

Rådet for **Digital Sikkerhed**

- Uafhængig medlemsorganisation indenfor informationsikkerhed og privatlivsbeskyttelse
- Ca 70 medlemmer
- Netværk og samarbejde
- Arbejdsgrupper
- Gå-hjem-møder

POLITIK

Gennemtænkt regulering af lovgivning
Høringssvar, holdningspapirer, dialog med ordførere, politiske ekspertråd og oplæg på konferencer

Vision:

...at fremme et trygt og frit digitalt samfund for alle

BORGERNE

Oplyst brug af teknologi og anvendelse af deres data
Tips til danskernes og debat i pressen

ERHVERVSLIVET

Efterlevelse af EU's persondataforordning og fornuftig regulering
Information og vejledning om sikkerhed og dataetik, gå-hjem møder og seminarer

Dataetik og industri 4.0

- en praktisk tilgang

Dataetik på den politiske dagsorden

Frontløberne: Dataethics

- ”en tænkehandletank, der arbejder for at fremme dataetiske produkter og tjenester.”
- ”flytte den digitale forretningsmodel fra tracking-by-default til privacy-by-default”
- Dataetiske principper: <https://dataethics.eu/da/dataetiske-principper/>
- <https://dataethics.eu/da/>

Dansk IT

<https://www.dit.dk/da/Nyheder/2018/Dataetik>

DTU Compute

<https://www.altinget.dk/digital/artikel/dtu-professor-vi-boer-have-faerdselsregler-for-kunstig-intelligens>.

IDA

Siri kommissionens anbefalinger: <https://ida.dk/media/1583/ai-etik-sirikommissionen-rapport.pdf>.

Løkke-regeringen

Ekspertgruppen om dataetik: <http://dataetikdk.dk/>.

Dataetisk Råd: <http://www.justitsministeriet.dk/ministeriet/raad/dataetisk-raad>.

Nærværende kilder:

RfDS 10 dataetiske principper:

<https://static1.squarespace.com/static/5592479ee4b0224fac5497af/t/5d00e6560187cc00011c703b/1560340055738/RfDS%2BD-E-principper.pdf>.

Ethics – Kan dataetik siges at følge af de persondataretlige regler?

Af Henning Mortensen og Charlotte Bagger Tranberg, Revision og Regnskabsvæsen, nr. 9, 2019:

<https://www.karnovgroup.dk/artikler/rr-09-2019-kan-dataetik-siges-at-folge-de-persondataretlige-regler>

Hvad er dataetik?

Definition af dataetik?

- Ingen kanoniseret definition
- Oxford Dictionary: "A set of moral principles, especially ones relating to or affirming a specified group, field, or form of conduct"
- Cambridge Dictionary: "a system of accepted beliefs that control behaviour, especially such a system based on morals"
- Merriam-Webster: "the discipline dealing with what is good and bad and with moral duty and obligation"
- Summa sumarum: Begrænse aktiviteter til gøre det gode og rigtige og udvise den gode og rigtige opførsel ud fra moralske overvejelser
- Vi skal altså gøre os nogle overvejelser om, hvad der er det gode og rigtige at gøre; hvor vi inddrager alle aspekter – både de umiddelbart indlysende positive aspekter og de aspekter der er negative for nogle

Risiko for misbrug af positivt ladet ord

- Forudsige sygdommes spredning mhp. beredskab
- Udryd al kriminalitet gennem dataindsamling, -sammenstilling og -mining
- Dataetikken kan hurtigt bruges til at forfalde til utilitarisme
- Når nogen taler om dataetik er der derfor grund til at være på vagt

Dataetisk ophæng 1

Dataetik er ikke noget nyt

- Der findes **allerede et juridisk ophæng** i form af GDPR, artikel 5, stk. 1, litra a: ”personoplysninger skal behandles, lovligt, rimeligt og gennemsigtigt”
- Lovgiver har således lagt op til, at den dataansvarlige skal vurdere, om behandling af personoplysninger er rimelig
- ”Rimelig” er imidlertid elastik i metermål – tænk forbruger vs. markedsføringsafdeling eller borger vs. politik
- Derfor er der rum til at lave **dataetiske principper, som guidelines, hos den dataansvarlige**
- Derfor er der rum til at lave **Code of Conducts for brancher** i GDPR
- Derfor har **Datatilsynet i en række afgørelser** lagt en praksis for rimelighedsbetragtninger
- De to sidste er bindende for den dataansvarlige, så den dataansvarlige ikke kan hævde, at hvad som helst er dataetisk
- Praksis udvikler sig langsomt, hvorfor dataetikken har en værdi i form af at skabe et vidensgrundlag som dem der danner praksis kan lade sig inspirere af, og som kan bruges indtil praksis kommer på plads.
- Dataetikken har dog den svaghed, at hvor praksis besluttet gennem vores institutioner må anses for at være demokratisk er dataetikken selvbestaltet.
- Datatilsynets praksis: Udbetaling Danmark, må ikke samkører data om alle personer i en husstand, når de skal afgøre om en given person, skal have udbetalt en pension (dataminimering og rimelighed): ”Datatilsynet fandt, at kravet om proportionalitet ikke var opfyldt, da den mulige behandling af personoplysninger om en stor kreds af personer, som ikke var kunder i pensionsinstitutterne, ikke stod i rimeligt forhold til lovforslagets formål.”

Dataetisk ophæng 2

Dataetik er ikke noget nyt

- Etiske overvejelser finder også anvendelse i forhold til forvaltningsloven, hvor der skal foretages vurderinger af ”**god forvaltningsskik**”.
- Folketingets Ombudsmand: ”God forvaltningsskik er normer og principper for, hvordan myndigheder bør opføre sig i forhold til borgerne.”
- Noget af denne ”God forvaltningsskik” er allerede indskrevet i lovgivningen – f.eks. Forvaltningsloven og offentlighedsloven.
- Der findes ikke en entydig kilde til ”God forvaltningsskik”. **Noget er skrevet direkte ind i loven, noget foreligger nedskrevet i vejledninger mens noget er forblevet uskrevet.**
- Eksempel: **Journaliseringspligten** er nedskrevet i offentlighedslovens § 15, stk. 1: ”Dokumenter, der er modtaget eller afsendt af en forvaltningsmyndighed som led i administrativ sagsbehandling i forbindelse med dens virksomhed, skal journaliseres, i det omfang dokumentet har betydning for en sag eller sagsbehandlingen i øvrigt.”
- Baggrunden er dels at beskytte borgeren ved at afgørelser kan dokumenteres og dels at beskytte embedsværket ved at sikre at alle akter til grund for en afgørelse er tilgængelige, således at embedsværket kan dokumentere, at der ikke har været usaglige momenter i afgørelsen.
- Denne bestemmelse kan være i modstrid med GDPR artikel 17, stk. 1: ”Den registrerede har ret til at få personoplysninger om sig selv **slettet** af den dataansvarlige uden unødigt forsinkelse”.
- Baggrunden er at den registrerede altid skal have retten til at bestemme over sine data og ”blive glemt”.
- **Politikerne har her vurderet at bestemmelsen i offentlighedsloven er vigtigere for de registrerede end bestemmelsen i GDPR**, og derfor er meget vanskeligt (grænsende til umuligt) at få slettet oplysninger som stat, region og kommuner har registreret.
- Etiske overvejelser kendes altså også fra ”god forvaltningsskik”
- Hanne Marie Motzfeldt: ”Digital Forvaltning - udvikling af sagsbehandlende løsninger”

Hvad er industri 4.0?

Jeg har ikke fundet en entydig og god definition...

- Cyber-fysisk systemer
- IoT / IIot
- Big Data analyse
- Kunstig intelligens
- Avancerede robotter
- 3D-print
- Selvkørende biler
- Droner
- Smart cities
- Genteknologi
- Bioteknologi
- Sensorer
- Materialevidenskab
- Realtime
- Trådløse netværk
- Virtuel kopi af fysisk verden og decentrale beslutninger
- Customisering og selv-servicering

Smart manufacturing and servicing in cyber/physical systems made by interconnected machines/robots using AI/ML to make decisions themselves based on real time big data from cloud connected IoT/sensors and interconnected supplychains

Brug af dataetik på AI

EU Kommissionens ekspertgruppe

- <https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai>
- ”ramme for opnåelse af pålidelig kunstig intelligens baseret på grundlæggende rettigheder som fastlagt i EU's charter om grundlæggende rettigheder (EU-chartret) og i relevant international menneskerettighedslovgivning”, p. 6.
- **A. Lovlig kunstig intelligens**
 - EU's traktater og charter
 - EU afledt ret (f.eks. GDPR, ikkediskrimination, maskindirektiv, produktansvarsdirektiv,...)
 - FN og Europarådets konventioner
 - Nationale love
 - Områdespecifikke regler
- **B. Grundlæggende rettigheder anvendt på AI (konkretisering af ovenstående)**
 - **Respekt for menneskets værdighed:** iboende værd => mennesket behandles med respekt og ikke kun som data
 - **Den enkeltes frihed:** mennesket træffer egne beslutninger og skal kunne udleve rettigheder og forblive inkluderet
 - **Respekt for demokrati, domstolene og retsstatsprincippet:** understøtte demokrati og pluralitet af enkeltpersoners værdier og valg
 - **Ligestilling, ikkediskrimination og solidaritet:** undgå udstødelse og forudindtagne resultater
 - **Borgerrettigheder:** stemme, god forvaltning, aktindsigt, indbringe andragende for myndigheder

Brug af dataetik på AI

- **C. Ethiske principper for AI – etiske imperativer**
 - **respekt for menneskers autonomi:** frihed og selvbestemmelse, understøtte kognitive, sociale og kulturelle færdigheder
 - **forebyggelse af skade:** beskytte værdighed samt mental og fysisk integritet; forbehold for magtassymmetri
 - **retfærdighed:** undgå diskrimination og stigmatisering; lige muligheder; proportionalitet mellem mål og midler
 - **forklarlighed:** gennemsigtige procedurer og forklarlighed til alle
- **D. Syv krav til AI afledt af etiske principper**
 - **Menneskelig udførelse og kontrol**
 - Herunder grundlæggende rettigheder, menneskelig udførelse og kontrol
 - **Teknisk robusthed og sikkerhed**
 - Herunder modstandsdygtighed over for angreb og sikkerhed, fallback-plan og generel sikkerhed, nøjagtighed, pålidelighed og reproducerbarhed
 - **Overholdelse af privatlivets fred og datastyring**
 - Herunder respekt for privatlivets fred, datakvalitet og -integritet og dataadgang
 - **Gennemsigtighed**
 - Herunder sporbarhed, forklarlighed og kommunikation
 - **Diversitet, ikkediskrimination og retfærdighed**
 - Herunder undgåelse af urimelig skævhed, tilgængelighed og universelt design samt inddragelse af interessenter
 - **Miljø- og samfundsmæssig velfærd**
 - Herunder bæredygtighed og miljøvenlighed, social indvirkning, samfund og demokrati
 - **Ansvarlighed**
 - Herunder mulighed for revision, minimering og rapportering af negative virkninger, afvejninger og klageadgang.

Brug af dataetik på AI

- **E. Konkrete spørgsmål til evaluering af de syv krav (pp. 28-34)**
 - **Ex. Teknisk robusthed og sikkerhed**
 - **Modstandsdygtighed**
 - Har du vurderet de potentielle former for angreb?
 - Har du indført foranstaltninger, der kan sikre AI-systemets integritet?
 - Har du vurderet, hvordan dit system opfører sig i uventede situationer og miljøer?
 - Har du overvejet om dit system kan have dobbelt anvendelse og truffet passende foranstaltninger mod dette?
 - **Fall-back-plan og generel sikkerhed**
 - Har du sørget for, at systemet har en tilstrækkelig fallback-plan ved angreb og andre uventede situationer?
 - Har du overvejet risikoniveau...?
 - Har du overvejet sandsynlighed for at systemet kan skade brugere...?
 - Har du estimeret sandsynlige virkninger af fejl i AI-systemet – herunder samfundsmæssigt uacceptable resultater...?
 - **Nøjagtighed**
 - Har du vurderet, hvilket niveau og hvilken definition af nøjagtighed der kræves?
 - Har du vurderet den skade, der kan forårsages, hvis AI-systemet foretager unøjagtige forudsigelser?
 - Har du indført muligheder for at måle, om systemet foretager et uacceptabelt antal unøjagtige forudsigelser?
 - Hvis der foretages unøjagtige forudsigelser, har du da indført en serie af trin for at løse problemet?
 - **Pålidelighed og reproducerbarhed**
 - Har du indført en strategi med det formål at overvåge og teste, om AI-systemet opfylder de fastsatte mål, formål og tiltænkte anvendelser?

Rådets dataetiske principper

Rådet for Digital Sikkerheds dataetiske principper

- Ligger tæt op af GDPR,
<https://static1.squarespace.com/static/5592479ee4b0224fac5497af/t/5d00e6560187cco0011c703b/1560340055738/RfDS%2BDE-principper.pdf>
- 1. NØDVENDIGHED
Er det umuligt at opfylde formålet med løsningen helt uden at indsamle personoplysninger eller med fuld anonymisering af data? (hvis nej, så vælg at re-designe løsningen)
- 2. LOVLIGHED
Er der fuld klarhed over hjemmelsgrundlaget? (er metoden lovlig pga. samtykke, legitime interesser, kontrakt eller særlov)
- 3. ETISK DESIGN
Sikres individets rettigheder og principperne i GDPR gennem it-løsningens design? (forudbestemt formål, kun indsamling af nødvendige data, indsigt, oplysningspligt, kontrol over egne data, sletning m.v.)
- 4. KONSEKVENSER
Er der på forhånd taget stilling til, hvilke konsekvenser forslaget/løsningen kan have for de registrerede på kort og på lang sigt?
- 5. VALGFRIHED
Er det valgfrit for den enkelte, hvorvidt data om vedkommende registreres eller ej?

Rådets dataetiske principper

- **6. SIKKERHED**
Er der etableret en passende sikkerhed i og omkring systemet i tråd med de nødvendige og bedst tilgængelige tekniske og organisatoriske metoder?
- **7. TRANSPARENS**
Er der gennemsigtighed i behandlingen, herunder ved brug af algoritmer og er der menneskelig kontrol med resultaternes rimelighed?
- **8. RESPEKT FOR MENNESKERETTIGHEDER**
Er der sikkerhed for, at databehandlingen ikke er bias med risiko for diskriminering, marginalisering eller stigmatisering af individer?
- **9. PROPORTIONALITET**
Er der foretaget en proportionalitetsafvejning og dermed sikret, at individets rettigheder ikke undermineres ud fra en ”målet helliger midlet” tankegang?
- **10. ANSVARLIGHED**
Er der klarhed om ansvarsplacering, løbende tilsyn og klageadgang?

Dataetiske principper i praksis

Dataetisk princip	Compliant	Evaluering	Dataetisk alternativ (i tilfælde af nej=rød kan man formulere et dataetisk alternativ mhp . At komme i ja=grøn)
<p>1. Nødvendighed</p> <p>Er løsningen designet på en måde, der gør at den kun indsamler relevante data eller anvender fuld anonymisering af data?</p>	Nej	Løsningen indsamler nummerpladeoplysninger om alle nummerplader der kører ind i miljøzonen. Der synes således ikke at være overvejet om der kan ske en begrænsning i indsamlingen af oplysninger, til hvad der må anses for at være strengt nødvendigt	Der kan designes en løsning, hvor de nummerplader, der skannes, kan sammenlignes med en liste over ikke forurenende køretøjers nummerplader i en central database. Dette kan ske uden at det registreres, hvilken nummerplader, der faktisk foretages opslag på i databasen. De nummerplader, som ikke fremgår af databasen, er dermed udenlandske nummerplader og nummerplader, der ikke er godkendte til miljøzonerne.
<p>2. Lovlighed</p> <p>Er der fuld klarhed over hjemmelsgrundlaget?</p>	Måske	Der kan formodentlig vedtages lovgivning, som lovgiggør dette tiltag, og det må også formodes at være hensigten. Det er vanskeligt at forestille sig at tiltaget er compliant med de persondataretlige regler uden særlovgivning og pt. er der ikke et hjemmelsgrundlag.	Lovforslaget kunne udformes på en måde, at der opstilles begrænsninger på hvilke oplysninger, der indsamles.
<p>3. Etisk design</p> <p>Sikres individets rettigheder og principperne i GDPR gennem it-løsningens design?</p>	Nej	Dataminimeringsprincippet er ikke opfyldt i den oprindelige løsning, da der indsamles langt flere oplysninger end nødvendigt for formålet: alle de køretøjer, som lovligt befinder sig i miljøzonen.	Der kan imidlertid vælges et design, som skitseret ovenfor, der er kompatibelt med de persondataretlige regler.

Dataetiske principper i praksis

<p>4. Konsekvenser</p> <p>Er der på forhånd taget stilling til, hvilke konsekvenser forslaget/løsningen kan have for de registrerede på kort og på lang sigt?</p>	<p>Måske</p>	<p>Konsekvenserne for de registrerede er, at man kan fastslå om et køretøj befinder sig i miljøzonen eller ej. Der er dermed med det oprindelige forslag tale om en unødvendig <u>tracking</u> af borgerne.</p>	<p>Konsekvenserne kan begrænses betydeligt ved at indsamle oplysninger om færre personers nummerplader.</p>
<p>5. Valgfrihed</p> <p>Er det valgfrit for den enkelte, hvorvidt data om vedkommende registreres eller ej?</p>	<p>Nej</p>	<p>De registrerede har ikke indflydelse på om de registreres eller ej.</p>	
<p>6. Sikkerhed</p> <p>Er der etableret en passende sikkerhed i og omkring systemet i tråd med de nødvendige og bedst tilgængelige tekniske og organisatoriske metoder?</p>	<p>Nej</p>	<p>Der foreligger ikke <u>RfDS</u> bekendt oplysninger om sikkerhedstiltagene i løsningen.</p>	<p>Foruden de skitserede designmæssige tiltag skal der være sikkerhedsmæssige tiltag i overensstemmelse med ISO27XXX, således at der f.eks. er adgangsbegrænsning, beskyttelse af systemet mod ondsindede angreb og sletning efter en passende periode.</p>
<p>7. Transparens</p> <p>Er der gennemsigtighed i behandlingen, herunder ved brug af algoritmer og er der menneskelig kontrol med resultaternes rimelighed?</p>	<p>Ja</p>	<p>Det forudsættes at der opstilles skiltning, som signalerer, at optagelse af nummerplade finder sted.</p>	

Dataetiske principper i praksis

<p>8. Respekt for menneskerettigheder</p> <p>Er der sikkerhed for, at databehandlingen ikke er bias med risiko for diskriminering, marginalisering eller stigmatisering af individer?</p>	<p>Måske</p>	<p>Der synes ikke at være nogle menneskeretlige konsekvenser af forslaget, så længe overvågningen anvendes alene til det skitserede formål.</p>	
<p>9. Proportionalitet</p> <p>Er der foretaget en proportionalitetsafvejning og dermed sikret, at individets rettigheder ikke undermineres ud fra en "målet helliger midlet" tankegang?</p>	<p>Nej</p>	<p>RfDS er ikke bekendt med om der foreligger en proportionalitetsvurdering. Henset til at man imidlertid kunne sikre proportionalitet ved at vælge et andet design må RfDS lægge til grund at en proportionalitetsvurdering ikke er foretaget.</p>	<p>Det er muligt at opnå proportionalitet gennem det skitserede design.</p>
<p>10. Ansvarlighed</p> <p>Er der klarhed om ansvarsplacering, løbende tilsyn og klageadgang?</p>	<p>Nej</p>	<p>Der foreligger ikke RfDS bekendt oplysninger om, hvor ansvaret for anvendelsen af løsningen, tilsyn med løsningen eller klageadgang skal placeres.</p>	<p>Der skal i den endelige udgave tages stilling til ansvarsplacering, tilsyn og klageadgang.</p>

Vi har brug for at sikre industri 4.0

Hvis vi ser på teknologierne, som nævne i relation til industri 4.0...

- Cyber-fysisk systemer
- IoT / IIot – **hack af kameraer, babyalarmer, ...**
- Big Data analyse
- Kunstig intelligens – **profilering af familier med belastede børn, langtidsledige...**
- Avancerede robotter – **hack af kraner, gravemaskiner,...**
- 3D-print
- Selvkørende biler – **hack af Jeep Cherokee,...** <https://www.youtube.com/watch?v=MKoSrxBC1xs>
- Droner – **alternativ anvendelse, ISIS anvendelse,...**
- Smart cities
- Genteknologi
- Bioteknologi
- Sensorer
- Materialevidenskab
- Realtid
- Trådløse netværk – **sker hele tiden**
- Virtuel kopi af fysisk verden og decentrale beslutninger
- Customisering og selv-servicering

En note om ISO27701

ISO27701

- Ny standard som mapper (supplerer og udvider) kontroller til behandling af personoplysninger ind i kravene til informationssikkerhed fra ISO27001/2.
- Mange gode krav og en god systematisk for at skabe sammenhæng mellem sikkerhed (CISO) og persondatabeskyttelse (DPO)
- Stiller krav om at designe (GDPR, artikel 25) de grundlæggende principper (GDPR, artikel 5) for behandling af personoplysninger ind i den dataansvarliges (og databehandlerens) IT-systemer
- Hermed bliver rimelighedsprincippet / dataetikken et (teknisk) designkrav
- Det hænger fint sammen med Cavoukians privacy by design – principper
- Læs mere om ISO27701: <https://wiredrelations.com/gdpr-iso27701-sammenhaeng-mellem-sikkerhed-og-persondatabeskyttelse/>.
- Det kan godt være, at vi ikke kommer hele vejen rundt om dataetikken, men vi får et **rammeverk**, hvor vi kan komme de **centrale dataetiske vurderinger** ind i
 - en procedure i...
 - et designframework ifølge...
 - en standard

En note om tid

Balance

- Vi skal være **på beatet** for at tiden ikke løber fra vores forretninger og fra vores samfundsmodel
- **Teknologierne kan på rigtig mange måder forbedre vores velstand og levevis!!!**
- Vi skal omvendt forsvare **værdierne** i vores samfund gennem love, sikkerhed og etik – og turde stå fast på dem
- Overvågningen er stigende
 - Fra **statens** side har vi gennem tiden fået den ene overvågningspakke efter den anden og som regel med terror eller kriminalitet (og enkelte gange effektivitet) som formål/begrundelse
 - Fra **virksomhedernes** side profileres vi som aldrig før online og det bliver udbygget i takt med at alle vores produkter kommer online – tilsyneladende uden politisk vilje til indgreb (e-Privacy)
 - Der har aldrig været nogen mennesker, der er så overvågede, som vi er i dag
- Området er **komplekst** (jura, teknologi, etik) – og svært at facilitere en folkelig debat om
- Vi risikerer **faldende tillid** til digitaliseringen fordi det er uforståeligt
- Vi har **brug for tid til debat**, og vi kan jo begynde her i dag!!!

Afslutning

hmo@ao.dk

<https://www.linkedin.com/in/henning-mortensen-343b0/>

(Connect gerne)