowling og The Cuckoo's Calling)
- Internet of EveryThing: Alt udstyr kommer online og kan devicefingerprintes (inkl. TV, køleskab, bil, el-vand og gasmålere – og børnelegetøj og sexlegetøj)

Udviklingen i trusselsbilledet

- IT-kriminelle: Alle personoplysninger kan sælges (e-mailkonti, brugerkonti, CPR-numre, kontonumre og selvfølgelig informationer om særlige privilegerede brugere (Se&Hør-sagen, CSC-sagen, osv.)
- Fremmede lande: Angreb på Office of Personel Management, indblanding i valgkampe, det danske forsvars personaleoplysninger (og i øvrigt angreb på kritisk infrastruktur)
- Idealistiske angreb: Ashley Madison, Anonymous, m.v.
- Whitehats: Tag godt imod dem!

Retskilder

Kilder

- Forordningen/direktivet
- Databeskyttelsesloven (den nationale præcisering af visse bestemmelser i forordningen)
- Betænkning 1565
- National lovgivning med bekendtgørelser og vejledninger – f.eks. Sundhedsloven og TV-overvågningsloven
- EMRK art. 8 (respekt for privatliv), 1950
- EU's charter om grundlæggende rettigheder art. 7 (respekt for privatliv) og art. 8 (beskyttelse af personoplysninger), 2000, retligt bindende med Lissabontraktaten i 2009.
- Europarådets konvention 108 og deraf følgende rekommendationer
- Praksis fra Datatilsynet (afgørelser) og Datatilsynets vejledninger, evt. som opsamlet i den kommenterede udgave af persondataloven
- Udtalelser fra Artikel 29-gruppen
- Domme (nationale, EU-domstolen, europæisk menneskerets domstol)
- Standarder

Persondataforordningen - baggrund

Formål:

- Styrke individernes ret til databeskyttelse
- Understøtte det frie flow af data
- Reducere administrative byrder

Forordning versus direktiv

Direktiv	Forordning
72 præambelbetragtninger	173 præambelbetragtninger
34 artikler	99 artikler
8 definitioner	26 definitioner

Kompliceret i forvejen; nu betydeligt større regelværk.

Forordning versus direktiv

Fra præambel 10: ”Denne forordning indeholder også en **manøvremargen**, så medlemsstaterne kan præcisere reglerne heri, herunder for behandling af særlige kategorier af personoplysninger (»følsomme oplysninger«). Denne forordning **udelukker** således **ikke, at medlemsstaternes nationale ret fastlægger omstændighederne i forbindelse med specifikke databehandlingssituationer**, herunder mere præcis fastlæggelse af de forhold, hvorunder behandling af personoplysninger er lovlig. ”

- Hertil 54 muligheder for at fastsætte national lovgivning
- **Summa sumarum: begrænsning af forordningens harmoniserende virkning**

Loven

- Principper: Lovlig, rimelig, gennemsigtig, formål, minimeret, korrekte, lagringsbegrænsning, sikkert, dokumenteret
- Rettigheder: Oplysningspligt, indsigtsret, berigtige, slette, begrænse, underrette, portabilitet, indsigelse, profilering
- Pligter: DPbDx2, databehandlere, fortegnelse, sikkerhedsforanstaltninger, DBN, DPIA, DPO, overførsel

- Summa sumarum: ved første øjekast er der ikke mange nyskabelser.

Definitioner

- **Personoplysning:** informationer relateret til en identificeret eller identificerbar person, herunder hvis personen kan udpeges. Omfattet er bl.a.
  - Navn, adresse, telefonnummer, e-mailadresse
  - Portrætfoto, film
  - Hashværdi af fingeraftryk
  - IP-adresse
  - Løbenummer eller ID-nummer
  - Cookies, RFID-numre, hardwarenumre
- **Behandling:** Enhver aktivitet som personoplysninger gøres til genstand for, f.eks. indsamling, registrering, organisering, systematisering, opbevaring, tilpasning eller ændring, genfinding, søgning, brug, videregivelse ved transmission, formidling eller enhver anden form for overladelse, sammenstilling eller samkøring, begrænsning, sletning eller tilintetgørelse.
- **Den registrerede:** En identificeret eller identificerbar fysisk person.
- **Dataansvarlig:** En fysisk eller juridisk person, en offentlig myndighed, en institution eller et andet organ, der alene eller sammen med andre afgør, til hvilke formål og med hvilke hjælpemidler der må foretages behandling af personoplysninger.
- **Databehandler:** En fysisk eller juridisk person, en offentlig myndighed, en institution eller et andet organ, der behandler personoplysninger på den dataansvarliges vegne.
- Mange flere definitioner i forordningen.

Lovlig behandling 1

Kategorier af personoplysninger

- Almindelige
- Følsomme
- Strafbare forhold
- Specifikke behandlingssituationer
  - CPR-nummer
  - Ansættelsesforhold
  - Særligt samtykke for børn

Lovlig behandling 2

Lovlig behandling af almindelige oplysninger

- Samtykke
- Opfyldelse af kontrakt
- Retlig forpligtelse hos dataansvarlig
- Vitale interesser
- Samfundets interesse eller myndighedsudøvelse
- Legitim interesse under hensyn til interesseafvejning

- Offentlige myndigheder må ikke bruge interesseafvejning
- På arbejdsmarkedet skal man være meget tilbageholdende med at bruge samtykke. Ditto i den offentlige sektor. Der skal være et reelt frit valg.

Lovlig behandling 3

Lovlig behandling af følsomme personoplysninger

- Følsomme personoplysninger:
  personoplysninger om race eller etnisk oprindelse, politisk, religiøs eller filosofisk overbevisning eller fagforeningsmæssigt tilhørsforhold samt behandling af genetiske data, biometriske data med det formål entydigt at identificere en fysisk person, helbredsoplysninger eller oplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering
  - Behandling er som udgangspunkt forbudt
  - Undtagelser (hjemmel i A9):
    - Eksplicit samtykke, med mindre national lovgivning fastslår at borgeren ikke har ret til at give et sådant samtykke
    - Overholde den dataansvarliges eller den registreredes arbejds-, sundheds- og socialretlige forpligtelser og specifikke rettigheder med hjemmel i EU-ret, national ret eller kollektive overenskomster
    - Vitale interesser
    - Stiftelser, foreninger m.v. som led i legitime aktiviteter (bl.a. fagforeninger)
    - Offentliggjort af den registrerede selv
    - Fastlæggelse af retskrav
    - Væsentlige samfundsinteresser på grundlag af lov
    - På sundhedsområdet (til dels med tavshedspligt)
    - Videnskabelig eller historisk forskning og statistik
- For følsomme personoplysninger skal samtykket være **eksplicit**

Principper for behandling

- Lovlig, rimelig og gennemsigtig
- Udtrykkeligt angivne og legitime formål (formålsbegrænsning)
- Data skal være tilstrækkelig, relevant og begrænset (minimering)
- Data skal være korrekte og om nødvendigt ajourførte (rigtighed)
- Data må kun lagres i en form, hvor den registrerede ikke kan identificeres i længere tid end nødvendigt (opbevaringsbegrænsning)
- Behandlingen må kun ske, hvis der er taget de fornødne sikkerhedsforanstaltninger (Integritet og fortrolighed)
- Den dataansvarlige er ansvarlig for compliance med principperne og skal kunne påvise compliance (ansvarlighed)

Datasubjektets rettigheder

- Hjælp fra dataansvarlig til udøvelse af rettigheder
- Letforståeligt og lettilgængelig og evt. med anvendelse af standardiserede ikoner
- Uden unødig forsinkelse og indenfor en måned
- Oplysningspligt
- Indsigtsret
- Berigtige
- Slette
- Begrænse
- Underrette
- Dataportabilitet
- Indsigelse
- Profilering
- Undtagelser – offentlig forvaltning

Dataansvarligs pligter

- Overordnet ansvar hos den dataansvarlige, men også noget ansvar hos databehandleren
- Data Protection by Design and Default
- Dataansvarlige må kun bruge databehandlere, der kan leve op til en række krav, som fastsættes i en detaljeret databehandleraftale
- Fortegnelse over behandlingsaktiviteter
- Passende tekniske og organisatoriske sikkerhedsforanstaltninger
- Data Breach Notofication
- Data Protection Impact Assessment
- Data Protection Officer
- Hjemmel til tredjelandsoverførsler:
  - EU/EØS
  - Lande med tilstrækkeligt beskyttelsesniveau
  - Lande uden tilstrækkeligt beskyttelsesniveau: Privacy Shield, SCC, BCR

JM om DPbD

PbDx2

- Ikke et nyt sikkerhedskrav
- Overvejelsesforpligtelse og håndteringsforpligtelse
- Fremtidige systemer f.eks. gennem PET
  - Eksisterende systemer SKAL ikke redesignes
  - Større ændringer kan kræve tilpasninger
  - Hvis standardindstillinger KAN ændres SKAL de ændres inden 25. maj 2018
- I betænkning 1565 redegør justitsministeriet for at de anser designtidspunktet, som det eneste delvist nye.

Kommentar: Jeg er ikke enig. DPbD har et selvstændigt materielt indhold.

Designprincipper

Ann Cavoukians designprincipper

Proaktiv, ikke reaktiv
Foranstaltninger skal altså iværksættes inden en risiko materialiserer sig.

Privacy som standardindstilling
Den registrerede skal ikke selv foretage sig noget for at beskytte sine oplysninger; beskyttelsen skal være slået til fra starten.

Privacy skal være indlejret i systemet
Foranstaltningerne skal designes ind i et systems arkitektur og ikke tilføjes efterfølgende.

Der skal være fuld funktionalitet
Der skal være fuld funktionalitet. Det må ikke være sådan, at man kan få begrænset funktionalitet, der er sikker og fuld funktionalitet, hvis man opgiver sin sikkerhed. Generelt må der ikke være en modstrid mellem sikkerhed og databeskyttelse.

Beskyttelse i hele livscyklussen
Beskyttelsen skal indbygges i designfasen inden systemet sættes i drift og være aktiv i hele systemets levetid.

Transparens
Der skal være gennemsigtighed i forretningsmodeller og teknologier og det der signaleres skal kunne verificeres (af en uafhængig tredjepart).

Brugeren i centrum
De registreres interesser skal være i fokus f.eks. gennem standardindstillinger, notifikation og empowerment af brugerne, så de er i kontrol.

Kommentar: Vi kan ikke støtte ret på præcis disse, men de giver en indikation af et materielt indhold i begrebet.

Afsluttende bemærkninger

- One-stop-shop og sammenhængsmekanismen
- Bøder
- Erstatning

- Vejledninger fra DT og JM
- Vejledninger fra artikel 29-gruppen

- Uløste problemer, jf. Rådet for Digital Sikkerhed og Alexandra Instituttet

Min personlige tilgang

- Virksomheden skal have udpeget en ansvarlig ekspert med forankring i topledelsen (kompetence og beslutning)
- Vi fastslår hvilke dele af forordningen m.v., der er relevant for virksomheden
- Vi kortlægger alle systemer og tjenester og fastslår, om der behandles personoplysninger (meget kort spørgeskema til direktører)
- Systemer og tjenester får tilknyttet ansvarlig, overordnet ansvarlig og teknisk ansvarlig (ansvar)
- For hver tjeneste, hvor der behandles personoplysninger, laver vi dokumentation, jf. excel-fil. (juridisk compliance) og sikrer at behandling er lovlig
- Vi laver risikoanalyse og kortlægning af sikkerhedstiltag for forretningskritiske systemer (sikkerhedsmæssig compliance)
- Procedurer, rutiner, systemer og tjenester tilpasses (lukke eller redesigne tjenester, slette data og implementere helt nye teknologier)
- Der vil opstå konflikter mellem lov og forretning. IT-sikkerhedsrådet beslutter hvilken risiko vi i tvivlstilfælde vil leve med.

Tools

- **Forordningen på dansk**
  http://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:32016R0679&from=DA
- **Justitsministeriets betænkning om påvirkning af dansk lovgivning**
  http://www.justitsministeriet.dk/nyt-og-presse/pressemeddelelser/2017/nye-regler-styrker-beskyttelsen-af-persondata-i-europa
- **Udkastet til Databeskyttelsesloven**
  https://hoeringsportalen.dk/Hearing/Details/60828
- **Excel-vejledning om dokumentation af forordningen**
  https://www.linkedin.com/pulse/nyt-gratis-v%C3%A6rkt%C3%B8j-kan-lette-arbejdet-med-henning-mortensen
- **Skema til håndtering af personoplysninger på HR-området**
  https://www.linkedin.com/pulse/nyt-gratis-skema-til-h%C3%A5ndtering-af-personoplysninger-p%C3%A5-mortensen
- **DI's vejledning om forordningen med mapping af forordningens krav og ISO27002-kontroller**
  http://di.dk/Virksomhed/Produktion/IT/itsikkerhed/personoplysninger/Pages/Vejledningompersondataforordningen.aspx
- **DI's DPIA-skabelon**
  http://di.dk/Virksomhed/Produktion/IT/itsikkerhed/personoplysninger/Pages/DIsskabelonforPrivacyImpactAssessment.aspx
- **DI's vejledning om sikkerhed ved cloud computing og outsourcing**
  http://di.dk/Virksomhed/Produktion/IT/itsikkerhed/vejledninger/Pages/Sikkerhedsmaessigeovervejelservedcloudcomputingogoutsourcing.aspx
- **Datatilsynets hjemmeside**
  http://www.datatilsynet.dk
- **Artikel 29-gruppens udtalelser**
  http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm
- **Hennings LinkedIn-profil**
  https://www.linkedin.com/in/henning-mortensen-343b0/ (connect gerne)