

AI og GDPR - i finans og i øvrig..



Eva Jarbekk 2018

SCHJØDT

1. Grunnlagsdata for AI
2. Om AI og artikkel 22
3. Om transparens, personvernerklæringer
4. ..og husk DPIA

GRUNNLAGSDATA FOR AI



MULIGE KILDER

- Kundehistorikk, alle aspekter
- Ansatthistorikk (AI er ikke bare for kunder)
- Internett, nettaviser
- Offentlige kilder
- Facebook
- Strømforbruk

AI OG GRUNNLEGGENDE PERSONVERNKRAV

- AI er ofte en behandling av PO
- AI må ha behandlingsgrunnlag – og møte de grunnleggende prinsippene i GDPR
 - Avtale
 - Samtykke
 - Lov
 - Berettiget interesse (lite praktisk..)

AI OG *PRINSIPPET* OM RETTFERDIGHET

Er grunnlagsdata rettferdige?

Er det bias i grunnlagsdata som videreføres?

Eks fra menneskeskapte erfaringsbaserte resultater:

- Amerikansk system for tilbakefallsprosent for domfelte ga dobbelt så høy feilaktig tilbakefallsprosent for svarte som for hvite

I FINANS..

Where machine learning predicts behavioral outcomes, the necessary reliance on historical criteria will reinforce past biases, including stability bias. This is the tendency to discount the possibility of significant change—for example, through substitution effects created by innovation. The severity of this bias can be magnified by machine-learning algorithms that must assume things will more or less continue as before in order to operate. Another basic bias-generating factor is incomplete data.

<https://www.mckinsey.com/business-functions/risk/our-insights/controlling-machine-learning-algorithms-and-their-biases>

I FINANS...

In credit scoring, for example, customers with a long history of maintaining loans without delinquency are generally determined to be of low risk. But what if the mortgages these customers have been maintaining were for years supported by substantial tax benefits that are set to expire? A spike in defaults may be in the offing, unaccounted for in the statistical risk model of the lending institution. With access to the right data and guidance by subject-matter experts, predictive machine-learning models could find the hidden patterns in the data and correct for such spikes.

<https://www.mckinsey.com/business-functions/risk/our-insights/controlling-machine-learning-algorithms-and-their-biases>

AI OG *PRINSIPPET* OM FORMÅLSBEGRENSNING

PO skal ikke brukes til andre formål enn de er innsamlet for

Hvis ikke:

- Forenlige formål?
- Finnes annet behandlingsgrunnlag? Avtale, samtykke?

Eksempel: Handlinger på FB inngår i algoritme som avgjør om man får huslån – har den registrerte forstått og samtykket til det?

AI OG *PRINSIPPET* OM DATAMINIMERING

- Dataminimering, proporsjonalitet, nødvendighet
- Uklart hvordan dette skal spille inn i virkeligheten – må adresseres i DPIA/konsekvensanalyse og privacy by design for AI – er antakelig løsbart

AI OG *PRINSIPPET* OM ÅPENHET/TRANSPARENS

- DT i sin veileder:
 - Hvordan kom modellen frem til resultatet, hvordan er opplysninger vektet og vurdert
 - Hva må endres for å få annet resultat
- Hvor lett det er å oppfylle, kan avhenge av typen AI
- Algoritme – dyp læring/nevralt nett
- DT: «Fordi informasjonen skal være forståelig for den registrerte, er det *ikke alltid nødvendig å gi en omfattende forklaring av algoritmen, eller å legge frem selve algoritmen.*»

SÆRTILFELLE

AI på sensitive/særskilte kategorier av PO krever samtykke eller lov

Kan **ikke** gjøres på bakgrunn av avtale

OBS: sammenstilling av flere enkle PO kan gi sensitive PO:

Sammenstilling av likes på FB kan vise seksuell legning, etnisitet eller tro

Har betydning for hvorfra man kan hente info

ANDRE ASPEKTER KNYTTET TIL GRUNNLAGSDATA

- Opphavsrett?
 - Fritt bruke alt som er lagt ut på nettet? Neppe!
 - Ulikt syn i USA og i Europa på opphavsrett, Europa er strengere
- Forretningshemmeligheter?



ARTIKKEL 22

PROFILERING OG AUTOMATISERTE BESLUTNINGER

WP29'S VEILEDER

HOVERDREGEL OM AUTOMATISERTE AVGJØRELSE

Den registrerte skal ha rett til ikke å være gjenstand for en avgjørelse som **utelukkende** er basert på **automatisert behandling, herunder profilering**, som har rettsvirkning for eller på tilsvarende måte i betydelig grad **påvirker vedkommende**

Med mindre:

- er nødvendig for å inngå eller oppfylle en avtale mellom den registrerte
- er basert på den registrertes uttrykkelige samtykke
- det er lovhjemmel

ARTIKKEL 22

Rett til å nekte eller forbud?

Forbud.

Det gjør unntakene, både i første ledd og senere viktige.

PROFILERING/AUTOMATISERTE AVGJØRELSE

Den registrerte skal ha rett til ikke å være gjenstand for en avgjørelse som **utelukkende** er basert **på automatisert behandling, herunder profilering**, som har rettsvirkning for eller på tilsvarende måte i betydelig grad **påvirker vedkommende**

- Ingen menneskelig inngripen overhodet
- Relevant inngripen:
 - Mennesket gjør en «selvstendig vurdering av opplysningene som ligger til grunn, og har myndighet til å overprøve beslutningen»
 - Innebærer at beslutningsstøttesystemer som hjelper mennesker med å fatte beslutninger, ikke omfattes (men transparenskravet gjelder likevel)

PROFILERING/AUTOMATISERTE AVGJØRELSE

Den registrerte skal ha rett til ikke å være gjenstand for en avgjørelse som **utelukkende** er basert på **automatisert behandling**, herunder **profilering**, som har rettsvirkning for eller på tilsvarende måte i betydelig grad **påvirker vedkommende**

- Automatisk avslag om kreditt på nett
- Automatisk avslag på lån
- Strøm kuttes fordi regning ikke er betalt
- E-rekruttering
- Innreiseforbud til et land

RELEVANT PÅVIRKNING?

- Recital 71:

- Renting a city bike during a vacation abroad for two hours;
- Purchasing a kitchen appliance or a television set on credit;
- Obtaining a mortgage to buy a first home.

PROFILING - BESLEKTET MED AI

- REGULERES STORT SETT LIKT

- The GDPR defines profiling as:
 - ..the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements
- Simply assessing or classifying individuals based on characteristics such as their age, sex, and height could be considered profiling, regardless of any predictive purpose

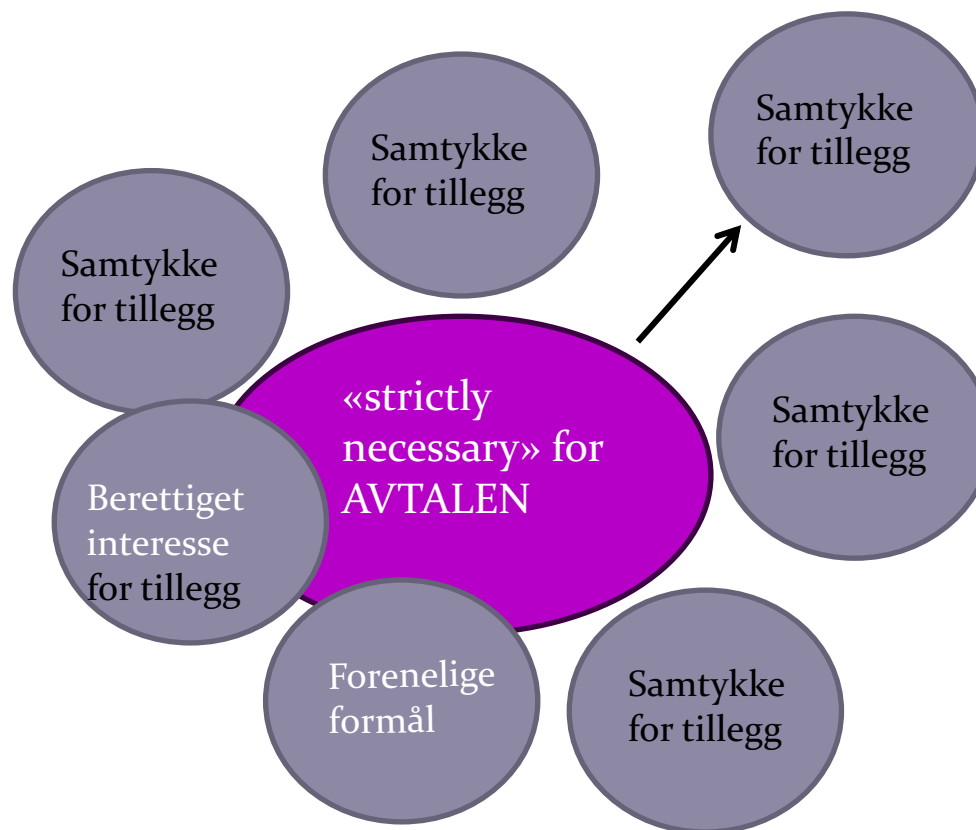
PROFILERING/AUTOMATISERTE AVGJØRELSER

Den registrerte skal ha rett til ikke å være gjenstand for en avgjørelse som **utelukkende** er basert på **automatisert behandling, herunder profilering**, som har rettsvirkning for eller på tilsvarende måte i betydelig grad **påvirker vedkommende**

Med mindre:

- **er *nødvendig* for å inngå eller oppfylle en avtale mellom den registrerte**
- **er basert på den registrertes uttrykkelige samtykke**
- **det er lovhjemmel**

HOVEDLEVERANSE OG TILLEGGSAKTIVITETER



Konsekvens? Strategisk definisjon av avtale blir viktig for å åpne for AI.

FLERE GRUNNKRAV ARTIKKEL 22 NR 2

Når samtykke eller avtale er grunnlag for AI/profilering:

“...skal den behandlingsansvarlige gjennomføre egnede tiltak for å verne den registrertes rettigheter og friheter og berettigede interesser, **i det minste retten til menneskelig inngripen fra den behandlingsansvarlige, til å uttrykke sine synspunkter og til å bestride avgjørelsen»**

Gjelder ikke når lov er hjemmelen

TRANSPARENS – INFORMASJON

If the controller is making automated decisions as described in Article 22(1), they must:

- tell the data subject that they are engaging in this type of activity;
- provide meaningful information about the logic involved; and
- explain the significance and envisaged consequences of the processing

GJENNOMSIKTIGHET - TRANSPARENS

Noen snapshots fra Artikkel 29-gruppens veileder

Hva må vi fortelle brukeren, kunde eller den ansatte?

- **Hva skjer – hvilke FORMÅL og hvilke PROSESSER som utføres for å sikre formål**
- **Hvor lenge**
- **Deles med hvem**
- **Behandles opplysningene utenfor EU/EØS**

HVA ER DET SOM ER UBEHAGELIG?

Å fortelle om formål? Greit. Også markedsføring og effektivitetsmåling

Ulike prosesser? Nja. Hvorfor?



Transparens på hvilke prosesser som kjøres for å utføre et formål:

- F eks profilering av foretatte kjøp
- F eks analyse av epost-åpning for markedsføring, når på døgnet?
- Hvordan beveger kunden seg rundt i butikken?
- Hvor går kunden fysisk videre når vedkommende forlater butikken?
- F eks «følger» oppførsel på internettsider – kobler med annen informasjon
- F eks algoritme basert på x faktorer finner ut om kunden kan få delbetaling
- Ulike målinger av ansatte

- Transparency applies not only at the point of collection of personal data but **throughout the processing life cycle**
- Controller should adhere to the same principles when communicating both the initial privacy statement/ notice and any subsequent **changes** to this statement

ENDRING SOM MÅ VARSLES OM

- **Fundamental changes**
- **The change is relevant to and impact upon the data subject**
- Enlargement of the categories of recipients
- Introduction of transfers to a third country

I god tid før endring trer i kraft

VARSLING OM ENDRING

- **notification of changes should always be communicated by way of an appropriate modality** (e.g. email/ hard copy letter etc.) specifically devoted to those changes
- **not together with direct marketing content**

FORSTÅELIGE VILKÅR OG ERKLÆRINGER



With regard to the substantive information which may be included in the **first layer** of the privacy statement/ notice, WP29's position is that this should always contain information on the **processing which has the most impact on the data subject and processing which could surprise the data subject.**

TIL SLUTT

Bruk av AI vil trigge behov for DPIA (Data Protection Impact Assessment) – utredning av personvernkonsekvenser



- Eva Jarbekk
- evja@schjodt.no
M: +47 900 51 011
- Blogg om teknologi og juss:
evajarbekk.blogg.no
- Legger ut tips på linkedin-profil