



Datatilsynets sandkasse; åpen workshop alle søkere 20. mai:

Tema: **Behandlingsgrunnlag**

Senioringeniør Eirik Gulbrandsen

Juridisk seniorrådgiver Kaja Breivik Furuseth

20. mai 2021

Den registrertes friheter, jf. EMK, og art. 24 (1).



- **Friheter:** retten til privatliv, men også retten til kommunikasjon, tanke- tros- og religionsfrihet, ytrings- og informasjonsfrihet



De registrertes rettigheter



- Informasjon (art 12-14)
 - Innsyn (art 15)
- } Forutsetning for de resterende rettigheter
- *Korrigerings* (art 16 & 19)
 - *Sletting/Retten til å bli glemt* (art 17 & 19)
 - *Rett til at personopplysninger begrensnings* (ny, art 18 & 19)
 - *Dataportabilitet* (ny, art 20)
 - *Innsigelse* (ny, art 21)
 - Automatiserte avgjørelser, inkludert profilering (art 22)





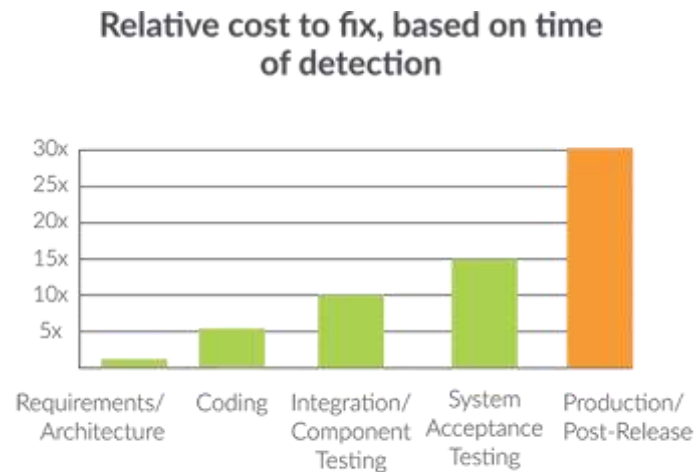
- De **registrerte** har **rettigheter**
- Behandlingsansvarlig, databehandler, underleverandører har **plikter**
- Hvilken **verdi** skaper disse pliktene for meg som tjenesteyter?



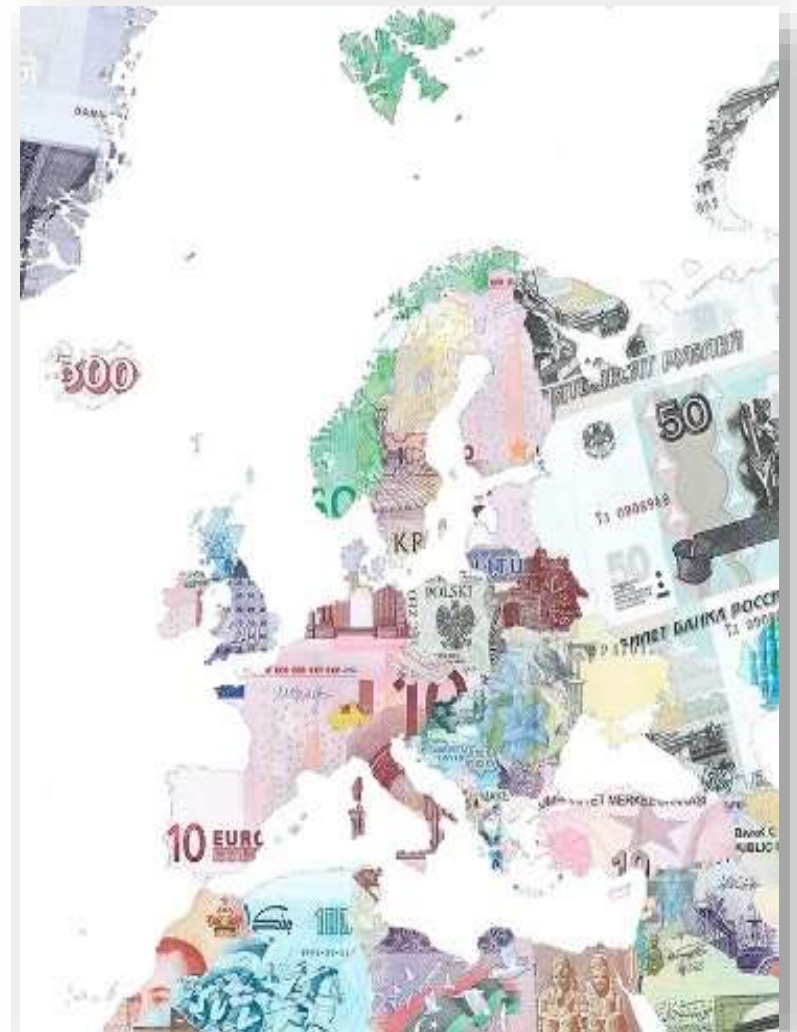
Verdien av pliktene i personvernforordningen



- **Tillit** vs. «nedkjøling»
- Effektiv samhandling vs. usikkerhet
- Direkte kostnadsbesparelser:



Source: National Institute of Standards and Technology





- **Artikkel 5. Prinsipper for behandling av personopplysninger**
 - Artikkel 6. Behandlingens lovlighet
 - Artikkel 21. Rett til å protestere
 - Artikkel 35. Vurdering av personvernkonsekvenser
 - Artikkel 22. Automatiserte individuelle avgjørelser, herunder profilering
- +
- EU-kommisjonens lovforslag: Artificial Intelligence Act



Rettslig grunnlag (behandlingsgrunnlag)

Juridisk seniorrådgiver Kaja Breivik Furuseth

20. mai 2021



- Ett eller flere formål må fastsettes før en starter å behandle personopplysninger
 - Spesifikke
 - Uttrykkelig angitte og
 - Berettigede formål
- Eksempel fra sandkassa – lagre alle søkeres kontaktinformasjon
 - Administrere søknadsprosessen for første runde
 - Arkivformål
 - Invitere til dette møtet?

Kan formålet endres?



- Formålet kan endres innen visse rammer
- Forbudt å bruke personopplysninger som er «uforenelig» med det opprinnelige formålet
 - Anonymisering regnes som et forenelig formål (tema for workshop 10. juni)
- Visse typer nye formål er likevel tillatt
 - art. 5 (1) b: Arkivformål, vitenskapelig eller historisk forskning, statistiske formål
 - Formålet bygger på lov, på nærmere vilkår
- Den registrerte kan også gi uttrykkelig samtykke til det nye formålet

a) Samtykke

- b) Nødvendig for å inngå **kontrakt** (med den registrerte)
- c) Nødvendig for å oppfylle en **rettslig forpliktelse**
- d) Nødvendig for å verne den registrertes vitale interesser
- e) Nødvendig for å utføre en oppgave i offentlighetens interesse eller utøve offentlig myndighet
- f) Nødvendig for formål knyttet til legitime interesser (**interesseavveining**)



- For at et samtykke skal være gyldig, må det være
 - informert
 - frivillig
 - spesifikt
 - utvetydig
- Samtykket må være mulig å trekke tilbake like lett som det ble gitt
- Trolig lite egnet for KI, med store mengder data



- Nødvendig for å oppfylle en avtale som den registrerte er part i
 - Eks: registrere postadresse for nettsalg
- NB Kravet til nødvendighet er strengt, ikke nok at det er praktisk
 - Personvernemnda 2020/09 Autopass
 - Var registrering av telefonnummer nødvendig for å oppfylle AutoPASS-avtale?
 - Personvernemnda: Nei, innlogging kunne skje med Bank-ID



- Både private og offentlige behandlingsansvarlige
 - Eks Datatilsynet: arkivplikt
 - Eks private og offentlige: rapportere lønn til skattemyndighetene
- NB Plikten må bygge på lov eller forskrift (ikke avtale)



Arbeid, trygd og pensjon

Lønn og tilsvarende ytelser 

Skattvik Bil

Lønn	628 000
Forsikring betalt av arbeidsgiver	10 000
Betalt telefon og bredbånd (elektronisk kommunikasjon)	4 000

[Endre](#)

Beløp vi bruker i skatteberegningen

Inntekt: Lønn mv	638 000
Inntekt: Elektronisk kommunikasjon	4 000

[Legg til lønn og tilsvarende ytelser](#)

Oppgave i allmennhetens interesse eller offentlig myndighet



- Først og fremst aktuelt for offentlige myndigheter
- Krever også supplerende rettsgrunnlag i lov eller forskrift
 - Nasjonale lovgivere har stort spillerom

Art 6 bokstav f – berettigede interesser



«behandlingen er **nødvendig** for formål knyttet til de **berettigede interessene** som forfølges av den behandlingsansvarlige eller en tredjepart, med **mindre den registrertes interesser eller grunnleggende rettigheter og friheter går foran** og krever vern av personopplysninger, særlig dersom den registrerte er et barn»



Ved protest etter art. 21:
terskelen heves til tvingende berettigede grunner



Unike forhold knyttet til behandlingsgrunnlag og KI

Senioringeniør Eirik Gulbrandsen

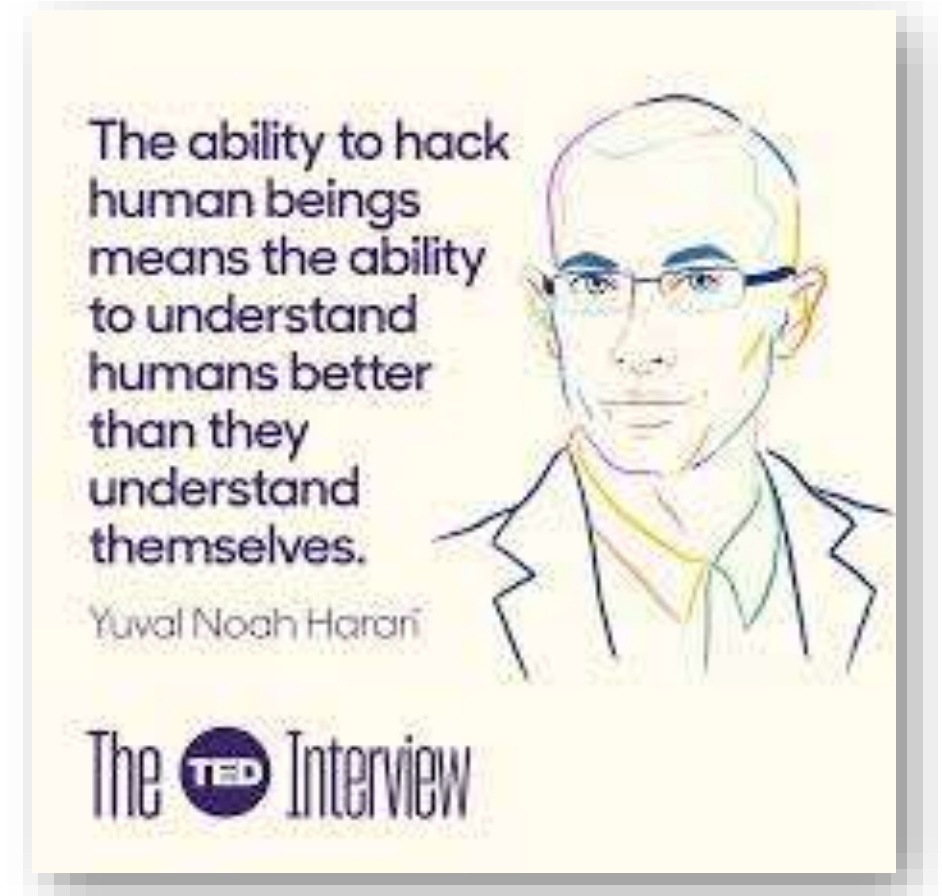
20. mai 2021

Hvorfor skaper KI spesielle utfordringer for personvernet?



“When you combine our increasing understanding of biology, especially brain science, with the enormous computing power that machine learning and AI is giving us, what you get from that combination is the ability to hack humans, which means to **predict their choices, to understand their feelings, to manipulate them** and also to replace them. If you can hack something you can also replace it.”

<https://www.aljazeera.com/indepth/features/hackable-humans-digital-dictators-qa-yuval-noah-harari-180824095306982.html>

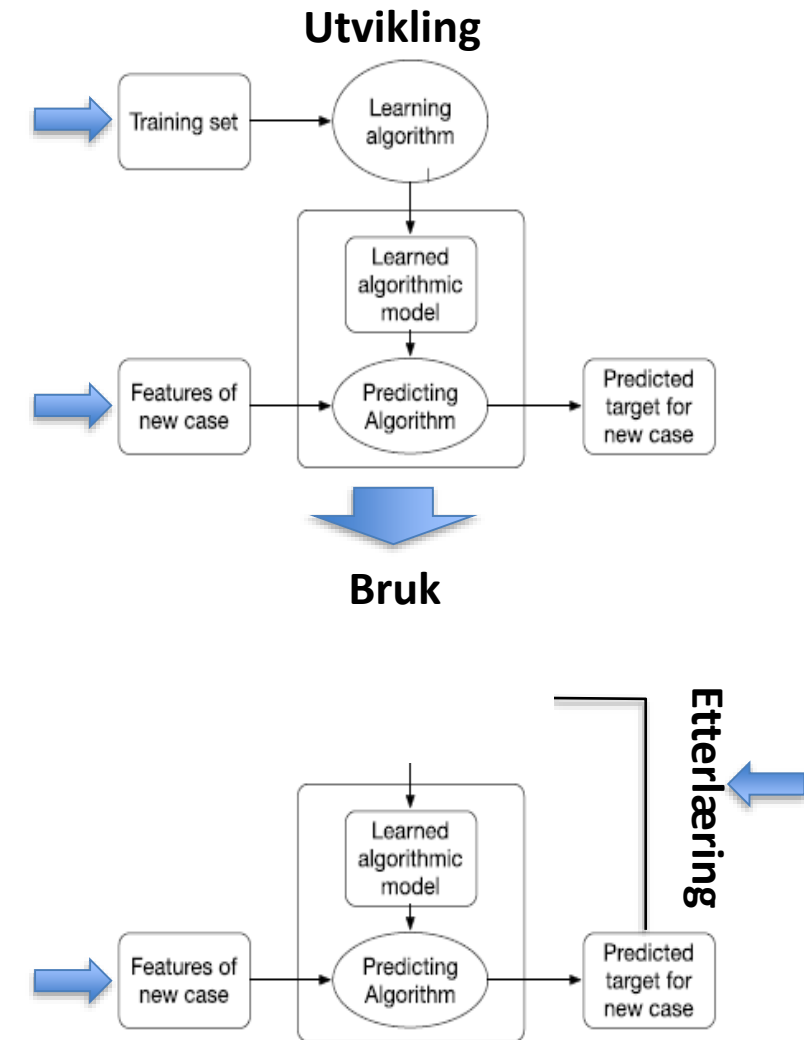


https://www.ted.com/talks/the_ted_interview_yuval_noah_harari_takes_us_into_the_past_and_reveals_the_real_dangers_ahead

Unike forhold knyttet til behandlingsgrunnlag og KI (ML)



- **Formålsbegrensning**
 - Data (modelltraining) vs programmering
 - Strukturerte vs ustrukturerte data (datakvalitet, falske data)
 - «Åpent» målbilde vs spesifikke målbilder
 - Velkjent teknologi vs «ny» teknologi (Art 35)
- **Dataminimering**
 - Store datamengder vs prinsippet om dataminimalisering
 - Fulle datasett vs pseudonyme/anonyme datasett (effektivitet og nøyaktighet)
- **Rettferdighetsprinsippet**
 - Skjevheter (oppdage)
 - Retten til en forklaring (algoritmetilsyn)
 - Premisset
- **Gjelder alle faser innen KI: utvikling, bruk, etterlæring**
 - Utvikling (selvstendig vurdering av risiko)
 - Bruk (selvstendig vurdering av risiko)
 - Etterlæring / dynamisk oppdatering av modellen (selvstendig vurdering av risiko)



Setter personvernforordningen spesifikke krav til KI?



- Artikkel 22.1 Automatiserte individuelle avgjørelser, herunder profilering
 - 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**.
 - *Artikkel 21. Rett til å protestere*
- Artikkel 35.1 Vurdering av personvernkonsekvenser
 - «Dersom det er sannsynlig at en type behandling, **særlig ved bruk av ny teknologi** og idet det tas hensyn til behandlingens art, omfang, formål og sammenhengen den utføres i, vil medføre en høy risiko for fysiske personers rettigheter og friheter, skal den behandlingsansvarlige før behandlingen **foreta en vurdering av hvilke konsekvenser den planlagte behandlingen vil ha for vernet av personopplysninger**.»
 - *Personvernkonsekvensutredning = DPIA (Data Protection Impact Assessment)*
- EU-kommisjonens lovforslag: Artificial Intelligence Act

9 momenter i vurderingen av om det er påkrevd med DPIA



1. **Evaluering eller poengsetting**, inkludert profilering og forutsigelse.
2. **Automatiske beslutninger med rettslig eller tilsvarende betydelig virkning**
3. **Systematisk overvåkning**
4. **Særlige kategorier av personopplysninger** (Art. 9 og 10) **eller opplysninger av meget personlig karakter** (relatert til privatlivets fred, utøvelse eller krenkelse av grunnleggende rettigheter Art. 9 og 10)
5. **Personopplysninger som behandles i stort omfang**
6. **Sammenstilling eller kobling av datasett**
7. **Personopplysninger om sårbare personer jf. fortale nr. 75** (skjev maktbalanse mellom behandlingsansvarlig og enkeltpersoner)
8. **Innovativ bruk av personopplysninger eller bruk av teknologiske eller organisatoriske løsninger**
9. **Når behandlingen forhindrer enkeltpersonen i å bruke en rettighet, en tjeneste eller en kontrakt**



Innhold

Denne veiledningen er laget for å hjelpe virksomheter med vurderingen av **om** av personvernkonsekvenser skal gjøres, og **hvordan** de skal gå frem.

En vurdering av personvernkonsekvenser er en prosess i forbindelse med behandlingen av personopplysninger, og vurdere om den er proporsjonal. Den skal også bidra til å håndtere de risikoene som behandlingen medfører for enkeltpersoners rettigheter og vurdere dem og fastlegge risikoreduserende tiltak.

Vurdering av personvernkonsekvenser er et viktig verktøy ettersom det ikke bare hjelper den behandlingsansvarlige med kravene i personvernforordningen, men også med å gjøre tilstrekkelige tiltak for å sikre at regelverket overholdes (artikkel 24). Med andre ord er en vurdering av personvernkonsekvenser en prosess som skal bidra til å skape og påvise etterlevelse av regelverket.

- 

 Skriv ut alt innholdet

<https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/vurdere-personvernkonsekvenser/vurdering-av-personvernkonsekvenser/>



sjekkliste-for-dpiafaser.pdf 2 / 10 80%

1. En systematisk beskrivelse av behandlingen
Dette kravet forutsetter en gjennomgang av dokumentasjonen dere allerede skal ha i internkontrollen, men der gjennomgangen sees opp mot artiklene 24, 30, 32, 40 og 42. Målet er at den behandlingsansvarlige skal ha en fullstendig oversikt over behandlingen, og sørge for at beskrivelsene som er gjort er komplette og tydelige.

Behandlingens art, omfang, formål og sammenheng
For å få en fullstendig oversikt over behandlingen, må man gå systematisk til verks og sørge for at beskrivelsene er tydelige.

Behandlingens art
Forsikre deg om at beskrivelsen omhandler behandlingens iboende karakteristiske beskrivelser av hva dere planlegger å gjøre med personopplysninger.

- Hvordan skal personopplysningene samles inn? (Samles personopplysningene registrerte eller fra andre?)
- Hvordan skal personopplysningene lagres?
- Hvordan skal personopplysningene brukes?
- Hvem skal ha tilgang til personopplysningene?
- Hvem skal det samles inn personopplysninger om? (For eksempel elever/studenter/barnehagebarn, kunder/klienter/brukere, medlemskap, osv.)
- Hvordan kan den registrerte utøve sine rettigheter?
- Vil det være en systematisk behandling av personopplysninger?
- Brukes det ny teknologi eller ny bruk av eksisterende teknologi? personvernkonsekvenser ikke har blitt vurdert?

Behandlingens omfang
Forsikre deg om at beskrivelsen inkluderer:

- kategorier av personopplysninger (om det behandles personopplysninger som for eksempel lokasjonsopplysninger, opplysninger om bevissthet, og om det behandles særskilte kategorier av personopplysninger)



Ansvar:

- Den behandlingsansvarlige er ansvarlig for og skal kunne påvise at Artikkel 5 (1) overholdes.
- Den behandlingsansvarlige skal gjennomføre egnede tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen utføres i samsvar med denne forordning. Nevnte tiltak skal gjennomgås på nytt og skal oppdateres ved behov Artikkel 24 (1).

Spørsmål og kommentarer



postkasse@datatilsynet.no
Telefon: +47 22 39 69 00

datatilsynet.no
personvernbloggen.no