

IT-sikkerhed:

Privacy og data protection

GDPR lovgivningen

Privacy by Design/Data Protection Engineering

Privacy Technologies

Carsten Jørgensen
Department of Computer Science
25. oktober 2024



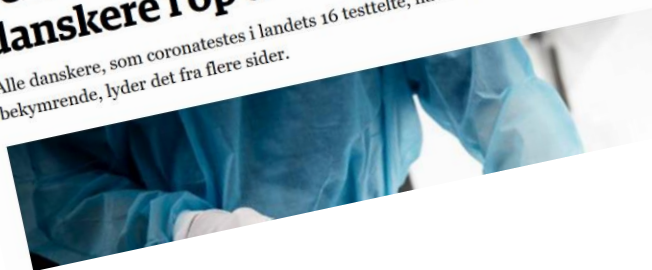
Fortsat fra forelæsningen d.21.oktober

Privacy vs. Data Protection



Privacy er ikke noget nyt

31.05.2020 KL. 20:45
Seruminstitut gemmer dna fra coronatestede danskere i op til 10 år efter deres død
 Alle danskere, som coronatestes i landets 16 testte, havner med dna-spor i Danmark bekymrende, lyder det fra flere sider.



Københavns Politi vil have adgang til ansigtsgenkendelse
 tre og DF støtter politiets ønske om ansigtsgenkendelse, mens regeringen
 r, at det er nødvendigt.

Det er kulturelt hvor meget man deler

Men der har altid været ting man holdt for sig selv –
 Man fortalte ikke naboen hvor på marken man havde
 begravet sin guldskat, uanset hvor tæt man boede

Privacy: tidselementet og hukommelsen



De ved du gik på
gaden, men (hvis du
havde tøj på) kan de
ikke huske hvad
dag, hvad tid eller
hvad tøj

Teknologi ændrer
fundamentalt

Privacy

Privacy drejer sig om kontrol over data:

Hvem får data, hvordan bliver det brugt, gemmer
de det, hvem bliver data delt med og kan man få
det slettet



Grundprincipper

Fair Information Practices (FIPs) - 1970ies (5 regler)

1. User should know about the data collection
2. User should be able to see collected data
3. Data should only be used for the purpose data was collected for
4. User can correct, amend or delete collected data
5. Data should be securely stored

(Ingen "collection limitations")



Den Europæiske Unions Charter om Grundlæggende Rettigheder

Artikel 7 Charter: Respekt for privatliv og familieliv

Enhver har ret til respekt for sit privatliv og familieliv, sit hjem og sin kommunikation.

Artikel 8 Charter: Beskyttelse af personoplysninger

1. Enhver har ret til beskyttelse af personoplysninger, der vedrører den pågældende.
2. Disse oplysninger skal behandles rimeligt, til udtrykkeligt angivne formål og på grundlag af de berørte personers samtykke eller på et andet berettiget ved lov fastsat grundlag. Enhver har ret til adgang til indsamlede oplysninger, der vedrører den pågældende, og til berigtigelse heraf.
3. Overholdelsen af disse regler er underlagt en uafhængig myndigheds kontrol.



GDPR EU-lovgivning

En "forordning", dvs lovgivningen er "ens" i alle EU-landene

Lovgivningen betyder bl.a.:

- Der kan udstedes bøder på op til 100 millioner euro eller op til 4% af en koncerns globale årlige omsætning
- Krav om underretning inden 72 timer ved sikkerhedsbrister (data breach notifikation) med datatab til Datatilsynet - og i nogle tilfælde alle de berørte kunder



Nye GDPR EU-lovgivning

Mange virksomheder skal udnævne DPO'er:
Data Protection Officers/Databeskyttelsesrådgivere

- DPIA - Privacy Impact Assessments
(risikovurderinger)
- Gruppesøgsmål
- Data protection by design and by default



Hvad forstås ved personoplysninger?

Enhver form for information om en identificeret eller identificerbar fysisk person

Identificerbar: direkte eller indirekte identifikation gennem f.eks. navn, ID-nummer, journal nr. osv.

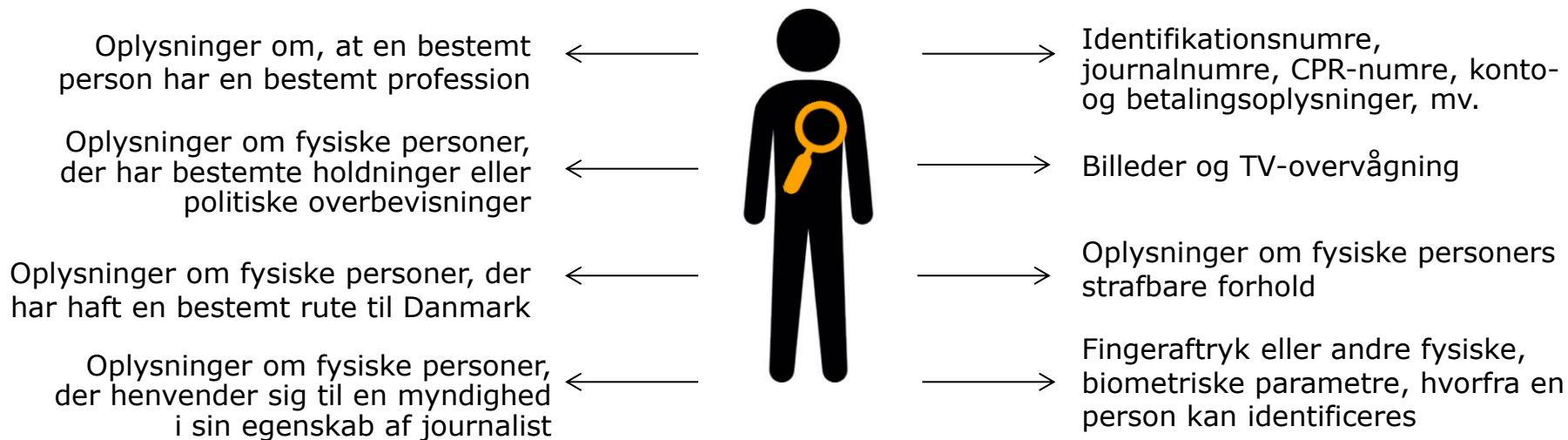
Alle rimelige hjælpemidler skal tages i betragtning

Både subjektive oplysninger (vurderinger) og objektive oplysninger



Eksempler på personoplysninger

"Enhver form for information om en identificeret eller identificerbar fysisk person (den registrerede)"



Billeder og TV-overvågning i USA?

Personoplysninger

Opdeles i to niveauer:

(Ikke personhenførbare oplysninger)

- Almindelige, ikke-følsomme personoplysninger
- Følsomme personoplysninger
(f.eks. oplysninger om helbred, race, politisk baggrund, religiøs overbevisning mv.)
- Andre typer af følsomme personoplysninger
(eksempelvis oplysninger om strafbare forhold, væsentlige sociale problemer mv.).
- Oplysninger til bedømmelse af økonomisk soliditet og kreditværdighed



Personoplysninger

Udgangspunktet er:

Almindelige, ikke-følsomme personoplysninger må
gerne behandles (til udtrykkeligt angivet lovligt formål)

Følsomme personoplysninger (f.eks. oplysninger om
sundhed, race, politisk baggrund, religiøs overbevisning
mv.) må IKKE behandles

**“collected for specified,
explicit
and legitimate purposes”**

Article 7

Respect for private and family life

Everyone has the right to respect for his or her private and family life, home and communications.

Article 8

Protection of personal data

1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed ~~fairly for specified purposes and on the basis of the consent~~ of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.

Legitim interesse

MediaMarkt, Inc.	Legitimate Interest <input checked="" type="checkbox"/>	Consent <input type="checkbox"/>	+
Sharethrough, Inc		Consent <input type="checkbox"/>	+
Smaato, Inc.	Legitimate Interest <input checked="" type="checkbox"/>	Consent <input type="checkbox"/>	+
Visarity Technologies GmbH	Legitimate Interest <input checked="" type="checkbox"/>	Consent <input checked="" type="checkbox"/>	+
Semasio GmbH		Consent <input type="checkbox"/>	+
Crimtan Holdings Limited	Legitimate Interest <input checked="" type="checkbox"/>	Consent <input type="checkbox"/>	+
Scene Stealer Limited	Legitimate Interest <input checked="" type="checkbox"/>	Consent <input type="checkbox"/>	+
Betgenius Ltd		Consent <input type="checkbox"/>	+
TreSensa Technologies, Inc.	Legitimate Interest <input checked="" type="checkbox"/>	Consent <input type="checkbox"/>	+
Tapad, Inc.		Consent <input type="checkbox"/>	+
Teroa S.A.		Consent <input type="checkbox"/>	+
Criteo SA		Consent <input type="checkbox"/>	+
1plusX AG	Legitimate Interest <input checked="" type="checkbox"/>	Consent <input type="checkbox"/>	+
Adloox SA			+

[Manage Settings](#)[Save Settings & Exit](#)[Continue with Recommended Cookies](#)

Samtykke

Et samtykke skal være en frivillig, specifik, informeret og utvetydig viljestilkendegivelse

Dataansvarlige skal kunne bevise, at datasubjektet har samtykket til behandlingen

Hvis samtykket gives skriftligt i en erklæring, der også vedrører andre forhold, skal en anmodning om samtykke forelægges på en måde, som klart kan skelnes fra de andre forhold

Samtykket kan gives mundtligt og skriftligt, herunder elektronisk

Afkrydsning af felt på hjemmeside – opt in, men ikke opt out (forudafkrydsede felter)

Ikke stiltiende samtykke



Grundlæggende principper i GDPR

Personoplysninger skal behandles

- a) lovligt, rimeligt og på en gennemsigtig måde i forhold til den registrerede ("lovlighed, rimelighed og gennemsigtighed")
- b) indsamles til udtrykkeligt angivne og legitime formål og må ikke viderebehandles på en måde, der er uforenelig med disse formål ("formålsbegrænsning")
- c) være tilstrækkelige, relevante og begrænset til, hvad der er nødvendigt i forhold til de formål, hvortil de behandles ("dataminimering")
- d) være korrekte og om nødvendigt ajourførte ("rigtighed")
- e) opbevares på en sådan måde, at det ikke er muligt at identificere de registrerede i et længere tidsrum end det, der er nødvendigt til de formål, hvortil de pågældende personoplysninger behandles ("opbevaringsbegrænsning")
- f) behandles på en sikker måde ("integritet og fortrolighed").

Artikel 8 Charter: Beskyttelse af personoplysninger

1. Enhver har ret til beskyttelse af personoplysninger, der vedrører den pågældende.
2. Disse oplysninger skal behandles rimeligt, til udtrykkeligt angivne formål og på grundlag af de berørte personers samtykke eller på et andet berettiget ved lov fastsat grundlag. Enhver har ret til adgang til indsamlede oplysninger, der vedrører den pågældende, og til berigtigelse heraf.
3. Overholdelsen af disse regler er underlagt en uafhængig myndigheds kontrol.

Grundlæggende principper i GDPR – Behandlingssikkerhed (Artikel 32)

*Under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder gennemfører den dataansvarlige og databehandleren **passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til disse risici**, herunder bl.a. alt efter hvad der er relevant:*

- a) pseudonymisering og kryptering af personoplysninger*
- b) evne til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester*
- c) evne til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse*
- d) en procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed.*



Persondata og AI – to pointer

Hvis **samtykke** udgør det retlige behandlingsgrundlag skal det være "frivilligt, specifikt, informeret og udtryk for en utvetydig viljetilkendegivelse". Et samtykke kan trækkes tilbage!

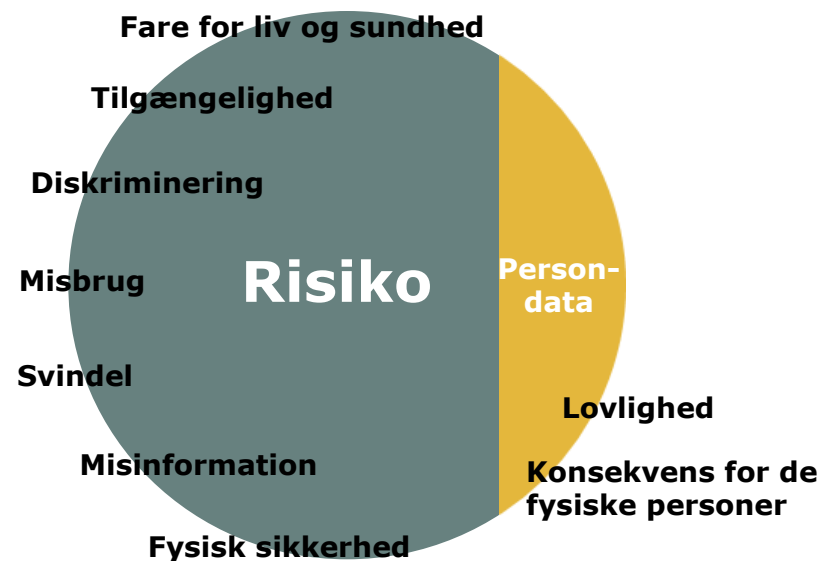
Automatiske afgørelser:

GDPR indeholder et generelt forbud imod afgørelser, "der alene er baseret på automatisk behandling, herunder profilering, som har retsvirkning eller på tilsvarende vis betydeligt påvirker den pågældende"



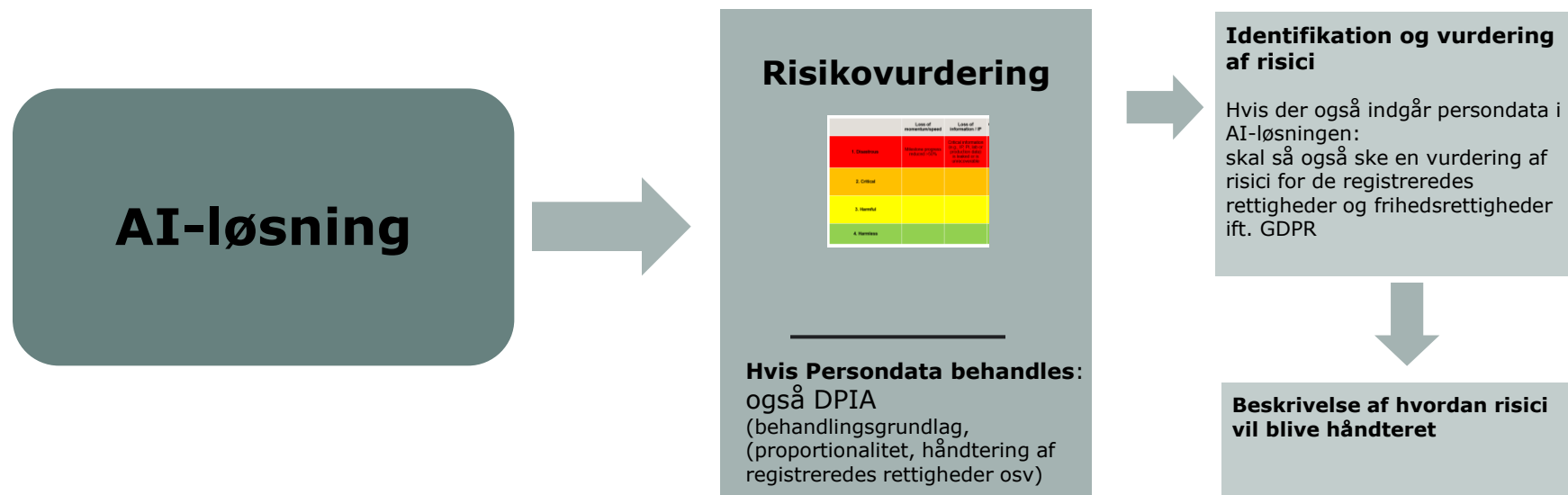
Risiko

Persondata og AI



“Det er Datatilsynets opfattelse, at behandling af personoplysninger som led i **udvikling og/eller drift** af AI-løsninger **næsten altid** vil udløse flere af de kriterier, der er udslagsgivende for, om der skal gennemføres en konsekvensanalyse.” s.37

Sikkerhedskrav **skal** baseres på risikovurderinger



"De registreredes" rettigheder

Adgang til data om sig selv
Få data om sig selv rettet eller slettet

- Ikke uforholdsmæssig/overdreven i forhold til indsamlingsformålet
- Nyt samtykke ved ændring af formål



Undtagelserne – her gælder forordningen ikke

- Aktiviteter af ren privat eller familiemæssig karakter
 - F.eks. korrespondance, føring af adressefortegnelse eller sociale netværksaktiviteter og den type onlineaktiviteter
- Aktiviteter uden for EU-retten, f.eks. national sikkerhed
- Den fælles udenrigs- og sikkerhedspolitik
- Særlige regler for politi, anklagemyndighed og domstole
- Behandlinger i EU's institutioner



Ret til at blive slettet?



Persondata loven

Samtykke er ikke altid nødvendigt
Overførsel til udlandet
"Behandling" af data

- Er en IP-adresse persondata?
- Hvorfor er et foto af en person jeg ikke kender persondata?
- IT-support i Indien?



Privacy / Databeskyttelse (Data Protection)

Firmaet DIKUprod indsamler forskellig persondata om sine kunder bl.a. navn, adresse, mail og telefonnummer

DIKUprod er begyndt at bruge Amazon Web Services (AWS) cloud løsninger. Persondata overføres til AWS



Privacy / Databeskyttelse (Data Protection)

Hvem ejer den persondata DIKUprod overfører til AWS?

Firmaet DIKUprod indsamler forskellig persondata om sine kunder bl.a. navn, adresse, mail og telefonnummer

DIKUprod er begyndt at bruge Amazon Web Services (AWS) cloud løsninger. Persondata overføres til AWS



Privacy / Databeskyttelse (Data Protection)

Privacy drejer sig om (din) kontrol over data:

Hvem får data, hvordan bliver det brugt, gemmer de det, hvem bliver data delt med og kan man få det slettet

Privacy != Secrecy

Man kan ikke skjule noget for big data, men man kan lave regler
- og der kan være konsekvens hvis nogen bryder reglerne



Privacy / Databeskyttelse er ikke secrecy

↻ the grugq Retweeted



Jessy Irwin ✨
@jessysaurusrex

Defeating Facial Re
doesn't have



privacy isn't
about hiding,
it's sharing
on ur terms

(_)/ ||
(•人•) ||
/ づ

22/12/2016, 19.46



Mit nye firma Privacy i en cloud-verden?



Mit nye firma

Rådmand vil registrere nattens ballademagere

Rådmand i Århus vil - som et forsøg - op

Rådmand Gert Bjerregaard (V) fremsender
forhører sig om mulighederne for på fors
natteliv.

- I dag kan en ballademager, der allerede
fortsætte "festen" på naborestauranten.

Når politiet har givet et tilhold, skal pe
er et kraftigt signal og en sanktion, der

- Det forudsætter dog et fælles register
kunne godt tænke mig at indføre en for
Espersen om mulighederne for at starte



SKREVET AF MORTEN ESPERSEN

BRØNDBY: GIV OS LOV TIL AT REGISTRERE BALLADEMAGERE

Brøndby beder politikerne om lov til at registrere ballademagerne til klubbens kampe.

👍 Synes godt om 5 personer synes godt om dette.

Brøndby har de seneste dage fået skudt i skoene, at de ikke gør nok for at forhindre ballademagere til klubbens kampe. Brøndby vil ikke registrere klubbens udebanefans, men vil gerne registrere ballademagerne, hvilket de dog ikke må. Direktør Ole Palmå gør opmærksom på, at Brøndby altså bruger mange resurser på fan-arbejde.

- Dette er DBU vidende om og det burde alle politikere være orienteret omkring både i folketinget og i Københavns Borgerrepræsentation! Hvis de er i tvivl om vores indædte lyst til og store arbejde for at minimere ballade i forbindelse med fodboldkampe, vores

Ritt: Ballademagere skal registreres

08. jan. 2008 18.14 Indland

Københavns overbørmeester Ritt Bjerregaard er nu parat til
system, der kan udelukke voldelige
eker i hovedstadens natliv.

al kunne registrere og afvise
tilhold af politiet, oplyser
ariat. Initiativet kommer efter den
og knivstikkerier.

anisation, Horesta, jubler over
Commune.

ringssystem på landsplan, men det
som har været fremsynet, set
taget det seriøst, siger Gry Asnæs
for Horesta Natliv.

aurationer ikke registrere
e, der har solgt narko eller
ingssystemet kræver derfor en



Superligaen
Matches

Odense BK - Brøndby
IF

06/11 17:00

2.00 3.35 3.65



Hvad var problemet?

TÆNK

FORBRUGERRÅDET | BLIV MEDLEM

FORSIDEN

TESTRESULTATER

NYHEDER

GODE RÅD

VÆR

Hvad søger du?:

Søg

Genveje: [Køb adgang](#) [Klager](#) [Aftaler og køb](#)

[Presse](#) » Bølleregister skal være mere sikkert

Bølleregister skal være mere sikkert

Vi er alle interesserede i et sikkert natteliv. Men det skal ikke ske på bekostning af vores privatliv, skriver Forbrugerrådet i et høringssvar til Justitsministeriet.

Af Charlotte Friis Eriksen

Sikkerheden skal være i top, når danskerne går i byen. Og det kommende registreringssystem, også kaldet bølleregistret, kan holde ballademagerne ude af landets diskoteker og barer.

Men sikkerheden i systemet skal forbedres. Det skriver Forbrugerrådet i et høringssvar til bekendtgørelsen om bølleregistret, der har det formelle navn "Bekendtgørelse om videregivelse og behandling af oplysninger om restaurationsforbud".

[Læs hele høringssvaret som pdf](#)

Oplysningerne kan udnyttes

Bøllerne er ikke de eneste, der registreres. Alle gæster vil ifølge diskoteks- og restaurationsbranchen kunne blive bedt om at oplyse navn, cpr-nummer, fingeraftryk, e-mail og foto.

Derfor er det meget vigtigt, at alle gæsternes oplysninger behandles på den rigtige måde, skriver Forbrugerrådet i høringssvaret til Justitsministeriet. Ellers kan oplysningerne udnyttes kommercielt eller personligt.

Kunderne bør anonymiseres

"Det er fuldt forståeligt, at restaurationsbranchen vil holde bøllerne ude. Men man kan sagtens indsamle oplysningerne og samtidig kryptere dem, så hver kunde ikke kan identificeres med navn og cpr-nummer," siger Anette Høyrup, jurist i Forbrugerrådet.

Anonymiseringen kan blandt andet ske ved at tildele gæsterne numre, så de bliver uidentificerbare for andre end diskoteket eller baren. Anette Høyrup henviser til IT- og Telestyrelsens anbefalinger om nye digitale sikkerhedsmodeller.

[Læs IT- og Telestyrelsens anbefalinger om nye digitale sikkerhedsmodeller \(pdf\)](#)

Sikkerheden skal følge tiden



LÆS OGSÅ OM

[Private registre ude af kontrol](#)
[Forbrugere fanges i databaser](#)

ANDRE HAR SET

[Virksomheder har et ansvar](#)

Mit nye firma

Mit nye firma tilbyder:

- Gratis kameraer med ansigtsgenkendelse til alle danske barer og diskoteker !
- Ingen registrering af navn, CPR eller anden personlig information – kun *foto og køn*

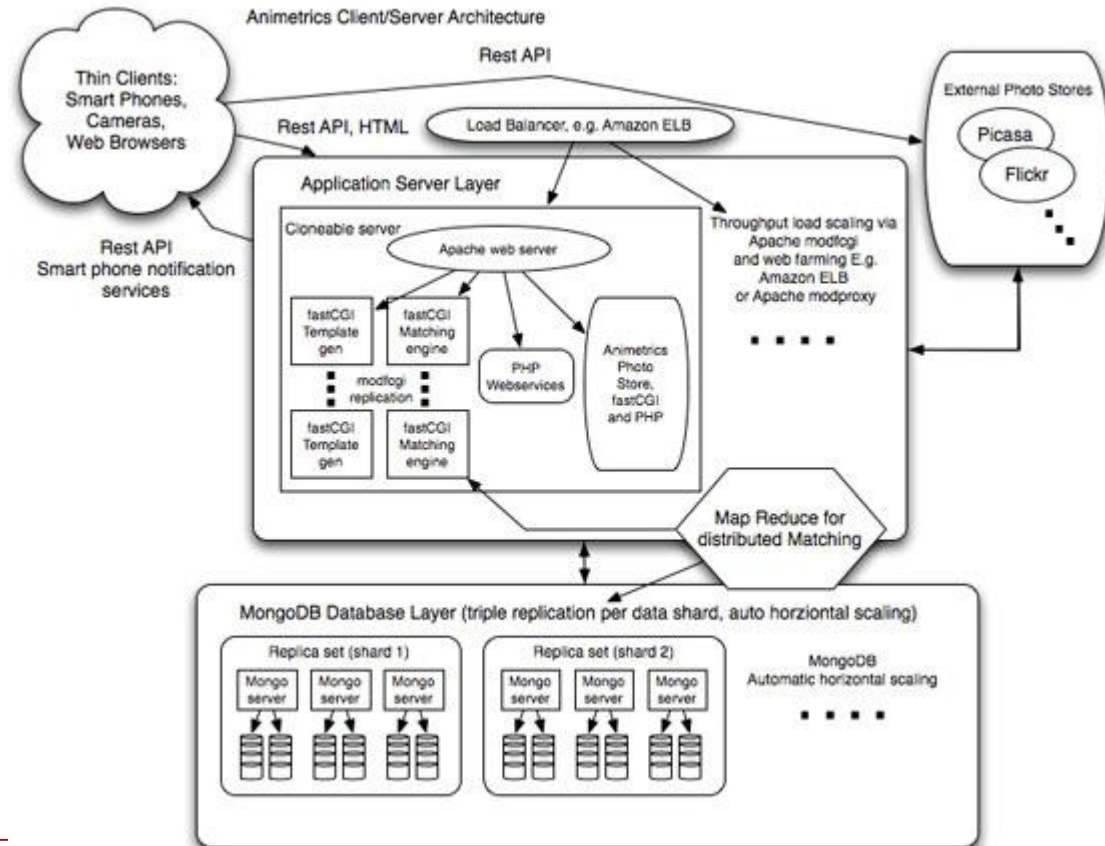


Mit nye firma

Mit nye firma tilbyder:

■ Cloud løsning, Serverless og webservices, alt over internettet

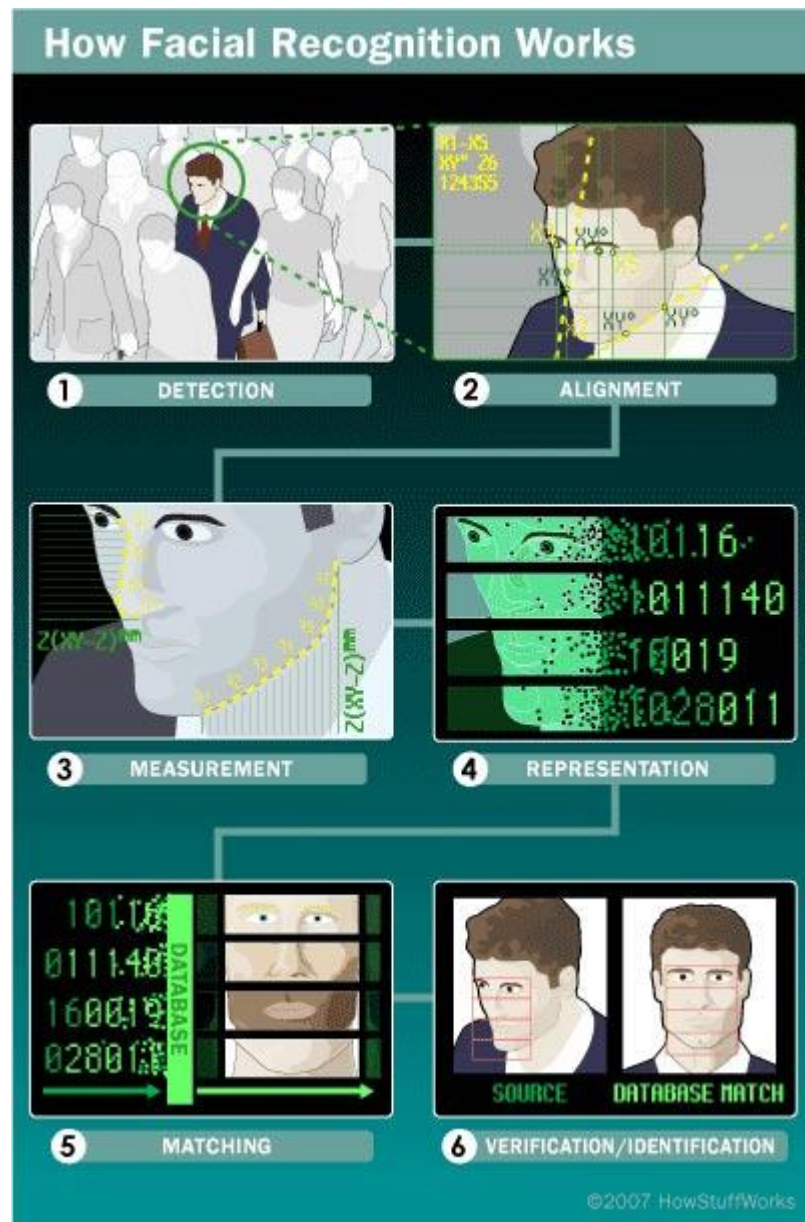
■ AI behandling



Mit nye firma

Mit nye firma tilbyder:

- Hurtig genkendelse, efter registrering.
- Ingen kø !
- Gratis udstyr og gratis deltagelse for alle barer og diskoteker



Mit nye firma

Hvad får de – og hvad får jeg?



Mit nye firma

Hvad får jeg – egentlig?

- Liste over kendte ballademagere (kan sælges)
- Hvor er pigerne – lige nu
- Hvilke barer og andre steder er populære

Og hvad så?



Mit nye firma

Hvad får jeg – egentlig?

- Hvor skal der reklameres i byen
- "Få en gratis drink hvis du ..."
- Gå i Byen App
- Få en gratis cocktail, når du alligevel skal forbi Salon 39



Mit nye firma

Hvad får jeg – egentlig?

- Map til Facebook...
 - Gratis information, begrænset aldersrum,
 - Skal kun bruge DK-profiler, køn og byer er kendt

Teknisk muligt – men er det også lovligt i EU?
hvad med USA?

En løsning med bedre data beskyttelse?

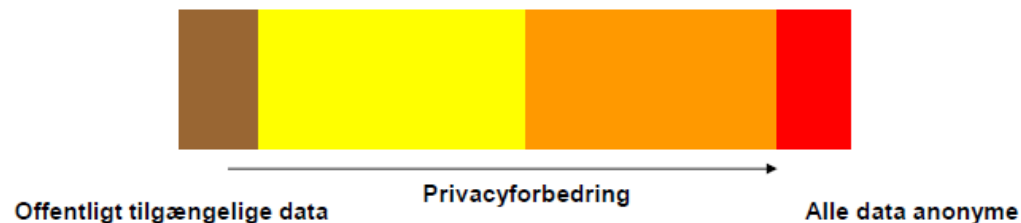


Privacy overvejelser

Designvalg
Privacy vurderinger

Privacy by Design
Privacy Enhancing Technologies
Data Privacy Engineering

Model for privacy



Privacy by Policy

Pause

© MARK ANDERSON

WWW.ANDERZTOONS.COM



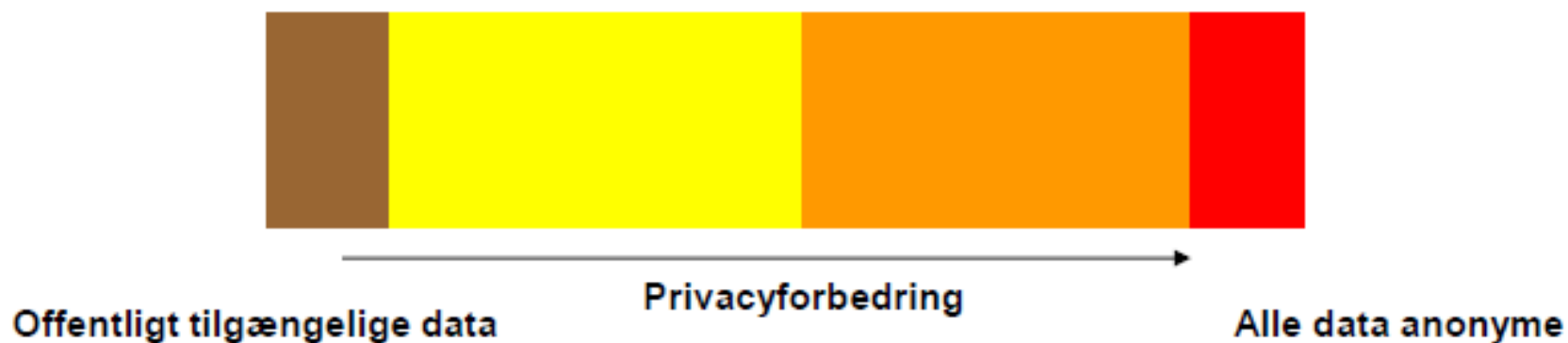
"Before I write my name on the board, I'll need to know how you're planning to use that data."

Privacy forbedringer



Privacy model

Model for privacy



Hvor vil i ligge – for den specifikke løsning?



Digital identitet - Trusler imod privacy

Forskel på kontanter og Dankort når
du køber en flaske vin i et
supermarked?



PIA og DPIA

**(Privacy Impact Assessments
og
Data Protection Impact Assessments)**



Privacy – risiko vurderingen er stadig vigtig

Threat model:

Skal der beskyttes imod uheld eller imod bevidste angreb imod privacy?

Hvem skal der beskyttes imod:

Global overvågning, virksomheden selv, 3.part, delt it-udstyr hos brugerne, eller imod andre brugere af tjenesten?

Konsekvens for de registrerede, ikke for virksomheden selv



PIA – Privacy Impact Assessment

Overvej:

Den data der indgår

Følsomhed, hvad bruges data til, potential konsekvens ved brud osv

Teknologierne der bruges

Nye/ukendte, "intrusive" osv

Data-flows

Hvordan data indsamles, opbevares, bruges , slettes –

I organisationen, udenfor organisationen, udenfor EU osv



Start med persondata-flow analyse

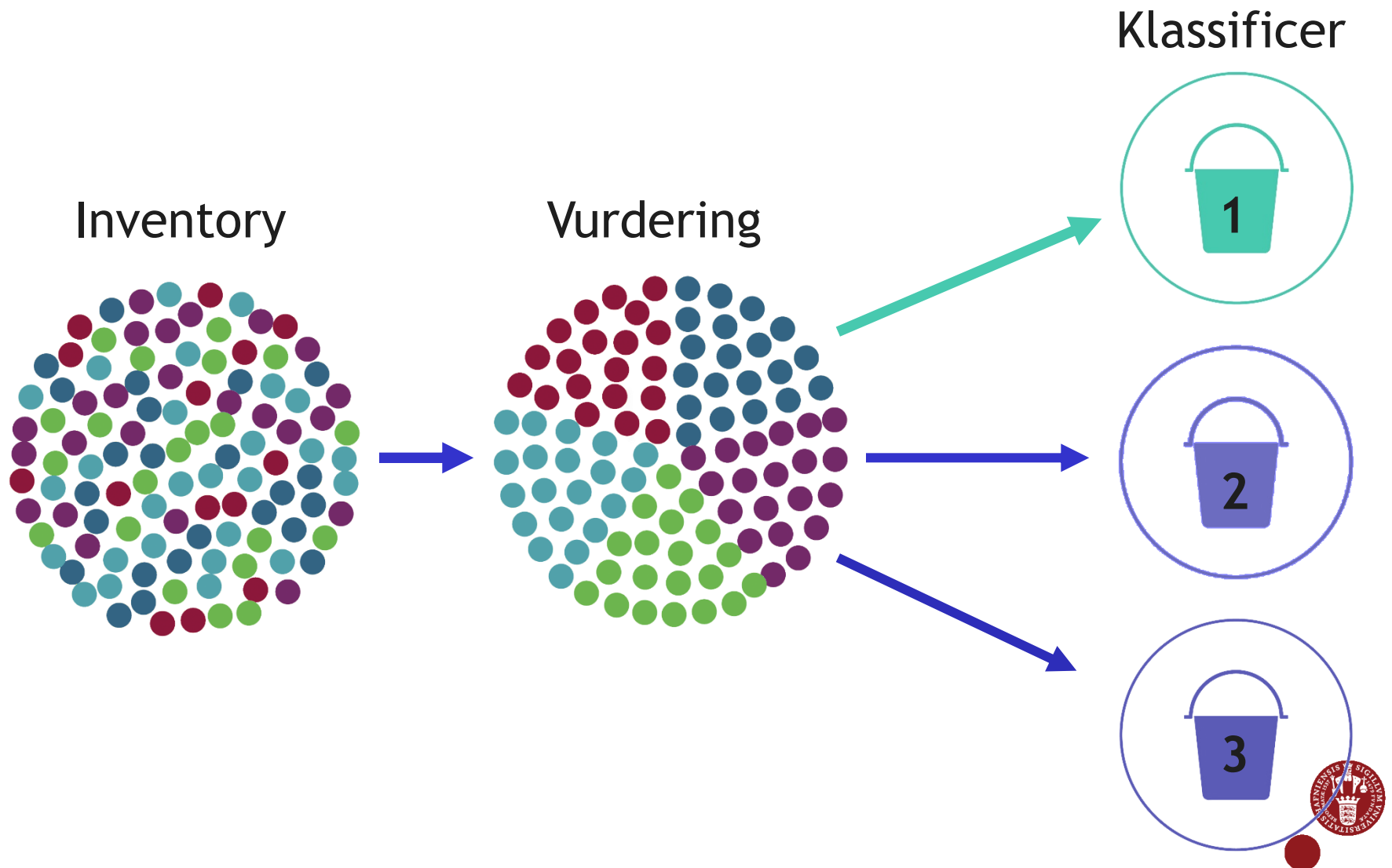
Skab overblik:

Dataflow analyse skal afklare:

- Hvor kommer persondata ind?
- Hvor går data hen?
- Hvor får 3.parties adgang til persondata?
- Er databehandleraftaler mm på plads?
- Hvad er hjemmelsgrundlag? (lovgrundlaget)
- Osv



Data klassifikation



Persondata – dokumenter, skab overblik

Persondatalovens sikkerhedskrav

Udgangspunktet for loven er, at en løsning der behandler persondata ALTID skal overholde de nedenstående 12 grundkrav:

Grundlæggende krav	
1. Er der lavet en risikovurdering?	Kravene til en løsning skal altid vurderes ud fra de specifikke omstændigheder. Man skal derfor ALTID lave en risikovurdering og en Privacy Impact Assessment, der beskriver hvilke ekstra krav, udover de 12 grundkrav, den specifikke løsning kræver.
2. Bliver persondata behandlet sikkert?	Der skal være sikkerhedspolitikker, procedurer og andre retningslinier i virksomheden, der beskriver, hvordan it-sikkerheden konkret er etableret i organisationen. Lokale sikkerhedspolitikker/procedurer kan være nødvendige. Politikker, procedurer og retningslinier skal efterleves, overholdelsen kan revideres af ekstern it-revision.
3. Ved medarbejderne hvordan de skal behandle persondata sikkert?	Medarbejdere, der behandler persondata skal instrueres i hvordan de skal behandle data. (Der skal være awareness aktiviteter i forhold til sikkerhedspolitikker, procedure og persondataloven)
4. Er kontrakter på plads med underleverandører?	Der skal være etableret skriftlige aftaler med databehandlere til sikring af, at datasikkerheden lever op til persondataloven, samt at den dataansvarlige påser dette. Dvs er databehandler aftaler og underdatabehandler aftaler på plads?

Krav kan ligge både i den underliggende infrastruktur og i den daglige brug af en applikation/løsning:

Infrastruktur	Applikationen
5. Fysisk adgangskontrol Uautoriseret adgang skal kontrolleres. Dette dækker fra begrænset adgang til	5. Fysisk adgangskontrol Fysisk adgang til applikationen/anden persondata skal beskyttes.



Overvej om der kan defineres standard sikkerhedskrav

Minimumskrav skal efterfølges af risikovurderingen

	MINIMUMSKRAV (RED-LINE/BASE-LINE)	MEDIUM KRAV	HØJE KRAV
GRUNDSIKKERHED			
		X	X
		(X)	X
	X	X	X
		(X)	(X)
PERSON DATA			
	X	X	X
	X	X	X
	X	(X)	X
		(X)	X
(...)			

X = Minimumskrav (X) = Optional (når påkrævet)



Privacy by Design

Databeskyttelse Transparens, bruger-kontrol mm



Privacy by Design – hvordan kan man opnå transparens

Privacy policies Privacy dashboards

Gennemsigtig oplysning, meddelelser og nærmere regler for udøvelsen af den registreredes rettigheder:

*Den dataansvarlige træffer passende foranstaltninger til at give enhver oplysning som omhandlet i artikel 13 og 14 og enhver meddelelse i henhold til artikel 15-22 og 34 om behandling til den registrerede i **en kortfattet, gennemsigtig, letforståelig og lettilgængelig form og i et klart og enkelt sprog**, navnlig når oplysninger specifikt er rettet mod et barn.*

GDPR artikel 12



Privacy by Design

Usability



Privacy by Design

Transparens er et krav i GDPR – "de registrerede" skal forstå **HVORFOR** deres persondata bliver indsamle og **HVORDAN** det bliver behandlet



Brugerens mentale model

The image shows a Google search interface for the query "dansende panda". The search results are partially visible in the background, showing image and video thumbnails. A white modal dialog box is overlaid on the search results, containing a Google logo, a language selector set to "Dansk", and the heading "Inden du fortsætter". The dialog text explains that to comply with data protection laws, users must review Google's privacy policy. It includes icons for Google services (Gmail, YouTube, Maps, etc.) and a blue button labeled "NÆSTE" (Next).

Google

dansende panda

Alle Billeder Videoer Shopping

Ca. 1.470.000 resultater (0,29 sekunder)

Billeder af dansende panda

Flere billeder af dansende panda

Videoer

Dansende panda

B Karso
YouTube - 23. feb. 2015

Dancing f

Cy Shimizu
YouTube - 3

Google

Dansk

Inden du fortsætter

For at overholde lovgivningen om databeskyttelse beder vi dig om at gennemgå de vigtigste punkter i Googles privatlivspolitik. Det er ikke, fordi vi har ændret noget – det er blot en mulighed for at se de vigtigste punkter.

Dette er nødvendigt, for at du kan fortsætte med at bruge Google-tjenester.

NÆSTE

Usability and Psychology

Eksempler er f.eks.

- Sikre defaults/standard indstillinger

- Privacy icons

- Korte tekster, med mulighed for mere information

- Just in time

- Feedback

- Path of least resistance

- OSV, OSV



Privacy by Design

Privacy Enhancing Technologies (PETs)



Privacy by Design - PETs



3 forskellige nøgler:

Er det ikke lettere at have den samme nøgle til hoveddøren som til pengeskabet og til cykellåsen ?

Risiko og forskellige sikkerhedsniveauer

Digital identitet

Diagnose baseret på blodprøve:

a) CPR = samme nøgle

- Identificeret overfor lægen
- Identificeret overfor laboratoriet

b) Ingen sammenkædning

- Ikke identificeret overfor laboratoriet
- (Måske) ikke identificeret overfor lægen

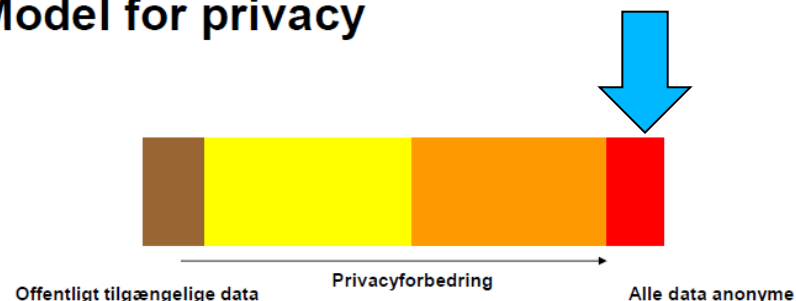


Privacy by Design – Privacy Enhancing Technologies

- **Transaktionsisolering/transaktionsanonymisering**
- **Anonymous credentials ("Kontekstafhængige akkreditiver")**
- **Formålsspecifikke nøgler**

Formålet er ofte ikke "identifikation af en bruger" men at få valideret et sikkerhedsaspekt ("er over 18", "kvinde", "er aktiv studerende ved DIKU", "er dansk statsborger")

Model for privacy



Identity og privacy

Selektiv afsløring af attributter fra akkreditiv

CPR: [REDACTED]
Kommune: [REDACTED]
Køn: [REDACTED]
Alder: >18 år

Bruger kan ikke direkte sammenkædes på tværs af serviceudbydere

Serviceudbyder 1

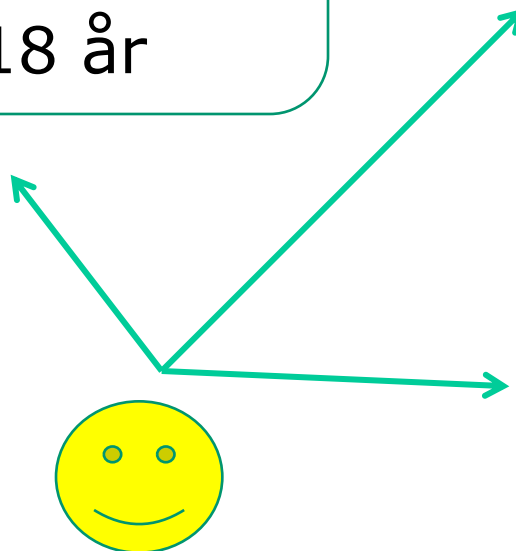
CPR: [REDACTED]
Kommune: [REDACTED]
Køn: [REDACTED]
Alder: >18 år

Serviceudbyder 2

CPR: [REDACTED]
Kommune: KBH
Køn: [REDACTED]
Alder: [REDACTED]

Serviceudbyder 3

CPR: [REDACTED]
Kommune: [REDACTED]
Køn: [REDACTED]
Alder: >18 år



Transaktionsanonymisering vs. kommunikationsanonymisering

Kommunikationsanonymisering:

Bevidst: Ingen registrering af IP-adresser, mail, telefonnumre, cookies, device-ids, mac-adresser osv., osv

Øger sandsynligheden for virksomhed ikke kan identificerer parter

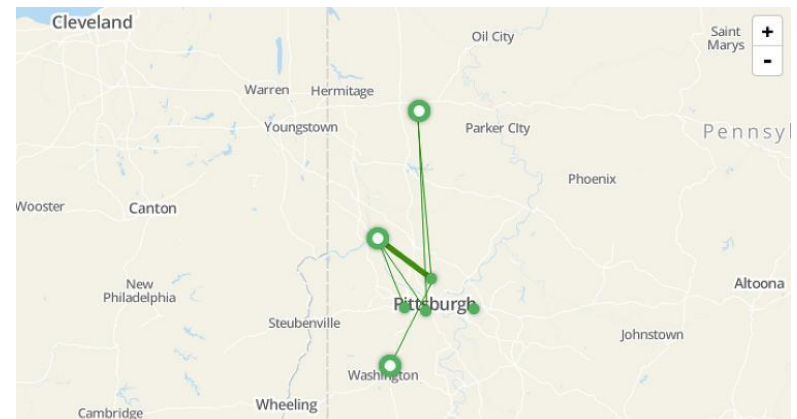
Se f.eks. Whistleblower systemer



Privacy by Design - dataminimering

Save/compute: On device vs in the network

Undgå unikke identifiers



Et par privacy by design eksempler



Movia



Slut med overvågning billetkontroll

Fra i dag er Movias billetkontrollører udstyret med bodycams på uniformen.

FAKTA Sådan behandles

ØKONOMI 8. JAN. KL. 11.25

Billetkontrollører får kameraer på uniformen efter flere trusler, spark og slag

Fra i dag bliver ansatte i Movia udstyret med bodycams.



Må man det?

Straffelovens § 263, stk. 1

"Med bøde eller fængsel indtil 6 måneder straffes den, som uberettiget

...

3) ved hjælp af et apparat hemmeligt aflytter eller optager udtalelser fremsat i enrum, telefonsamtaler eller anden samtale mellem andre eller forhandlinger i lukket møde, som han ikke selv deltager i, eller hvortil han uberettiget har skaffet sig adgang."

Argumenter

- Ikke "hemmelig" optagelse
- Kontrolløren deltager i samtalen
- Ikke forsæt til at optage bi-personer



Må man det?

Straffelovens § 263, stk. 1

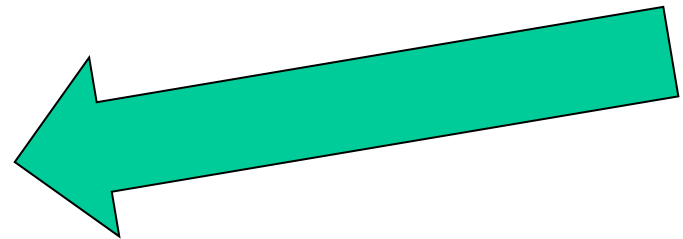
"Med bøde eller fængsel indtil 6 måneder straffes den, som uberettiget

...

3) ved hjælp af et apparat hemmeligt aflytter eller optager udtalelser fremsat i enrum, telefonsamtaler eller anden samtale mellem andre eller forhandlinger i lukket møde, som han ikke selv deltager i, eller hvortil han uberettiget har skaffet sig adgang."

Argumenter

- Ikke "hemmelig" optagelse
- Kontrolløren deltager i samtalen
- Ikke forsæt til at optage bi-personer



Hvad skal der til?

Sådan informerer vi

- Skilt på uniform
- Mundtlig information
- Folder
- Information på website
- Pressemeddelelse
- Interne retningslinjer

Indsigtsret

Personer på optagelsen har indsigtsret;

- Kunder der kontrolleres
- Kontrolløren selv
- Andre (bi-personer)

Hvordan gennemføres indsigtsretten?

- Optagelsen sikres fra sletning
- Teknisk sløring af billede og lyd
- Sikker identifikation af kunden
- Sikker udlevering

Hvad skal der til?

Sikkerhed

- Udleveres kun til politiet
 - Skærm er deaktiveret og password-beskyttet
 - Kontrolløren kan ikke se optagelsen
 - Få medarbejdere har adgang
 - Ved udlevering til politiet
 - Ved håndtering af indsigtsbegæringer
 - Automatisk sletning efter 14 dage
- Tag informationsdelen alvorligt
 - Begræns lagring af optagelser
 - Vær klar til at håndtere indsigtsbegæringer



Data protection technologies



Databeskyttelsesteknikker/privacy engineering i AI/ML

Overvej privacy engineering teknikker til bedre databeskyttelse, som use limitation og andre GDPR-principper.

Vurder f.eks. brugen af **minimeret-, anonymiseret og syntetisk data** hvor muligt

Nyere teknikker inden for ML/AI er for eksempel:

- **Data enclaves:** opbevar grupper af persondata i særligt sikre systemer med yderligere begrænset adgang
- **Federated learning:** decentralisering af ML der undgår behovet for at samle data på ét enkelt sted. I stedet trænes modellen ad flere gange med data på forskellige lokationer



Anonymi

Enhver form for information om
en identificeret eller
identificerbar fysisk person

Identificerbar: direkte eller
indirekte identifikation gennem
f.eks. navn, ID-nummer, journal



Anonymisering >< Pseudonymisering

'Pseudonymous data' means personal data that cannot be attributed to a specific data subject without the use of additional information, as long as such additional information is kept separately and subject to technical and organizational measures to ensure non-attribution;

Anonymt data er **ikke** persondata,
pseudonymiseret data **er** persondata

Anonymisering/pseudonymisering

Anonymisering >< Pseudonymisering

Begrænse risiko ved datatab
Dele data internt/eksternt
Forskning
OSV...

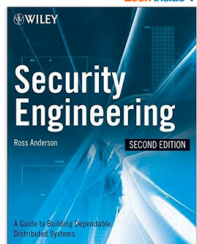


Eksempel på pseudonymisering: Kun adgang til persondata med specifikt arbejdsbehov



Security Engineering: A Guide to Building Dependable Distributed Systems 2nd Edition

by Ross J. Anderson (Author)
★★★★☆ 29 customer reviews



ISBN-13: 978-0470068526
ISBN-10: 0470068523

Kindle	Hardcover	Paperback	Other Sellers
\$61.86	\$21.14 - \$62.46	\$30.75	from \$26.42

☐ Rent \$21.14
☐ Buy used \$34.70
☒ Buy new \$62.46

In Stock. Ships from and sold by Amazon.com. Gift-wrap available.

List Price: \$65.00 Save: \$22.54 (27%)
\$2 New from \$39.98

Want it tomorrow, April 27? Order within 11 hrs 11 mins and choose One-Day Shipping at checkout.

[Add to Cart](#)
 Turn on 1-Click ordering
 Ship to:

Address information for shipping



Frequently Bought Together



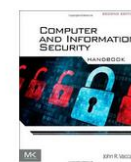
Total price: \$185.91

[Add both to Cart](#)
[Add both to List](#)



- ☒ This item: Security Engineering: A Guide to Building Dependable Distributed Systems by Ross J.
- ☒ Computer and Information Security Handbook, Second Edition by John R. Vacca Hardcover \$123.4

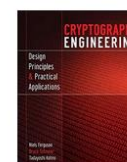
Customers Who Bought This Item Also Bought



Computer and Information Security Handbook,



Threat Modeling: Designing for Security



Cryptography Engineering Design Principles and

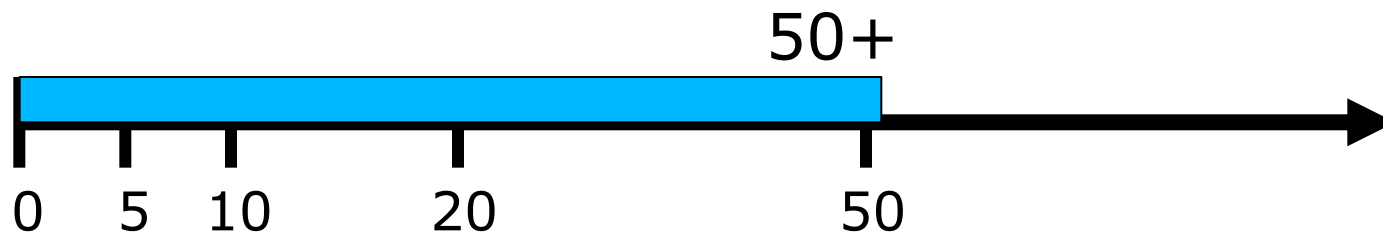


Privacy by Design – dataminimering igennem pseudonymisering

Hvor mange gange har en bruger brugt "Hjælp":



Tydeligt tegn på usability problemer, bør måske overveje vores løsning



Gruppering/"buckets": "Under 5", "Under 10" osv



1b. Pseudonymise personal data as soon as possible

“Pseudonymisering”: udvalgte kategorier af personpdata erstattes med “koder” så data ikke kan henføres til en specific person uden nøglen kendes. F.eks. kan CPR-numre erstattes af en kode, der opbevares et andet sted. (cpr 123456-1234 = ID 12345abc)

Pseudonymiseringen kan give en bedre beskyttelse fordi det ikke umiddelbart er muligt at genkende individer

Husk: pseudonymiseret data er stadig persondata fordi det stadig er muligt at koble oplysningerne sammen



Pseudonymisering

Vi indsamler: CPR, mail, købshistorik, alder. Vi har tre kunder:

CPR	Mail	Købshistorik	Alder
112233-1122	aaa@mail.com	Bog	18
445566-1234	bbb@gmail.com	TV	55
321321-6543	cccc@live.dk	Avis	55

Pseudonymisering af kunde data:

CPR	Mail	Købshistorik	Alder
a	1	Bog	18
b	2	TV	55
c	3	Avis	55

Vi kan nu lave big data:

18 årige fortrækker bøger, 55 årige foretrækker tv og aviser



Men pas på

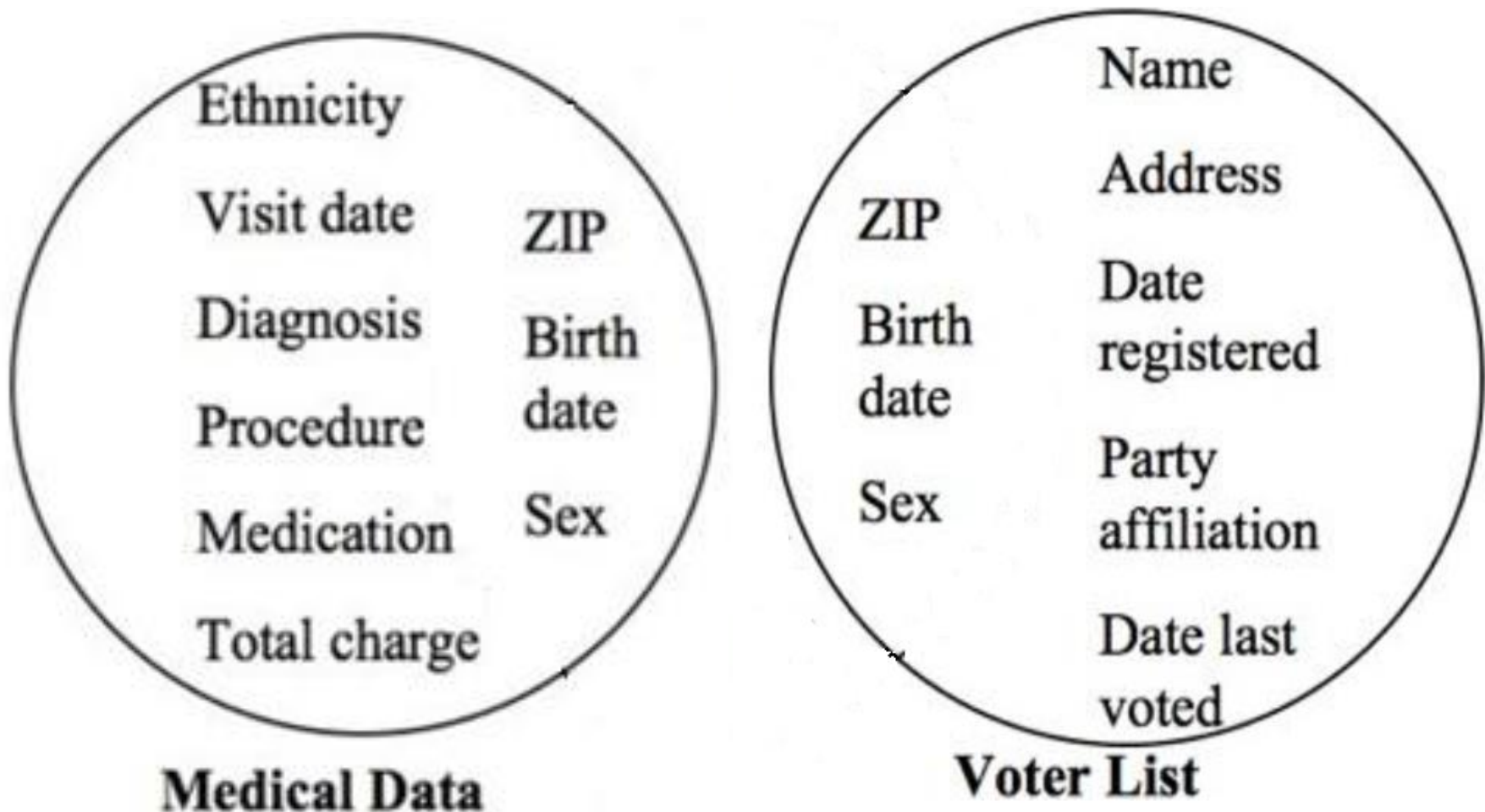
Singling out er muligheden for at isolerer data om et individ

Linkability er muligheden for at sammenkæde to eller flere records i en eller flere databaser
Hvis man kan identificerer at to records matcher same gruppe individer, men ikke bestemme individet i gruppen beskytter teknikken imod “singling out”, men ikke imod linkability

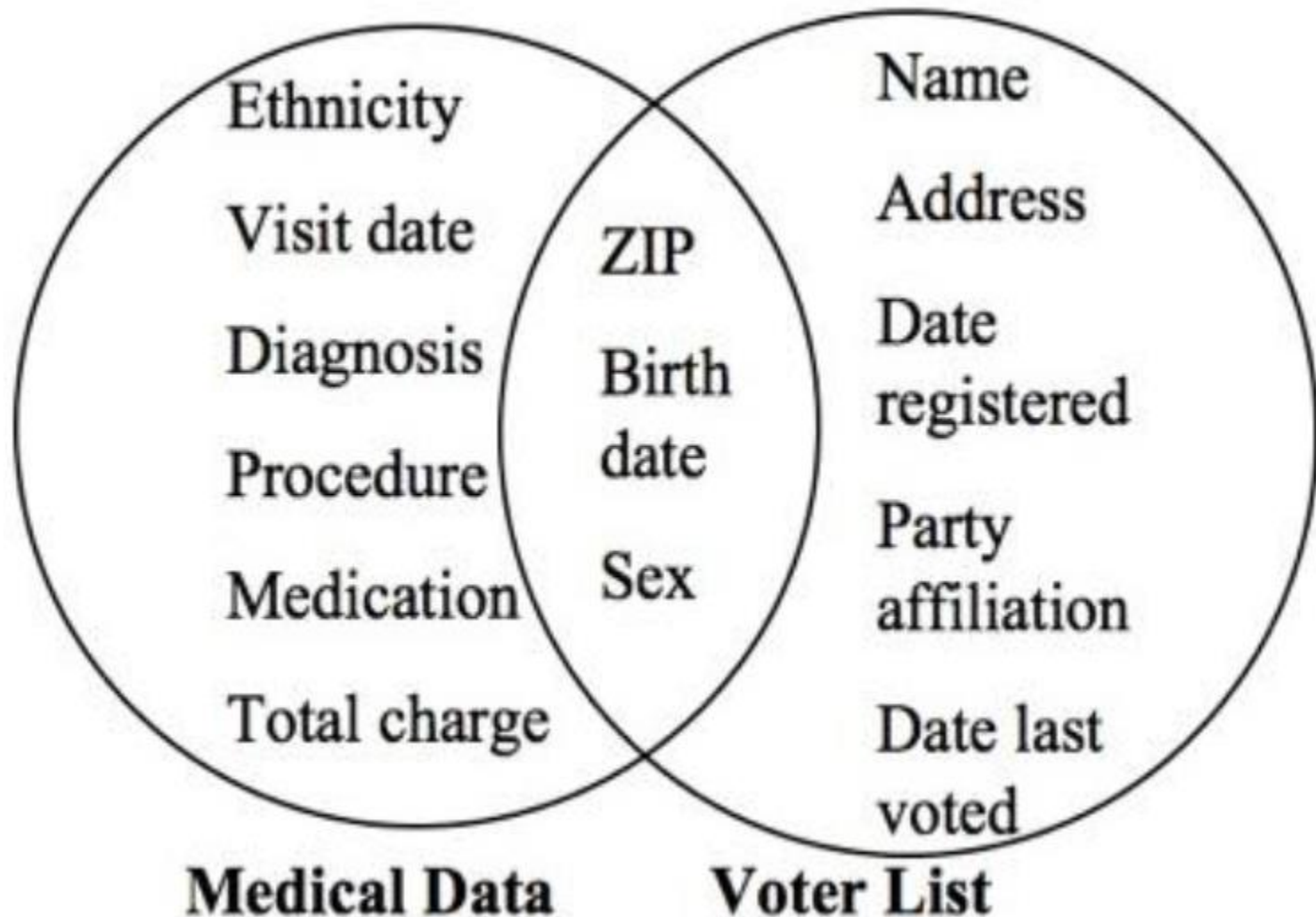
Inference er muligheden for at udlede en værdi udfra en anden værdi.



Anonymising/pseudonymising - linkability



Anonymising/pseudonymising - linkability



Pseudonymisering

Vi indsamler: CPR, mail, købshistorik, alder.
Vi har tre kunder:

CPR	Mail	Købshistorik	Alder
112233-1122	aaa@mail.com	Bog	18
445566-1234	b@gmail.com	TV	55
321321-6543	cccc@live.dk	Avis	55

Pseudonymisering af kunde data:

CPR	Mail	Købshistorik	Alder
a	1	Bog	18
b	2	TV	55
c	3	Avis	55



Pseudonymisering

CPR	Mail	Købshistorik	Alder
112233-1122	aaa@mail.com	Bog	18
445566-1234	b@gmail.com	TV	55
321321-6543	cccc@live.dk	Avis	55

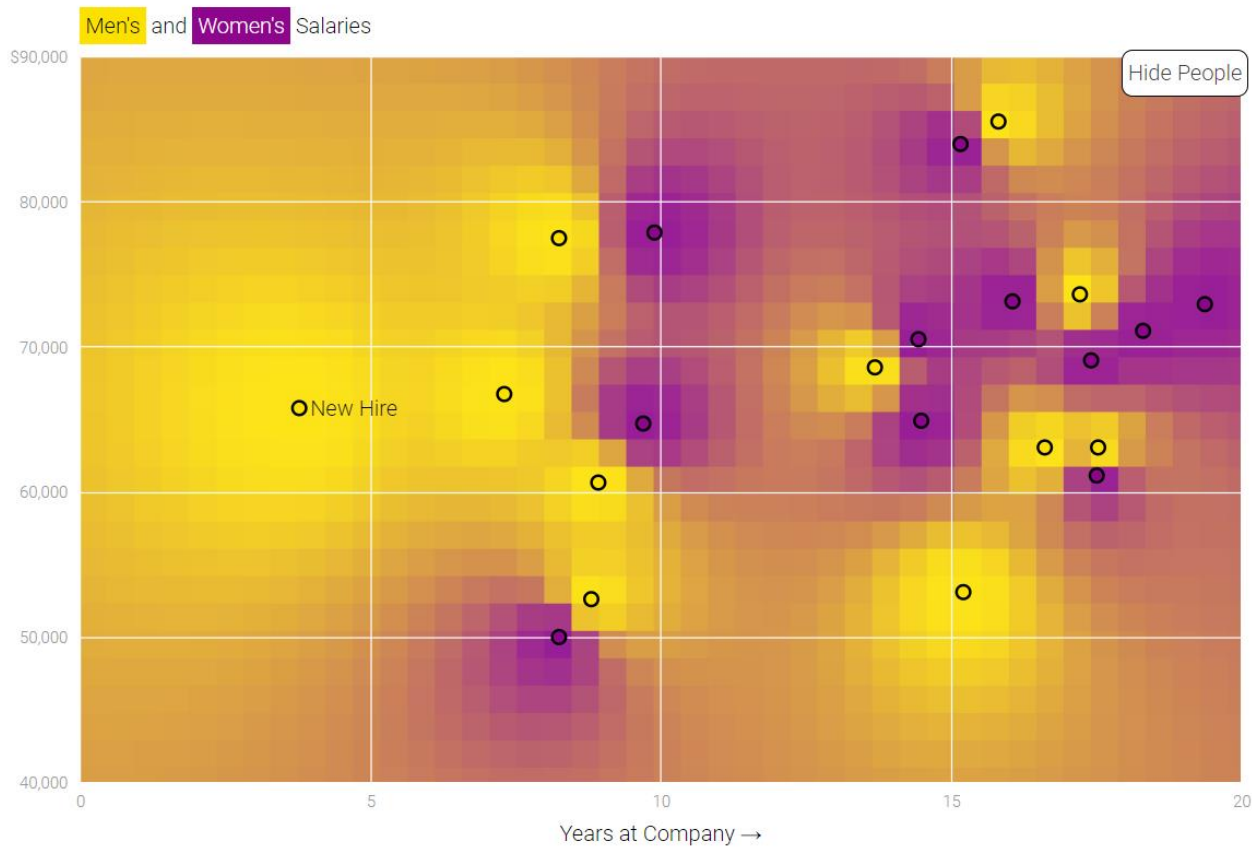
CPR	Mail	Købshistorik	Alder
a	1	Bog	18
b	2	TV	55
c	3	Avis	55

Vi ved "Alice er kunde, hun er 18 år":

Alice har købt en bog – Singling out



Membership inference attacks - why some AI models leak data if not trained correctly



Anonymisering



Anonymisering – incl. sletning

Effektiv anonymisering forhindre, at et individ bliver identificeret i et dataset, at 2 entries/datasæt sammenkædes og fra at udlede information

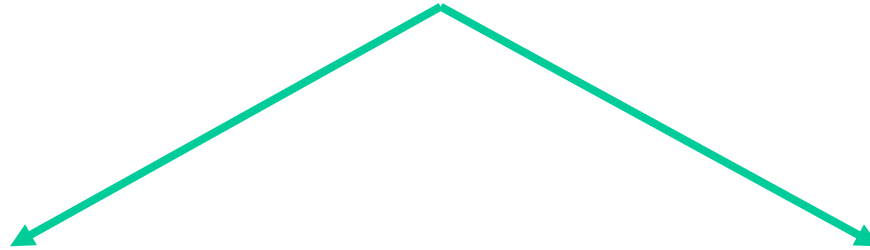
Afhængig af kontekst og formål for anonymiserede data vil der ofte være brug for forskellige teknikker for at forhinder identifikation af personen

Typisk vil det ikke være nok bare at fjerne direkte identificerbare elementer

Anonymisering er **en vidtgående teknik** for en virksomhed



Anonymisering



Data

generalisering

(Modificering af skala eller magnitude (dvs en måned i stedet for en uge, en hel region i stedet for en by).

Data

randomisering

(*Noice* – random ændring af værdier, f.eks. højde $\pm 10\text{cm}$),
Permutation – blanding af værdier så nogle er kunstigt linket til andre data subjects)

Bør altid kombineres med fjernelse af tydelige attributer/quasi-identifiers (sletning)

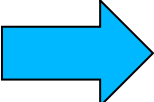
Data Generalization : K-anonymity

K-anonymity teknikker grupperer attributter med mindst K andre for at forhindre én person bliver identificeret

Attributter generaliseres så individerne deler samme værdi

Hvis k er for lille vil inference-angreb selvfølgelig være mere effektive:

K=2 eller $K > 10$

Alder		Alder
18	 K=2	<20
55		>20
55		>20

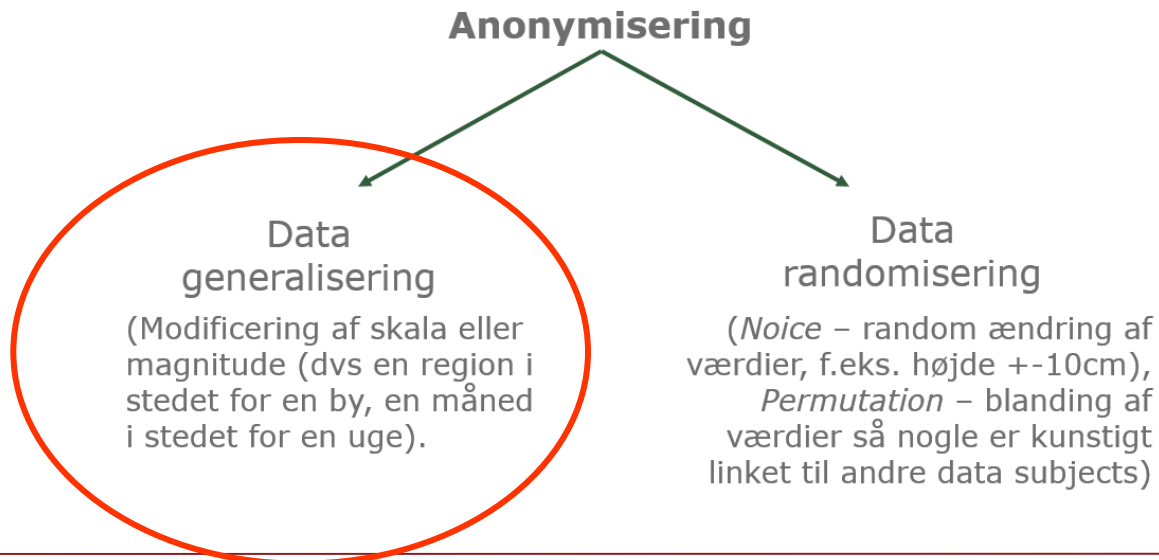


Anonymisering - Generalisering

Generalization

Generalisering kan effektivt beskytte imod Singling out - men beskytter ikke i alle tilfælde

Kræver specifikke ekstra overvejelser for at forhindre Linkability og Inference



Data Generalization

k-anonymity forhindre ikke *inference*-angreb:
Hvis angriberen ved, at et individ i datasættet blev født i 1964, ved man også at personen har haft et hjerteanfald

Year	Gender	ZIP	Diagnosis
1957	M	750*	Heart attack
1957	M	750*	Cholesterol
1957	M	750*	Cholesterol
1964	M	750*	Heart attack
1964	M	750*	Heart attack

Table 2. An example of poorly engineered k-anonymisation



Anonymisering er svært (inferens)



WIKIPEDIA
Den frie encyklopædi

Forside
Kategorier
Fremhævet indhold
Tilfældig side
Tilfældige artikler
Aktuelt

Deltagelse
Velkommen
Skribentforside
Landsbybrønden
Projekter
Portaler
Ønskede artikler
Oprydning
Kalender
Seneste ændringer
Hjælp

Værktøjer
Hvad henviser hertil
Relaterede ændringer
Læg en fil op
Specialsider
Permanent link
Oplysninger om siden

Ikke logget på [Diskussion](#) [Bidrag](#) [Opret konto](#) [Log på](#)

Artikel [Diskussion](#) [Læs](#) [Vis kilden](#) [Se historik](#)

I oktober 2019 fokuserer vi på **forældede artikler**. ([Læs her om sitenotice](#)) [\[Luk\]](#)

Margrethe 2. [Semibeskyttet](#)

Fra Wikipedia, den frie encyklopædi

"Dronning Margrethe" omdirigeres hertil. For andre dronninger med samme navn, se [Dronning Margrethe \(flertydig\)](#).

Hendes Majestæt **Dronning Margrethe II** (*Margrethe Alexandrine Þórhildur Ingrid, Danmarks dronning*) (født 16. april 1940 på Amalienborg Slot) er siden 14. januar 1972 Danmarks regent. Hun er datter af kong Frederik 9. og Dronning Ingrid. Margrethe II var gift med prins Henrik med hvem hun har sønnerne kronprins Frederik og prins Joachim.

Margrethe efterfulgte sin far ved dennes død den 14. januar 1972. Efter hendes tiltrædelse blev hun den første kvindelige monark i Danmark siden Margrethe 1. Som monark har hun den næstlængste **regeringstid** af alle danske monarker kun overgået af Christian 4.

Indholdsfortegnelse [\[skjul\]](#)

- 1 Formalia
- 2 Liv
 - 2.1 Fødsel og opvækst
 - 2.2 Tronfølger
 - 2.3 Uddannelse
 - 2.4 Ægteskab
 - 2.5 Dronning
 - 2.6 Enke
- 3 Opgaver

Ridder af Elefantordenen

1947

Margrethe 2.

Valgsprog:
Guds hjælp, folkets kærlighed, Danmarks styrke



To find Tony Blair's record, for example, you'd look for all patients who underwent cardioversion and catheter ablation at Hammersmith Hospital on October 19th 2003



Anonymisering er svært

POLITIKEN Torsdag

DANMARK > SAMFUND > POLITIK > UDDANNELSE > KØBENHAVN > UNDERVISNINGSPRISEN > MENU

Politiken Festival 1.-3. november: Mød Margrethe Vestager, Jørgen Leth og mange flere



Operationen gik fint, og Dronning Margrethe er nu udskrevet fra Rigshospitalet.

Dronningen udskrevet fra Rigshospitalet

Dronning Margrethe blev i dag udskrevet fra Rigshospitalet, hvor hun blev opereret for brok.

ALT DU BEHØVER VIDE FRA MORGENSTUNDEN
Tilmeld dig vores morgennyhedsbrev og en god start på dagen håndplukket overblik

DANMARK 18. SEP. 2006 KL. 11.49
LÆS ARTIKLEN SENERE

f t e p

Berlingske

NYHEDER OPINION BUSINESS AOK

SAMFUND

Dronningen udskrevet fra Århus Kommunehospital

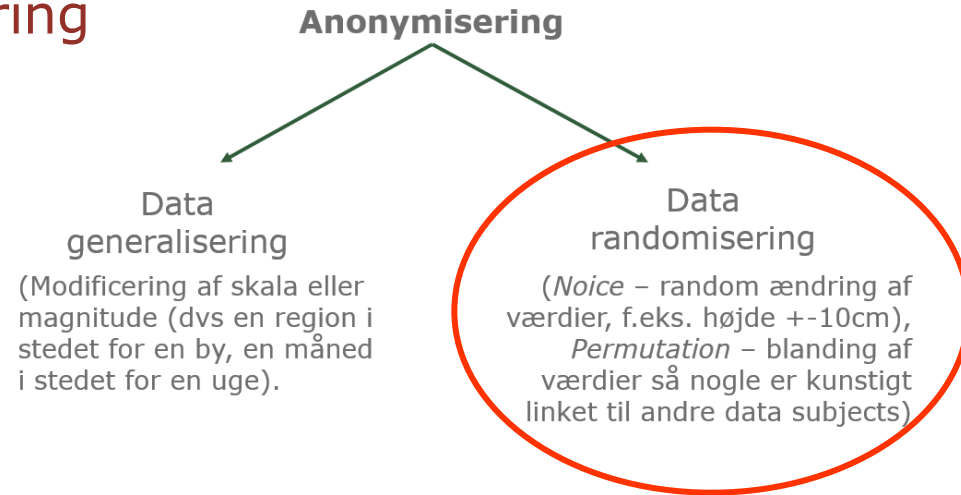
Dronning Margrethe blev i dag udskrevet fra Århus Kommunehospital. Efter den store operation i sidste uge for slidgigt i lænden blev dronningen kørt hjem til København og Amalienborg liggende i en ambulance.

Torsdag d. 23. januar 2003, kl. 19.00

Del denne artikel



Anonymisering - Randomisering



Randomization er grupperings-teknikker.
Fjerner sammenkædningen mellem data og individet

Data gøres tilstrækkeligt upræcist til det ikke kan henføres til et specifikt individ

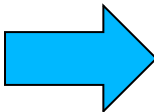
Noice/permutation



Anonymisering – Noise (Randomisering)

Noise ændrer attributter i et datasæt så de er mindre nøjagtige, men distributionen beholdes

Hvis højde oprindeligt blev målt til nærmeste centimeter kan anonymiseret datasæt f.eks. være præcist til $\pm 10\text{cm}$ (random)

Højde (cm)		Højde (cm)
154	 ± 3	158
192		189
172		175
183		186

Anonymisering – Permutering (Randomisering)

Permutering blander værdier i en table så de bliver kunstigt linket til et andet data subject
Nyttig når det er vigtigt at beholde distribution af attributer i datasættet

Kan være random værdier
(kan være svært, "ændre alle 2'er til 8'er" er ikke nok fordi mønstret kan genkendes)

Alternativt flyttes værdier fra en record til en anden → range og distribution er uændret, men korrelationen mellem værdier og individ er ødelagt



Anonymising – svag permutering

Year	Gender	Job	Income (permuted)
1957	M	Engineer	70k
1957	M	CEO	5k
1957	M	Unemployed	43k
1964	M	Engineer	100k
1964	M	Manager	45k

Table 1. An ineffective example of anonymisation by permutation of correlated attributes



Anonymisering

Both generalisering- og randomiserings teknikker har svagheder men begge kan have privacy værdi - afhængig af formål og situationen

“Identifikation” er ikke kun at identificerer en persons navn eller adresse. Husk også potential identifikation via:

**singling out,
linkability og
inference.**



Anonymisering

Fuld anonymisering er svært i praksis

Location data: nok med 4 location datapoint til entydig at identificere en person (1.5 mio personer i undersøgelsen) (hjem, arbejde, træning, ven, eller lign)

=> Svært at fjerne data nok til at anonymisere i praksis. Data skal stadig være brugbart og jo mere coarse, jo mindre brugbart i praksis

Netflix long tail problem:

http://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf



Differential privacy

Data indsamles af en central data-aggregator, som så indlægger støj $><$ Users behandler data på egne enheder inden data sendes til aggregator

Kan f.eks. bruges til at finde

- Gennemsnit
- Om bestemte attributter er til stede
- Frekvens

Interesseret i gennemsnit?

Check med 0,1%, eller er 10% tilstrækkeligt

= Sampling



Anonymisering

Anonymiseringsteknikker kan give fuld databaseskyttelse – men kun hvis det gøres rigtigt

Dvs kontekst (krav) og formål skal være helt klare for at kunne opnå rette niveau af anonymisering

Yderligere teknikker kan være nødvendige for at sikre imod data kan unikt identificerer et individ

Konsekvenser for "nytteværdien" ?



Privacy by Design - dataminimering



Eksempler på dataminimering:

- Kun indsamle efter en hændelse
- Kun indsamle med mellemrum
- Ikke gemme data hvis alt ok
- Slette data efter 2 timer - eller gemme 30 dage
- Ikke mere detaljeret information end nødvendigt, f.eks. generelt område > < detaljeret info
- Benzin ok ja/nej?

**“collected for specified,
explicit
and legitimate purposes”**

Privacy er interessant (og vigtigt)



- Din kontrol over din data
- Ikke samme nøgle til hoveddøren som til pengeskabet og til cykellåsen
- Tænk databeskyttelse med ind i arbejdet - ligesom sikkerhed

Hele jeres sikkerheds-værktøjskasse

Sikkerhedstest, sikker udvikling,
kryptering,
adgangskontrol, autentificering,
autorisering osv, osv



Privacy engineering - links

Awesome Privacy Engineering

A curated list of resources related to privacy engineering

Content

- [Courses](#)
- [Books](#)
- [Data Deletion, Data Mapping, and Data Subject Access Requests](#)
- [Privacy Tech Series](#)
- [Privacy Threat Modeling](#)
- [Machine Learning and Algorithmic Bias](#)
- [Facial Recognition](#)
- [De-Identification and Anonymization](#)
- [Homomorphic Encryption](#)
- [Tokenization](#)
- [Secure Multi-Party Computation](#)
- [Synthetic Data](#)
- [Differential Privacy and Federated Learning](#)
- [Designing for Trust with Users](#)
- [Deceptive Design Patterns](#)
- [Tagging Personally Identifiable Information](#)
- [Regulatory and Framework Resources](#)

Privacy Engineering:

<https://github.com/mpls-punk/awesome-privacy-engineering>



Spørgsmål

