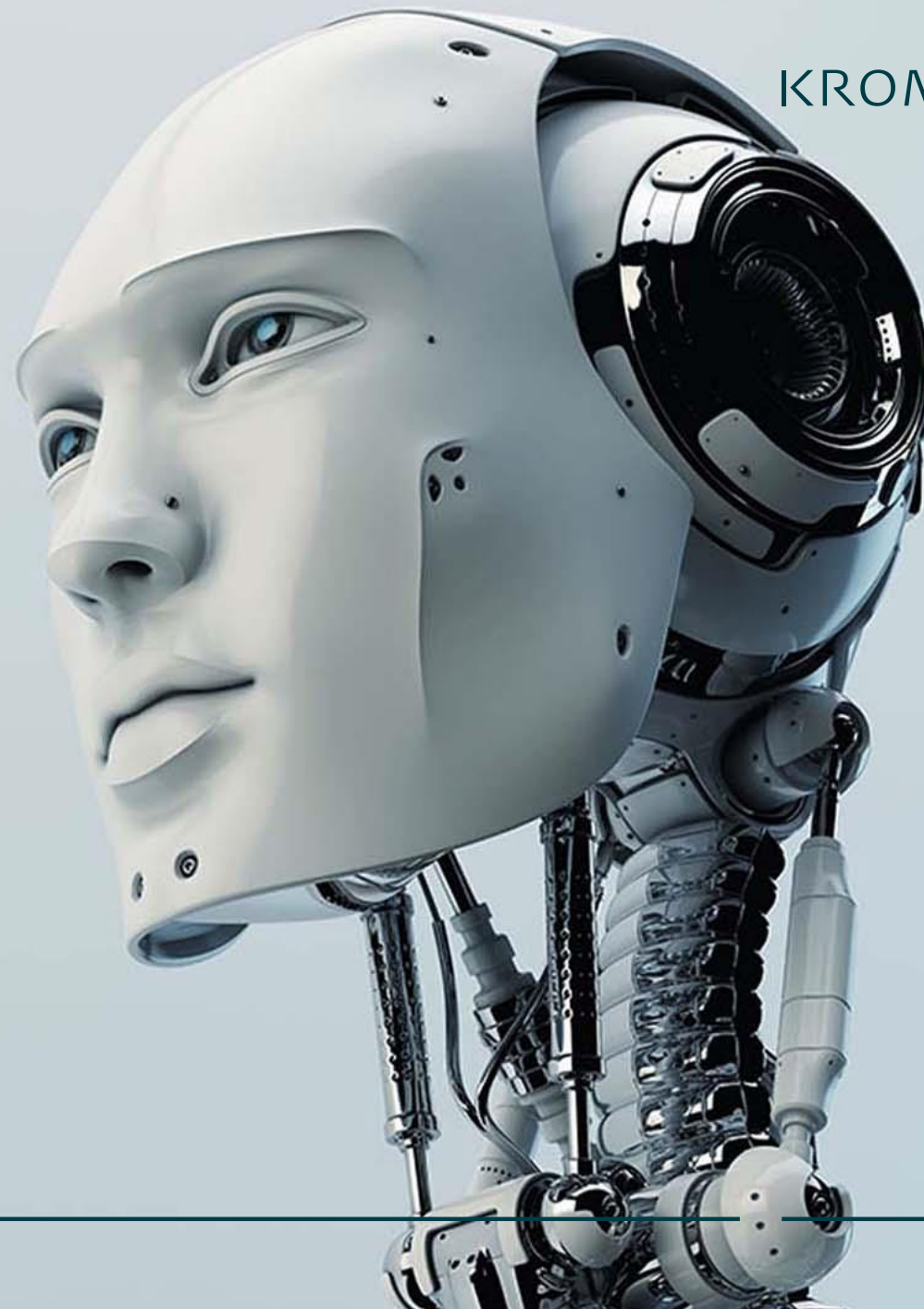


Kan vi ikke bare lade ChatGPT skrive proceduren?

Retlige perspektiver på generativ AI
Kristian Storgaard, partner, certificeret IT-advokat
kst@kromannreumert.com

Procedureadvokaternes temadag
9. november 2023



Når spørgsmålet om AI rammer en advokat...

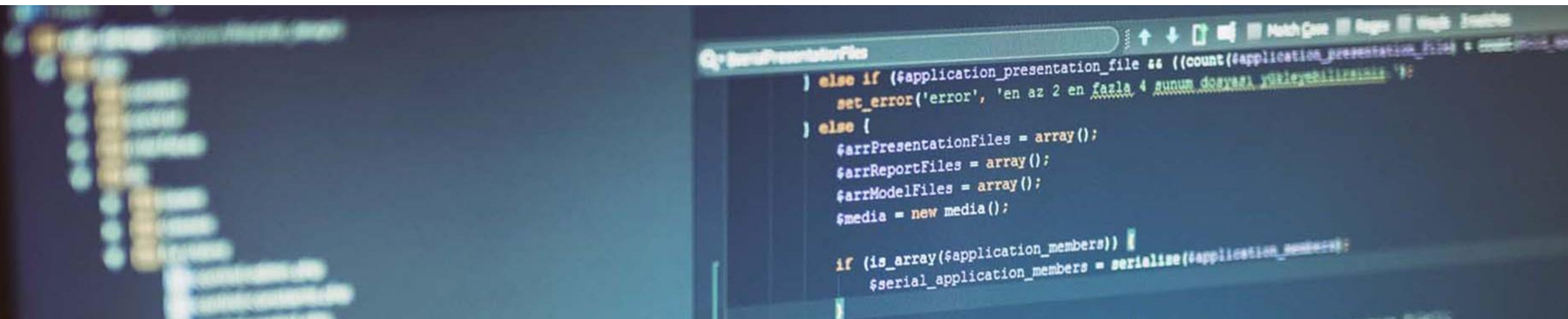
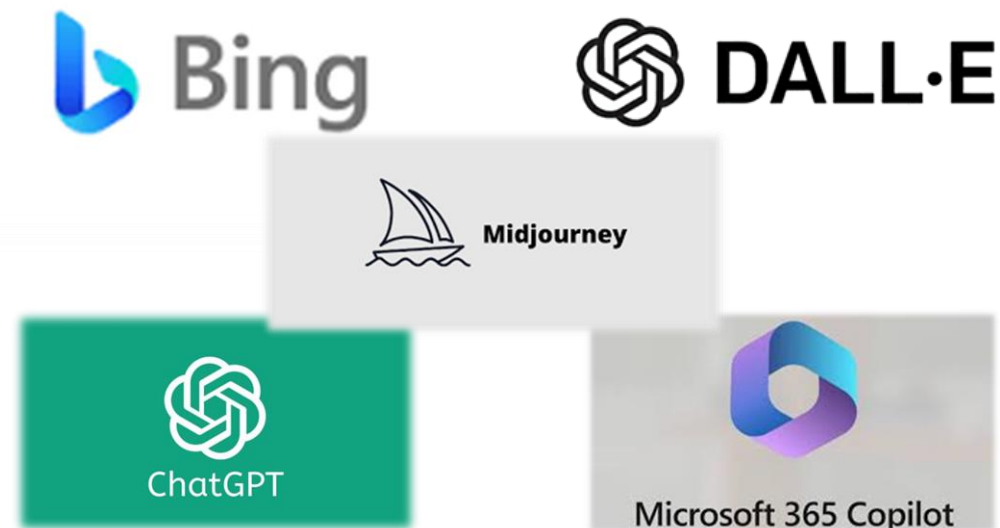


Virksomheder skal **se kunstig intelligens som en værdifuld mulighed og omfavne den**, men ikke være ukritiske eller glemme juraen i processen.



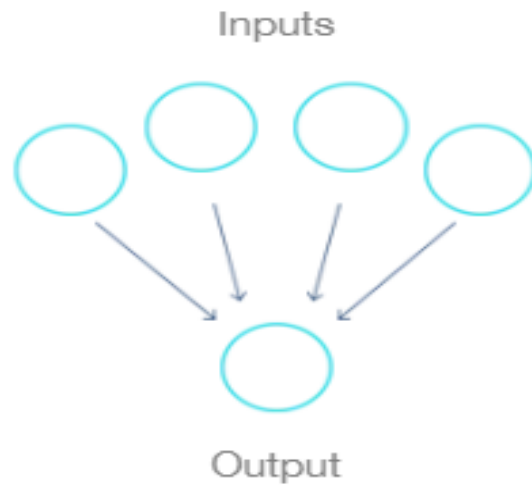
Hvad er generativ AI?

- **Bestemt type kunstig intelligens(-teknologi)**, som kan skabe originalt indhold, som:
 - Tekst, billeder, musik, stemmer, videoer m.v.
 - Syntetisk data, som kan bruges til at træne andre modeller.
- Indholdet er ikke fastlagt på forhånd, men **genereres dynamisk baseret på input og den indlærte model**.
- **Fleksibel og tilpasningsdygtig**, og kan derfor generere unikke og relevante resultater for forskellige brugsscenarier og brugerbehov.
- **Kapacitet til at lære, forbedre og udvikle sig over tid** gennem feedback og forfinelse af modeller.

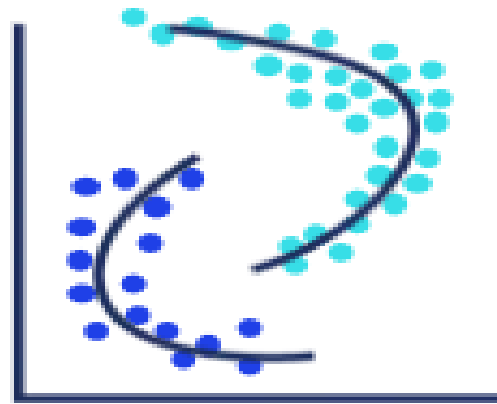


Machine learning

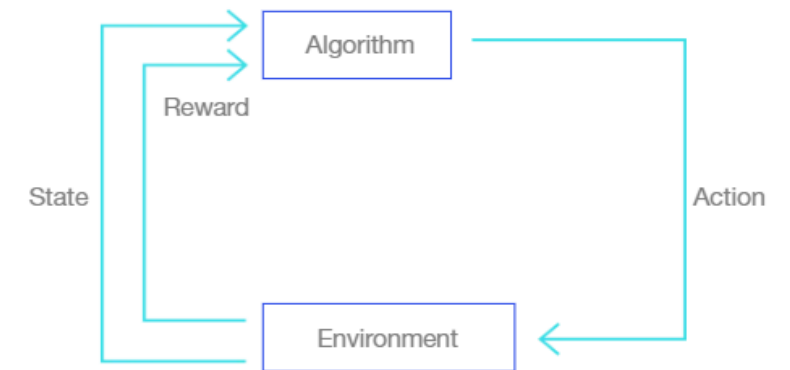
Supervised learning



Unsupervised learning



Reinforcement learning

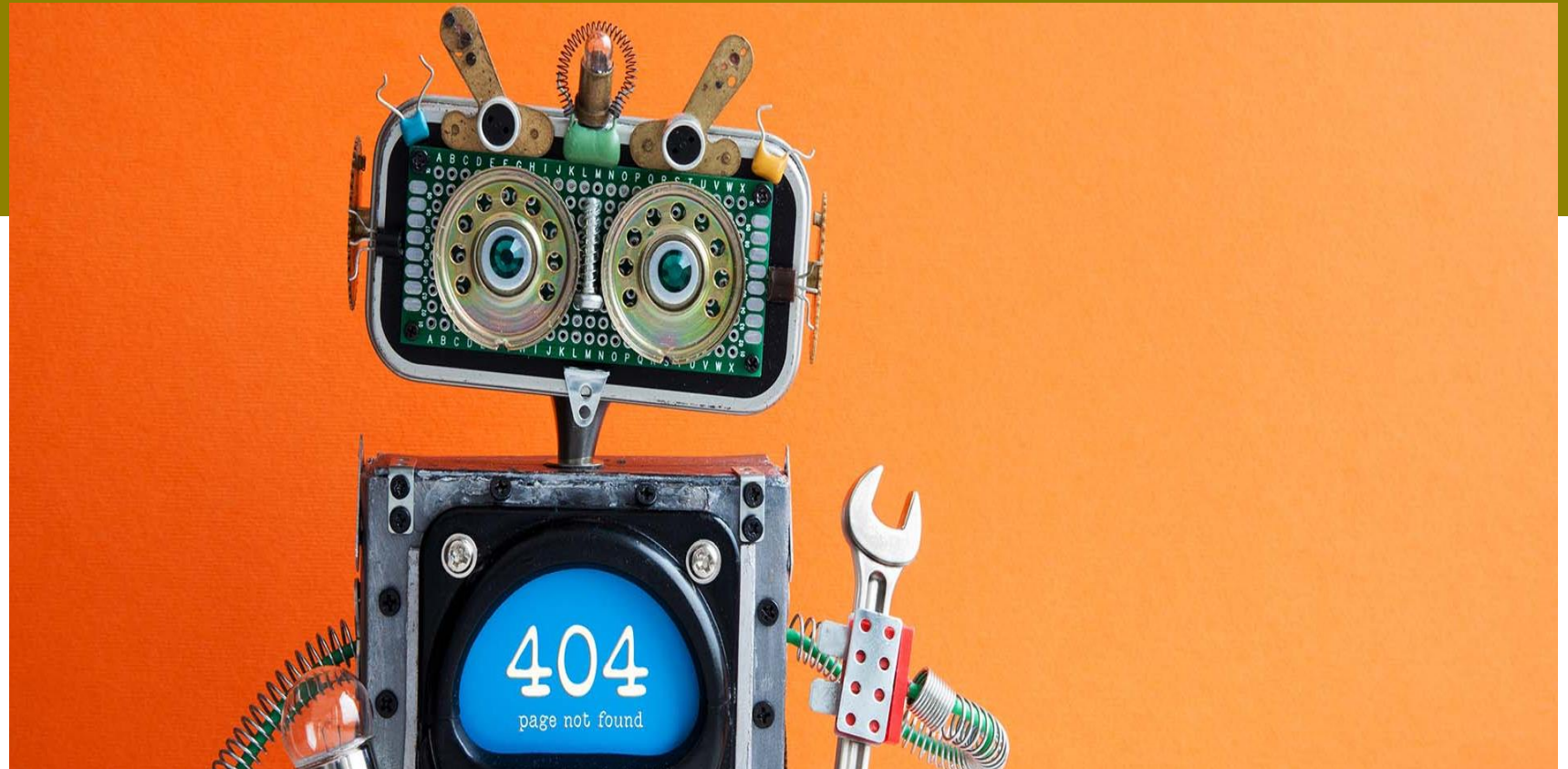


”Tay”

Den racistiske og sexistiske chatbot

Tay

- I 2016 lancerede Microsoft chatrobotten ‘Tay’
- Var designet til at chatte med folk og blive bedre til det over tid
- Måtte tage robotten ned efter 16 timer pga. sexistiske og racistiske kommentarer



Samsungs læk af data ind i ChatGPT

The image is a screenshot of a Bloomberg news article. At the top, the Bloomberg logo is on the left, and 'US Edition', 'Sign In', and 'Subscribe' are on the right. A navigation bar below the logo lists various categories: Live Now, Markets, Economics, Industries, Technology (highlighted), Politics, Wealth, Pursuits, Opinion, Businessweek, Equality, Green, CityLab, Crypto, and More. The article title is 'Samsung Bans Staff's AI Use After Spotting ChatGPT Data Leak'. Below the title are two bullet points: 'Employees accidentally leaked sensitive data via ChatGPT' and 'Company preparing own internal artificial intelligence tools'. The author is 'Mark Gurman' and the date is 'May 2, 2023 at 2:48 AM GMT+2'. On the right side, there is a 'Markets at a Glance' section showing 'Americas' selected, with 'Dow Jones' at 33,594.38, down 0.07%.

Bloomberg US Edition Sign In [Subscribe](#) 🔍

• Live Now Markets Economics Industries **Technology** Politics Wealth Pursuits Opinion Businessweek Equality Green CityLab Crypto More

Technology AI

Samsung Bans Staff's AI Use After Spotting ChatGPT Data Leak

- Employees accidentally leaked sensitive data via ChatGPT
- Company preparing own internal artificial intelligence tools

By [Mark Gurman](#)
May 2, 2023 at 2:48 AM GMT+2 Updated on May 2, 2023 at 7:54 AM GMT+2

Markets at a Glance

Americas	Europe	APAC	Your List
Dow Jones	33,594.38	▼ -0.07%	📈

Når det går galt i den juridiske virkelighed

BBC Sign in Home News Sport Reel Worklife Travel Future


NEWS

Home | War in Ukraine | Climate | Video | World | UK | Business | Tech | Science | Entertainment & Arts

World | Africa | Asia | Australia | Europe | Latin America | Middle East | US & Canada

ChatGPT: US lawyer admits using AI for case research

© 27 May



Forbes

FORBES > INNOVATION > CONSUMER TECH

Lawyer Uses ChatGPT In Federal Court And It Goes Horribly Wrong

Matt Novak Contributor @
FOIA reporter and founder of Paleofuture.com, writing news and opinion on every aspect of...

Follow

2 May 27, 2023, 06:11pm EDT



In this photo illustration, ChatGPT logo of a chatbot launched by OpenAI is seen on a smartphone in ... [+] SOPA IMAGES/LIGHTROCKET VIA GETTY IMAGES

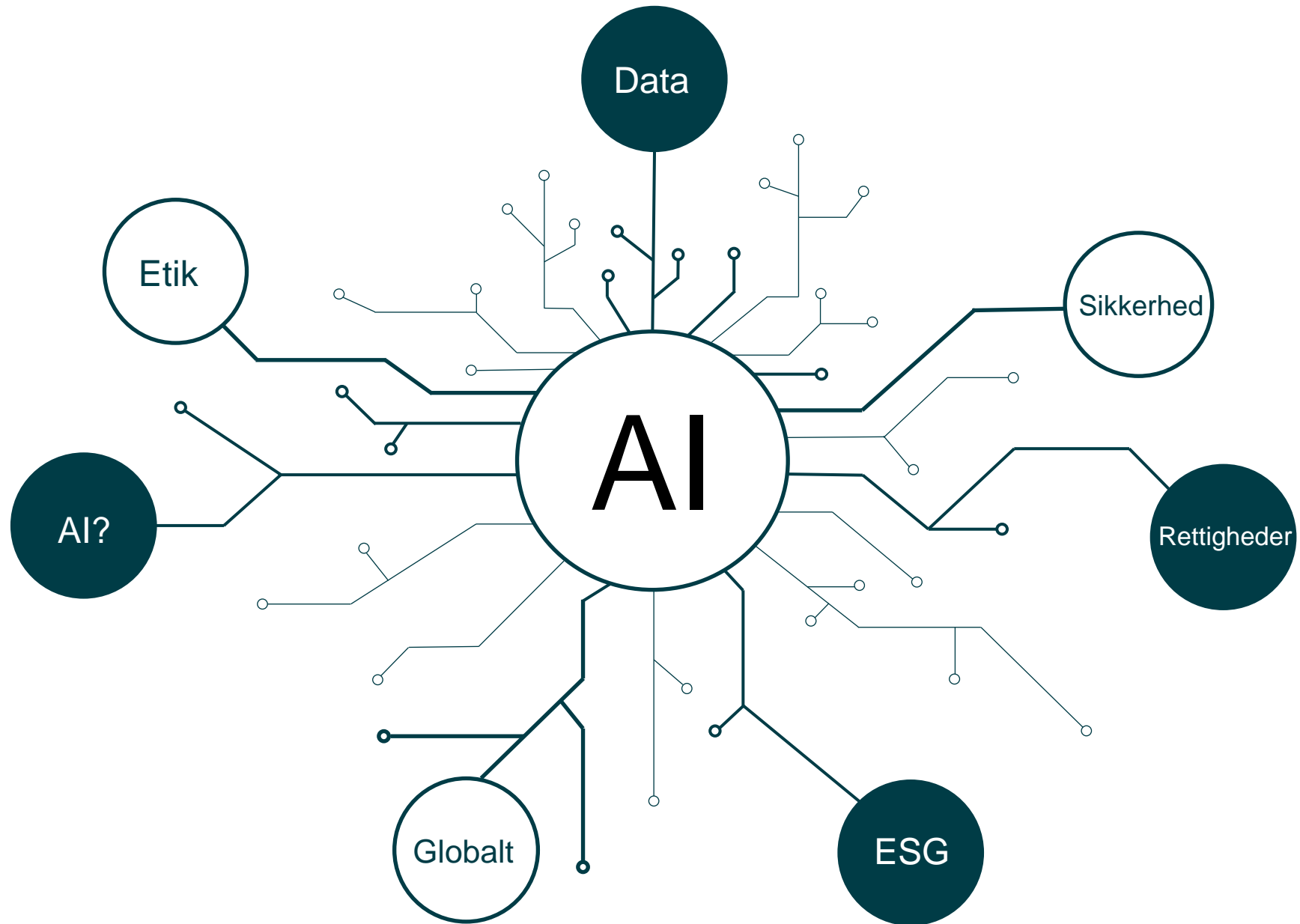
Hvad er det vi er bange for?

**Nye anvendelser
og formål**

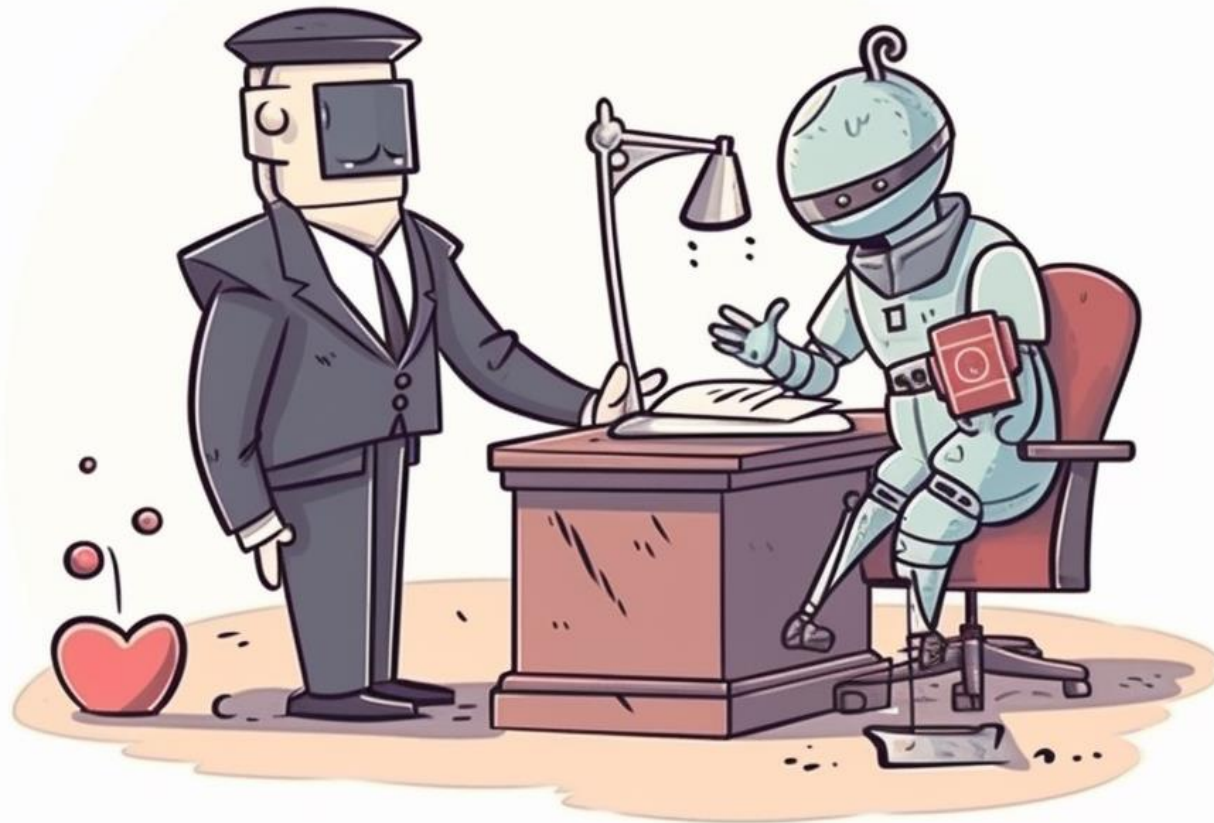
**Nøjagtighed og
korrekthed**

**Tab af
kontrol**

**Etik og
ansvar**



Må vi anvende generativ AI?



Ja... men....

- ✓ ...hav en omhyggelig tilgang, der omfatter **klare retningslinjer for brugen**
- ✓ Implementering og brug skal ske med **nødvendig omtanke for eksisterende område:**
 - Licens- og brugervilkår
 - IP
 - Databeskyttelse og fortrolighed
 - Cybersikkerhed
 - Fremtidig (AI-specifik) lovgivning
 - Etik og ansvar
- ✓ Ukritisk og ukontrolleret brug kan medføre **store juridiske og kommercielle risici**



Midjourney Bot **BOT** i dag kl. 17:54

lawyer looking at an engineer, the engineer is using a chatbot on a PC; chatbot is giving rubbish answers, lawyer is looking very distrustful at the PC; cartoon style --v 5 - (fast)

Licens- og brugervilkår

Brugere

- Forbud mod **kommerciel brug, deling af output** m.v.
- Restriktioner i forhold til **integration af AI-værktøjet med andre systemer eller teknologier.**
- **Ansvar**...for hvem og for hvad?
- **Jurisdiktionsmæssige udfordringer** som følge af leverandørens placering.



Leverandører

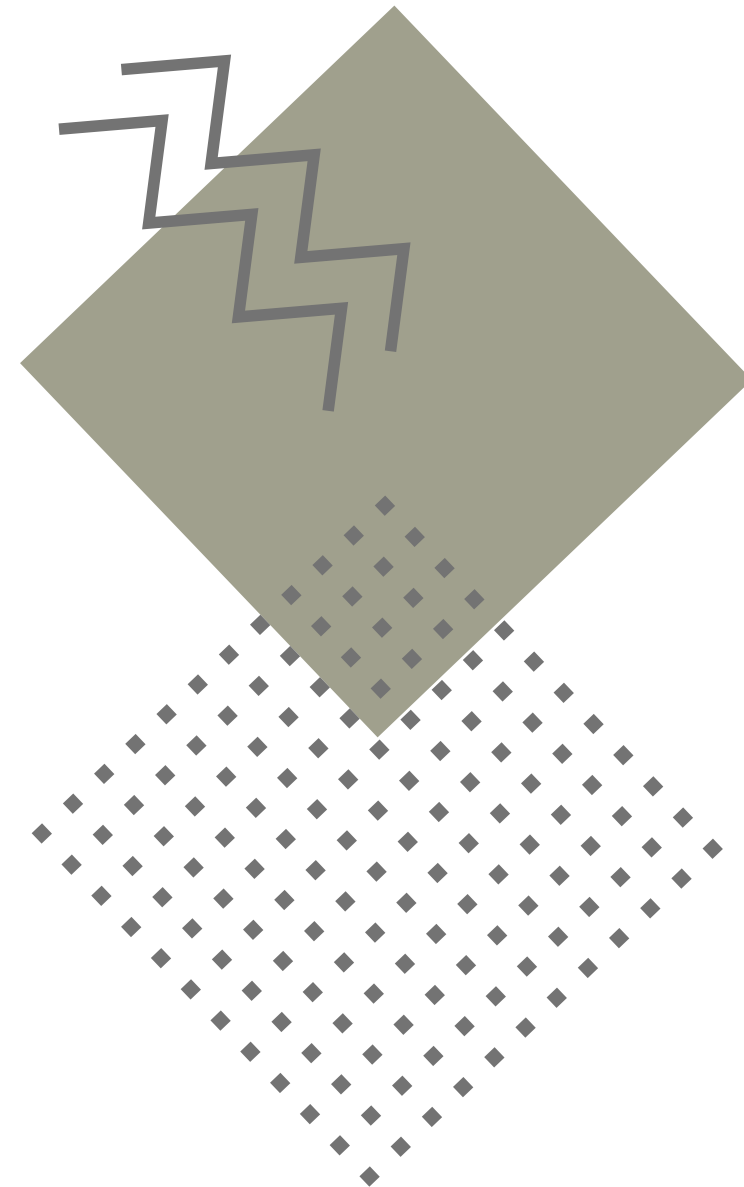
- Adgang til at **bruge input som træningsdata.**
- Ret til at **opdatere eller ændre AI og/eller vilkår** uden forudgående varsel.
- Ikke nødvendigvis **krav om overholdelse af specifikke standarder** ift. sikkerhed, databehandling e.l.



Køb af AI-løsninger

Hvordan afgør man, om en AI-løsning lever op til en aftale?

- *Kravspecifikation*
- *Afhjælpning*
- *Servicemål*
- *Compliance – eller bistand til opfyldelse*
- *Fortsat udvikling og træning?*

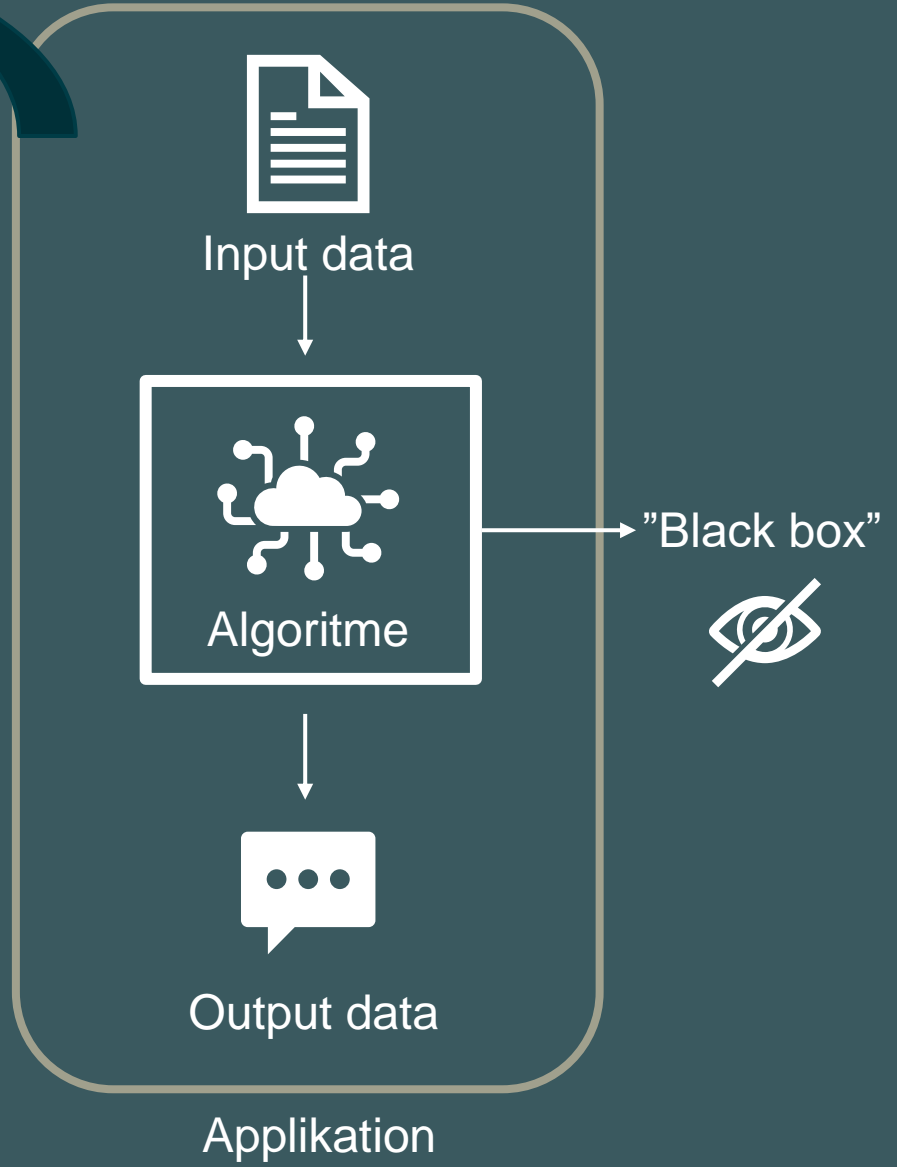
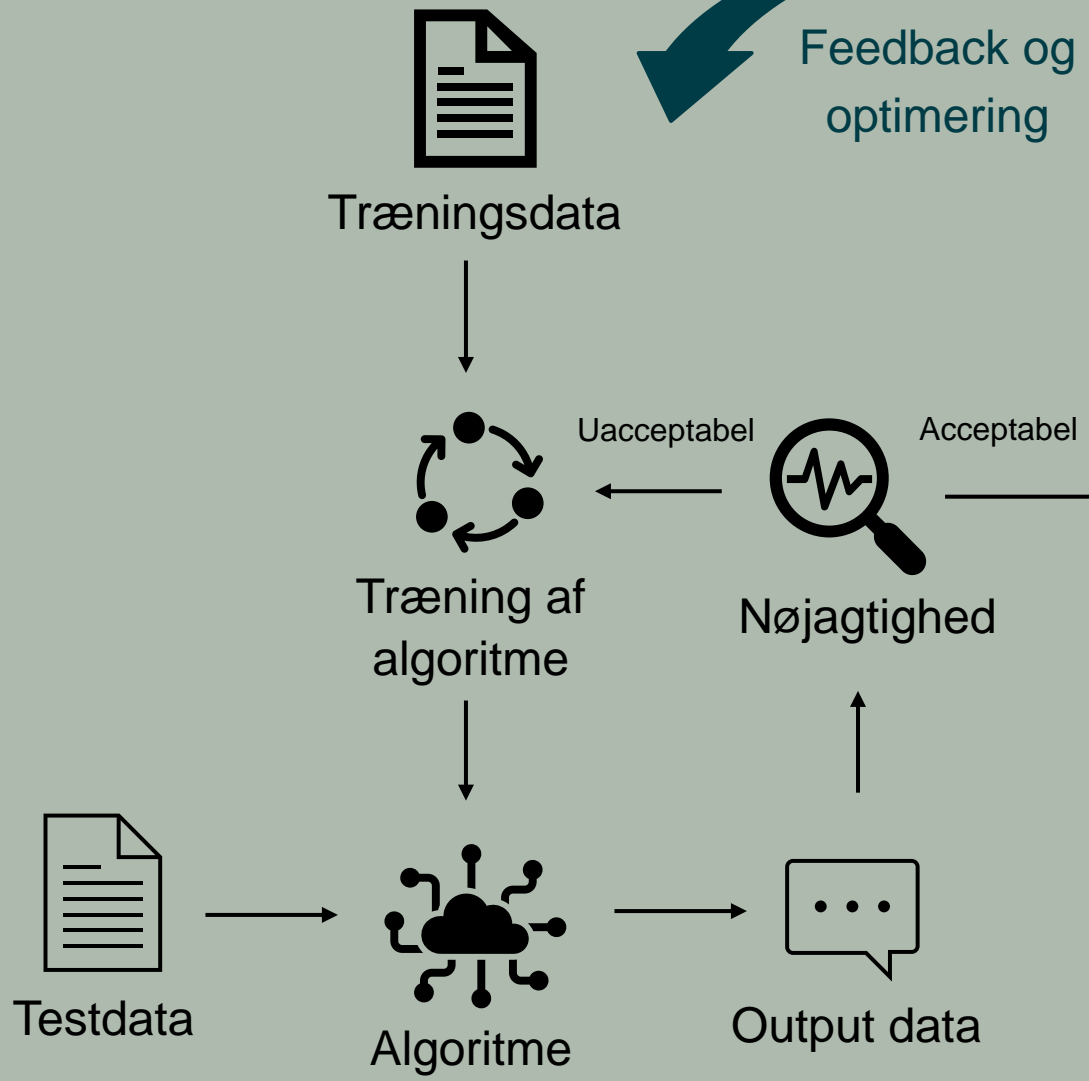


A stylized world map where the landmasses are dark teal with white outlines. A large, irregular red area highlights the upper right portion of the map, covering parts of North America, the Atlantic Ocean, and Europe. The text 'Leverandørstyring' is written in white serif font across the red area.

Leverandørstyring

Træning af modellen

Brug af modellen



Immaterielle rettigheder

Der er fortsat uklarhed vedrørende IP/rettigheder, når det kommer til træning af AI og brug af resultaterne.



Rettigheder til outputtet

Tvivlsomt om outputtet kan beskyttes som en immateriel rettighed.

I så fald er spørgsmålet, hvem der ejer sådanne rettigheder?

Vær altid opmærksom på rettighedsspørgsmålet inden kreativt indhold anvendes kommercielt.



Men hvad med den hybride intelligens?



Risiko for krænkelse

AI-løsningerne er trænet på eksisterende data, der kan være underlagt immaterielle rettigheder.

Det medfører en risiko for, at outputtet krænker eksisterende rettigheder.



Træning af AI

Adgang til at træne på data? – Ny regel i ophavsretslovens § 11 b

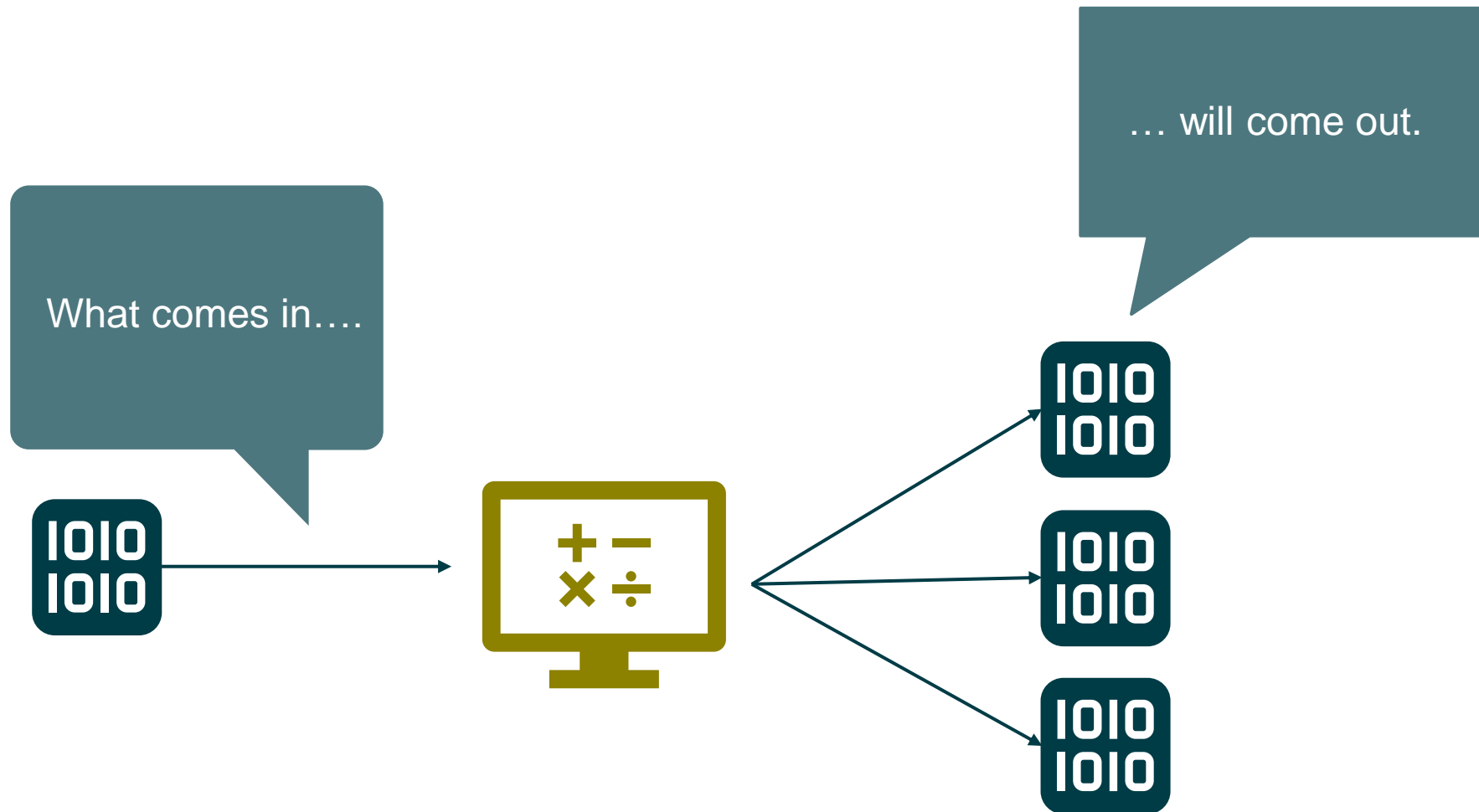
AI-systemer trænes også på de oplysninger, der indtastes.

Derfor skal det altid sikres, at der ikke indtastes forretningshemmeligheder.


“We will step in and defend our customers and pay the costs incurred if you face legal claims around copyright infringement, and this applies both to ChatGPT Enterprise and the API.”

- Sam Altman, CEO at OpenAI


Databeskyttelse og fortrolighed




Databeskyttelse og fortrolighed




Oplysninger i åbne, generative AI-systemer svarer næsten til offentliggørelse.




Risikovurderinger skal revideres og i endnu større grad være et fokusområde fremadrettet. Behov for DPIA



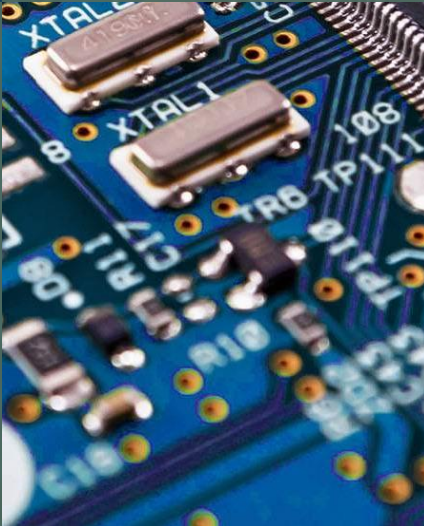
Dataansvar, risikovurdering, databehandler-aftaler, tilsyn med databehandlere.



Sikkerhed, og anmeldelse til databeskyttelsesmyndighederne i tilfælde af databrud.

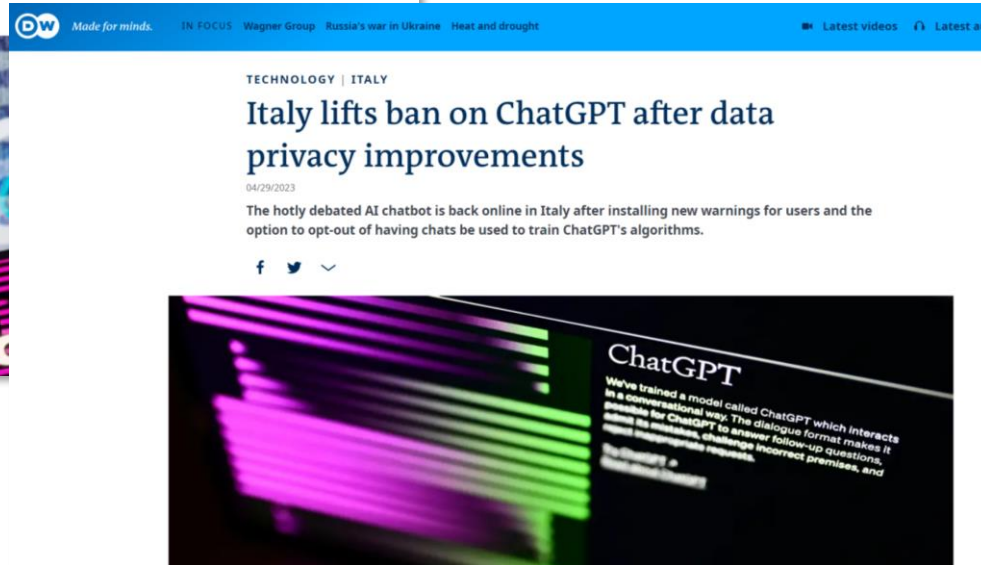


AI må ikke kompromittere virksomhedens forretningskritiske oplysninger.



Vejled medarbejdere om databeskyttelse i en AI-specifik kontekst.

Italiensk forbud mod ChatGPT



Already [under investigation](#) by the data protection authorities (DPAs) of several EU nations, OpenAI is now facing scrutiny in Poland in response to an August GDPR complaint.

GDPR - overblik

Personoplysninger er enhver form for information om en identificeret eller identificer fysisk person

Behandlingsgrundlag

Behandlingsgrundlag til indsamling, opbevaring og behandling af personoplysninger, fx brug af AI på eksisterende data

Transparens

Information til fysiske personer om, hvordan deres personoplysninger bliver indsamlet og behandlet, skal være tilgængelig og tilstrækkeligt detaljeret

Rettigheder

Hvordan håndteres retten til at blive glemt i en machine learning-model, hvis sletning af data underminerer modellens korrekthed eller er umulig?

Risikovurderinger

Sammen med NIS2/DORA risikovurderinger, vurderes og adresseres risici for de berørte individer

DPIA'er

Dyk ned i datastrømmene, systemer, samspil såvel som risici og nødvendige sikkerhedsforanstaltninger for de identificerede højrisiko-områder

Internationale overførsler

Schrems III lurder rundt om hjørnet

6. Cybersikkerhed



Procedurer og politikker



Risikovurdering



Sikkerhedsforanstaltninger



Overvågning



Data poisoning



Data leaks



Spear fishing



Adversarial attacks

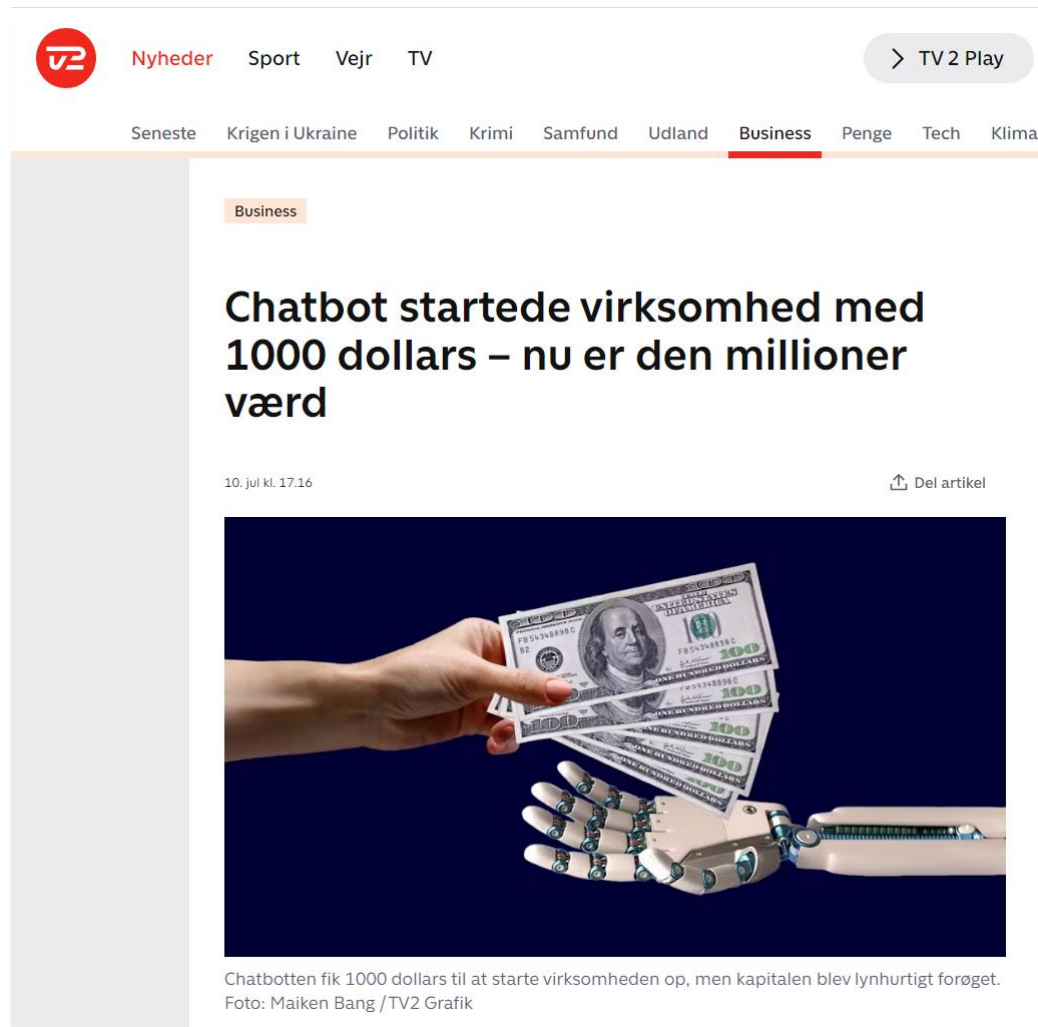


Model theft



Surveillance

Ansvar og business judgement




TV2 Nyheder Sport Vejr TV > TV 2 Play

Seneste Krigen i Ukraine Politik Krimi Samfund Udland **Business** Penge Tech Klima

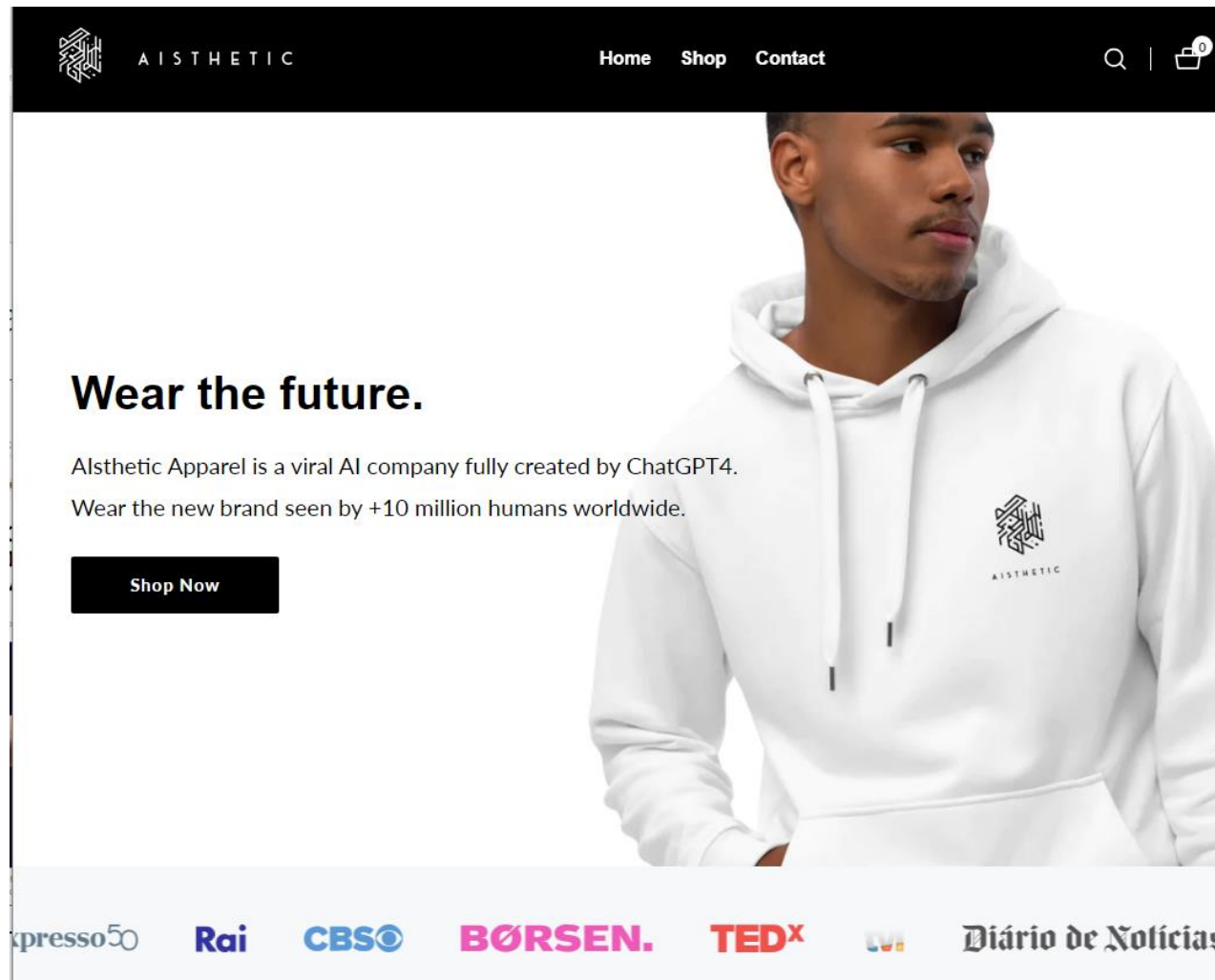
Business

Chatbot startede virksomhed med 1000 dollars – nu er den millioner værd

10. juli kl. 17.16 [Del artikel](#)



Chatbotten fik 1000 dollars til at starte virksomheden op, men kapitalen blev lynhurtigt forøget.
Foto: Maiken Bang / TV2 Grafik




A I S T H E T I C Home Shop Contact

Wear the future.

Alsthetic Apparel is a viral AI company fully created by ChatGPT4.
Wear the new brand seen by +10 million humans worldwide.

[Shop Now](#)



presso50 Rai CBSO BØRSEN. TEDx Diário de Notícias

Ansvarlighed



Hvad er AI bias?

Make a big impact with our professional slides and charts

MISSION

Make a big impact with professional slides, charts, infographics and more.

VISION

Make a big impact with professional slides, charts, infographics and more.



OUR FOCUS

Make a big impact with professional slides, charts, infographics and more.

KEY STRATEGY

Make a big impact with professional slides, charts, infographics and more.

The Amazon logo, consisting of a white lowercase 'a' with a curved arrow underneath it, set against a black circular background.

Amazon hemmelige rekrutteringssystem

Amazons nye rekrutteringssystem kunne ikke lide kvinder

A small, colorful robot made of electronic components like a breadboard, resistors, and a small screen. The screen displays the number '404' and the text 'not found'. The robot is holding a wrench and a screwdriver.

"Tay" Den racistiske og sexistiske chatbot

Blev taget ned på under 24 timer.

ESG?

- Environmental...
 - Miljøpåvirkning?
 - Hvad er egentlig sandt – og kan I få data?
- Social
 - Trivsel – påvirkning +/- ?
 - Diversitet og inklusion +/- ?
 - Menneskerettigheder +/- ?
- (Corporate) Governance
 - Etik

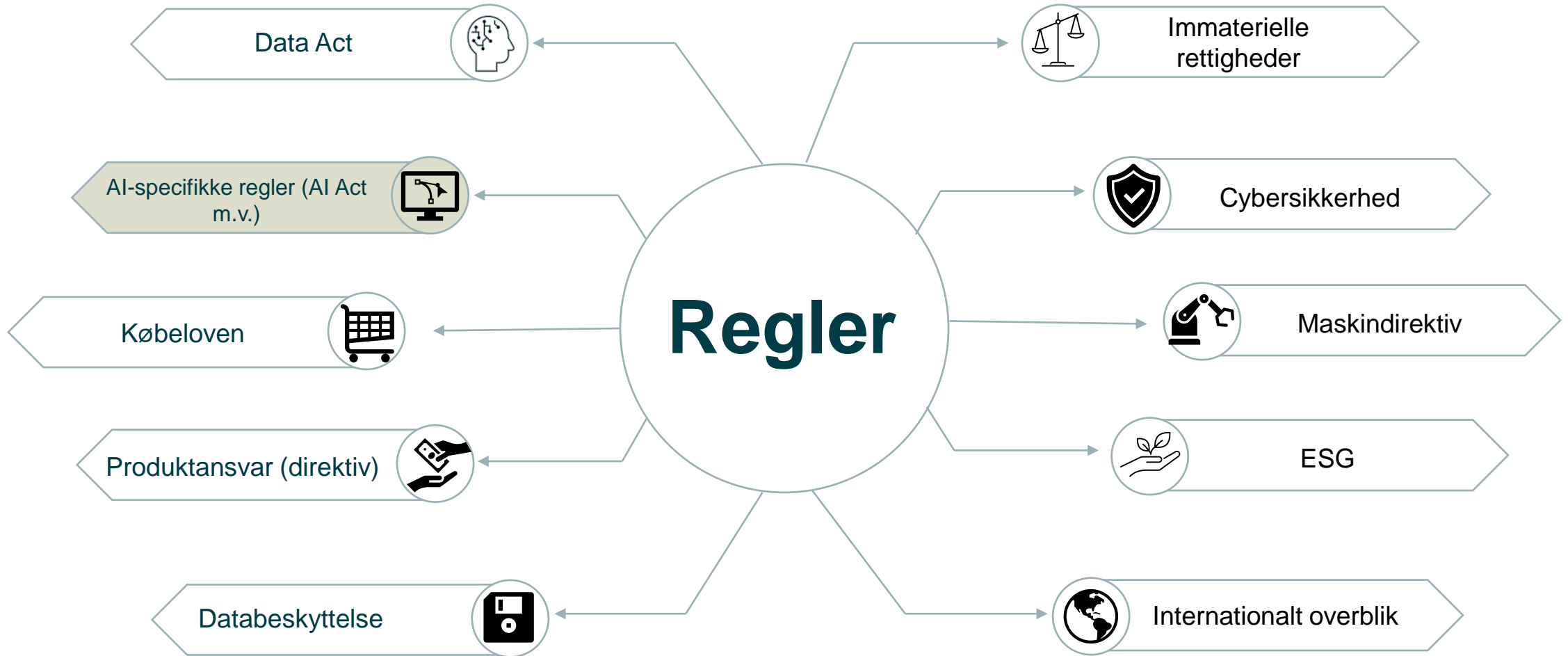
...OSV OSV OSV...

Beregninger fra forskere på Datalogisk Institut på Københavns Universitet (DIKU) viser, at en enkelt forespørgsel (prompt) til Chat GPT i gennemsnit koster et energiforbrug på 0,19 kWh eller det samme som 40 opladninger af din mobiltelefon. For samme mængde strøm kan du også køre 1 km i din elektriske bil eller streame en times video.

“
Beregninger fra Datalogisk Institut på KU viser, at en enkelt forespørgsel til Chat GPT i gennemsnit koster et energiforbrug på 0,19 kWh eller det samme som 40 opladninger af din mobiltelefon

Hvis vi antager, at du affyrer 20 prompts til Chat GPT for at finjustere en tekst, så den tilfredsstillende dine ønsker til format, længde og sproglig tone, så svarer det altså til, at du kan køre 20 km i din elbil, oplade din telefon dagligt i mere end to år eller binge din favoritserie i næsten et døgn.

Compliance



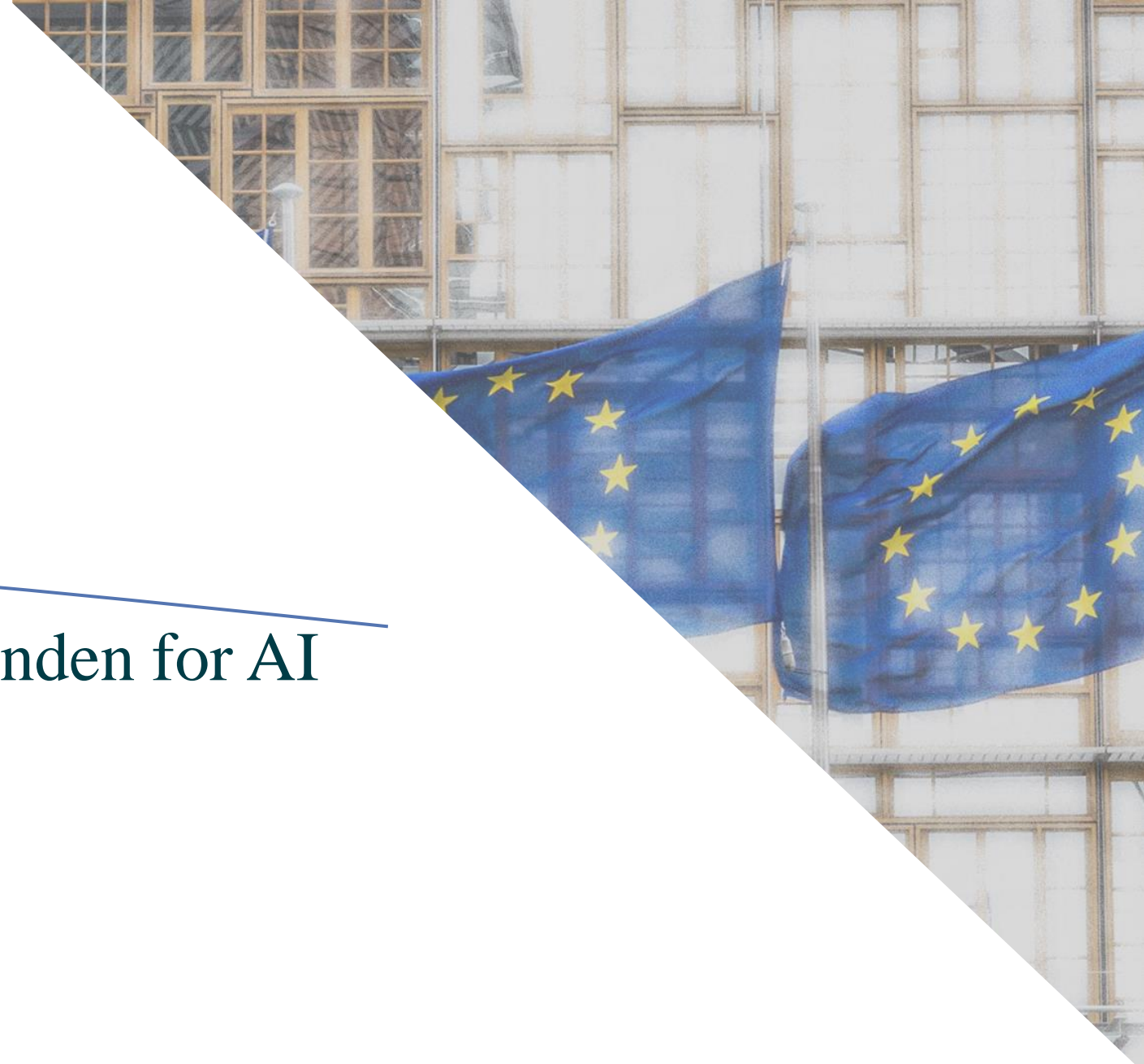
Fremtidig (AI-specifik) lovgivning

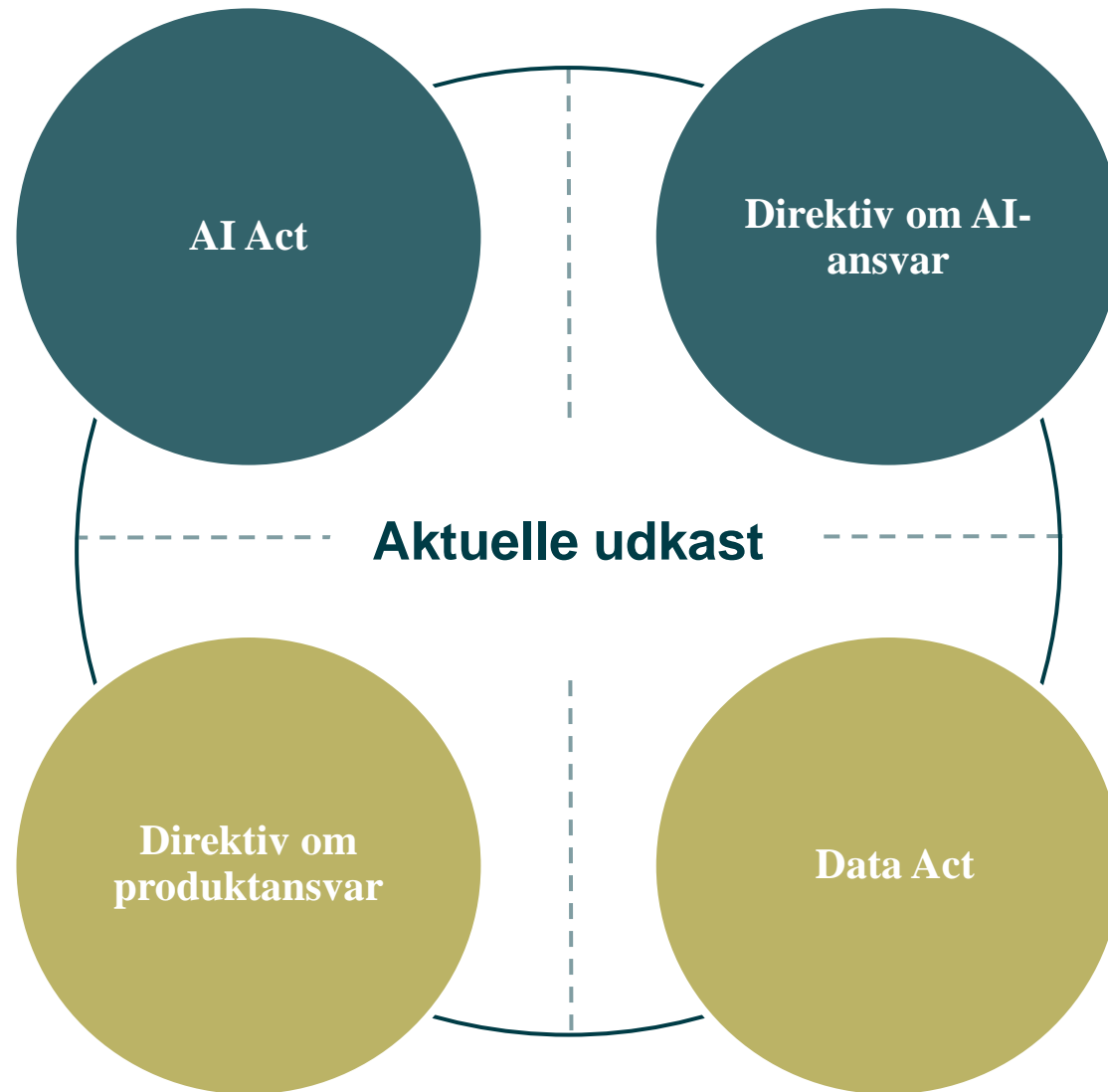
- Efter to års forhandlinger har Europa-Parlamentets ledende parlamentariske udvalg godkendt udkastet til den længe ventede AI Act.
- Men... Der er **LANG** vej igen før endelig vedtagelse og ikrafttræden.
- Vil medføre en række forpligtelser og mulighed for bøder, afhængig af kategorisering:
 - Minimal risiko → Skal være tilladt og enkelt at bruge
 - Begrænset risiko → Klare krav om transparens
 - Høj risiko → Hvor brug af software kan underminere borgere
 - Uacceptabel → Områder hvor Kommissionen forbyder kunstig intelligens
- Transparenskrav for generativ AI?



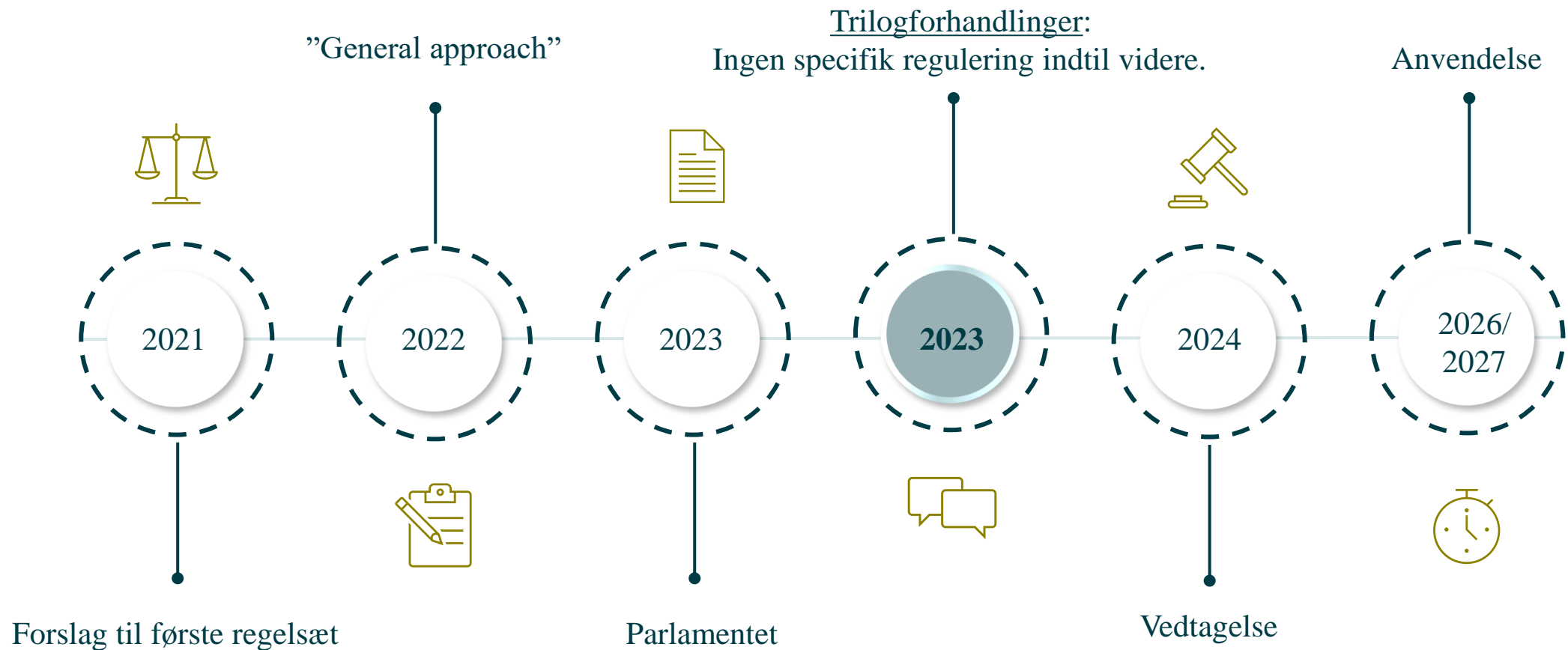
”Excellence and trust”

EU vil være global leder inden for AI





AI-forordningen



AI-forordningen = tre forskellige udkast



Brussels, 21.4.2021
COM(2021) 206 final

2021/0106 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

**LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE
(ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION
LEGISLATIVE ACTS**

{SEC(2021) 167 final} - {SWD(2021) 84 final} - {SWD(2021) 85 final}



**Interinstitutional File:
2021/0106(COD)**

Brussels, 29 November 2021
(OR. en)

14278/21

LIMITE

TELECOM 430
JAI 1288
COPEN 412
CYBER 307
DATAPROTECT 267
EJUSTICE 103
COSI 236
IXIM 262
ENFOPOL 465
FREMP 272
RELEX 1012
MI 879
COMPET 860
CODEC 1530

NOTE

From: Presidency
To: Delegations
No. Cion doc.: 8115/20
Subject: Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts
- Presidency compromise text



Committee on the Internal Market and Consumer Protection
Committee on Civil Liberties, Justice and Home Affairs

KMB/DA/AS

16/5/2023

Version: 1.1

DRAFT Compromise Amendments

on the Draft Report

Proposal for a regulation of the European Parliament and of the Council
on harmonised rules on Artificial Intelligence (Artificial Intelligence Act)
and amending certain Union Legislative Acts

(COM(2021)0206 – C9 0146/2021 – 2021/0106(COD))

Rapporteurs:

Brando Benifei & Ioan-Dragoş Tudorache

(Joint committee procedure – Rule 58 of the Rules of Procedure)

AI-forordningens indhold og formål

ARTICLE 1

Subject matter

The purpose of this Regulation is to promote the uptake of human centric and trustworthy artificial intelligence and to ensure a high level of protection of health, safety, fundamental rights, democracy and rule of law, and the environment from harmful effects of artificial intelligence systems in the Union while supporting innovation.



AI forordningens indhold og formål

Article 1

Subject matter

The purpose of this Regulation is to promote the uptake of human centric and trustworthy artificial intelligence and to ensure a high level of protection of health, safety, fundamental rights, democracy and rule of law, and the environment from harmful effects of artificial intelligence systems in the Union while supporting innovation.



- Fastsætter harmoniserede regler for **omsætning, ibrugtagning og anvendelse** af AI
- Finder anvendelse på **stort set alle AI systemer**
- **Forbyder** visse anvendelser af AI
- Stiller **krav til højrisiko AI** og de økonomiske aktører involveret i systemerne
- Fastlægger **gennemsigtighedsforpligtelser** for visse AI systemer
- Støtter **innovation** gennem oprettelse af “sandkasser”
- Skal implementeres gennem
 - Oprettelse af et **EU AI Office**
 - Udpegning af **nationale tilsynsmyndigheder**
 - Regler om **markedsovervågning**
- Indeholder **bøder** på niveau med eller over GDPR
- Træder i kraft **2-3 år** efter vedtagelsen

Uacceptabel risiko = forbud

Kognitiv adfærdsmæssig manipulation

Hvis det kan påføre den pågældende eller andre fysisk eller psykisk skade – eller specifikke sårbare grupper.

Social scoring

Klassificering af mennesker baseret på adfærd socioøkonomisk status eller personlige karakteristika.

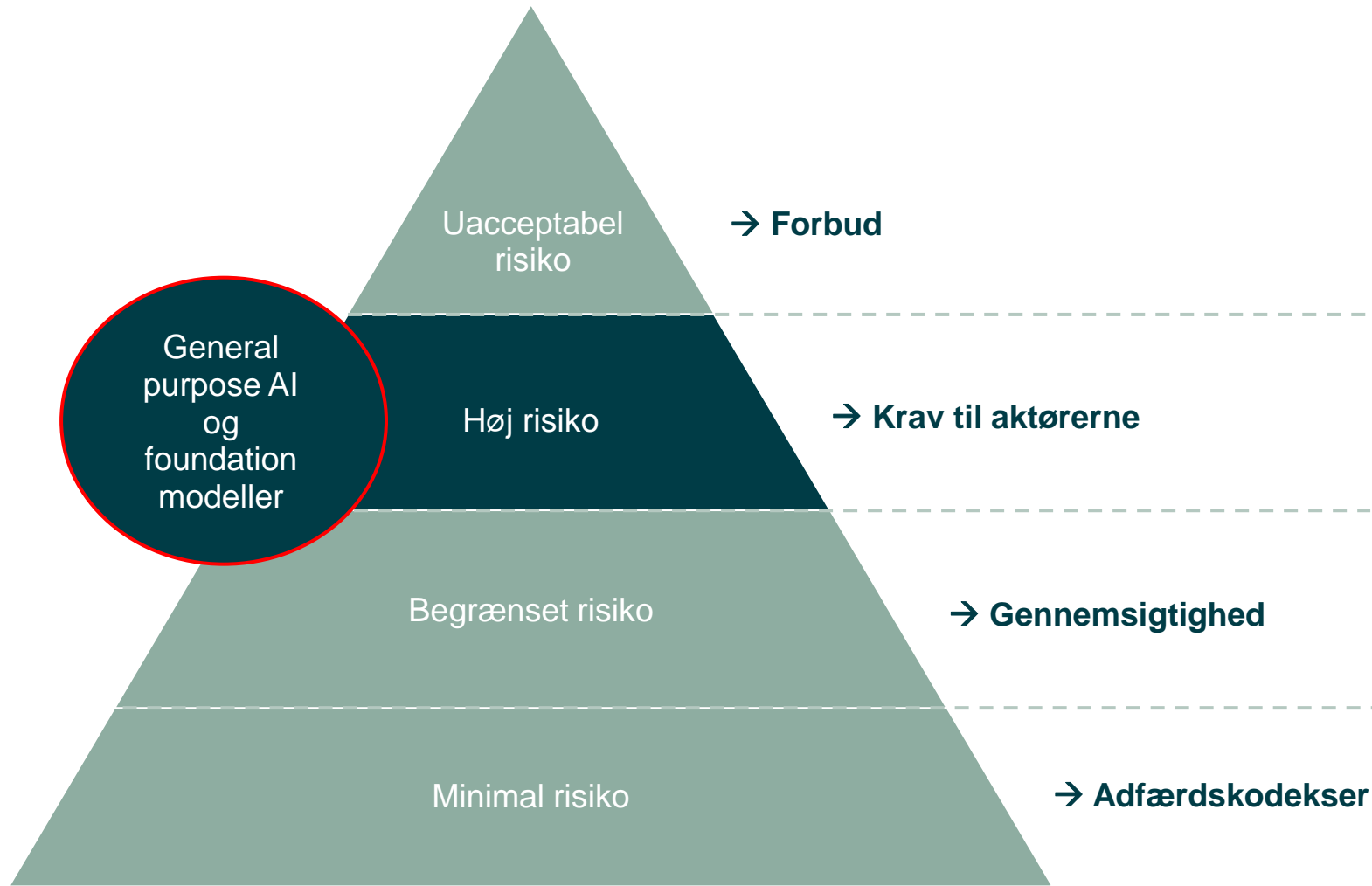
Biometriske identifikationssystemer i realtid og på afstand

Med mindre det er strengt nødvendigt til de formål der er oplyst i forordningen.

Undtagelser



Risikobaseret tilgang



Hvad er højrisiko AI?

”Farlige” produkter – AI systemer, som

1. udgør (en del af) et produkt omfattet af EU’s produktsikkerhedslovgivning og
2. skal undergives en overensstemmelsesvurdering fra en tredjepart, fx køretøjer, radioudstyr, medicinsk udstyr og legetøj.

Højrisiko use cases – AI systemer, som

1. falder under et af de kritiske områder og
2. uses cases oplistet i Annex III og som udgør en væsentlig risiko for menneskers sundhed, sikkerhed eller grundlæggende rettigheder.

Højrisiko områder og use cases oplistet i Annex III

Biometric and biometrics-based systems

Management and operation of critical infrastructure

Education and vocational training

Employment, workers management and access to self-employment

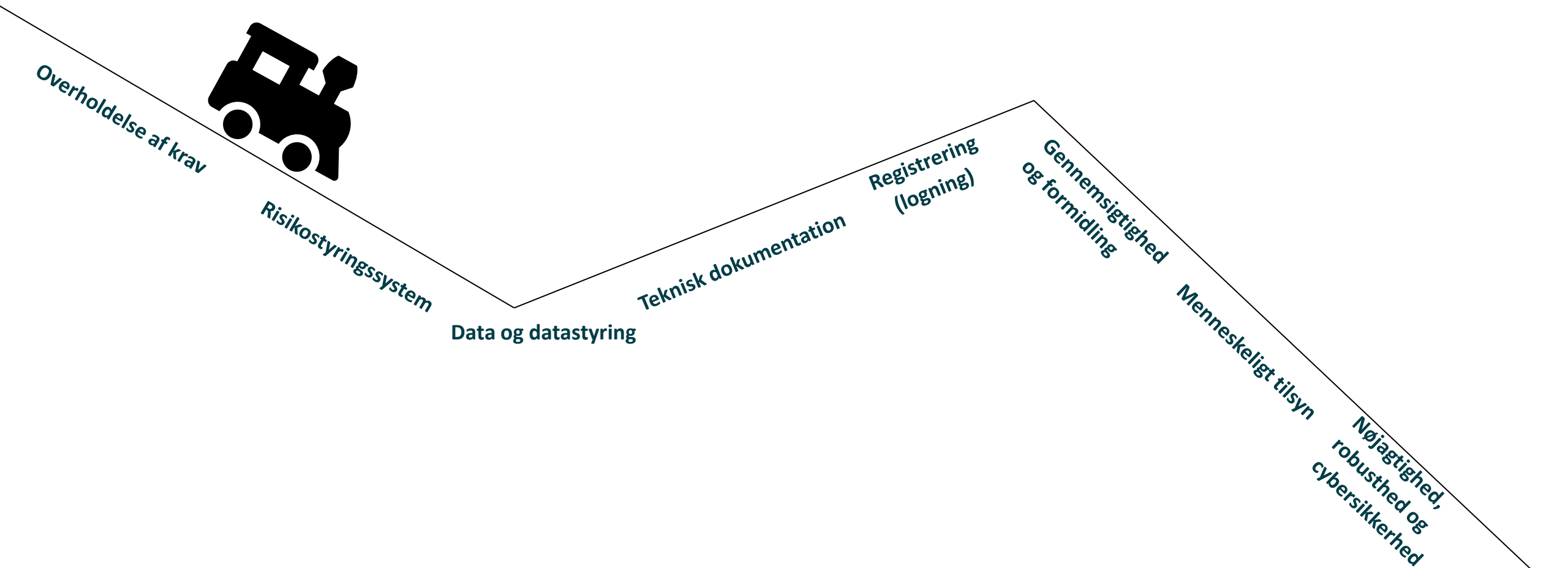
Access to and enjoyment of essential private services and public services and benefits

Law enforcement

Migration, asylum and border control management

Administration of justice and democratic processes

Krav til højrisko AI-systemer



Og så kom ChatGPT ...

- Foranledigt af bl.a. ChatGPT og den eksplosive udvikling inden for generativ AI har EU Parlamentet for nylig tilføjet en række særlige krav til "foundation models", som er store modeller, der kan tilpasses til flere forskellige formål

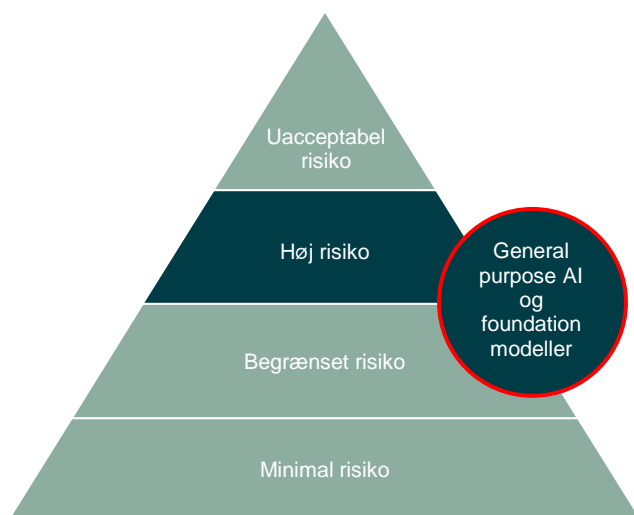
Forpligtelser for udbydere af "foundation models" (artikel 28 b)

Inden systemet sættes på markedet, skal udbyderen bl.a.

- Identificere, reducere og mitigere risici – og dokumentere de resterende
- Kun benytte data, som er underlagt passende data governance procedurer, herunder i relation til egnethed og mulige bias
- Designe og udvikle modellen på en måde, som sikrer et passende niveau af performance, forudsigelighed, forklarlighed og sikkerhed, herunder gennem inddragelse af eksperter og tests
- Energioptimere modellen
- Udarbejde teknisk dokumentation, så downstream operatører kan opfylde forordningen
- Etablere et kvalitetsledelsessystem

Er der tale om **generativ AI**, skal udbyderen desuden

- Opfylde visse gennemsigtighedsforpligtelser
- Træne, designe og udvikle modellen på en måde, som sikrer beskyttelse mod generering af indhold i strid med lovgivningen
- Offentliggøre et summary af anvendt træningsdata, som er underlagt ophavsretlig beskyttelse



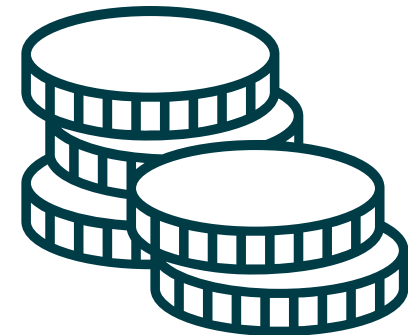
'foundation model' means an AI model that is trained on broad data at scale, is designed for generality of output, and can be adapted to a wide range of distinctive tasks;

'general purpose AI system' means an AI system that can be used in and adapted to a wide range of applications for which it was not intentionally and specifically designed;



Forpligtelser for **de økonomiske aktører** i relation til højrisiko AI systemer

- forordningen indeholder forpligtelser for hele værdikæden, herunder udbydere, distributører, importører, brugere og andre involveret i omsætningen af et højrisiko AI system



Udblik – resten af verden

› Australien	› Ingen specifik AI-lovgivning, men eksisterende national lovgivning regulerer brugen af AI.
› Brasilien	› I landet er foreslået en AI-bill, der temmelig udførligt regulerer AI
› Canada	› Landet forbereder den såkaldte AI and Data Act, som hovedsageligt tager sigte på højrisikosystemer.
› Kina	› Landet forbereder flere omfattende regelsæt på området og har allerede AI-regelsæt i kraft.
› Indien	› Landet forbereder en ny Digital Act, der også tager sigte på AI
› Israel	› Ingen regler om AI er vedtaget, men andre mitigerende tiltag forberedes såvel som lovgiver har politisk guides til AI til rådighed
› Japan	› Ingen regler om AI. Landet satser i øjeblikket på, at den private sektor selvregulerer.
› New Zealand	› Ingen specifikke regler om AI, men Algorithm Charter gælder, som regulerer brugen af algoritmer
› Saudi Arabien	› Ingen specifikke regler – lovgiver satser på at tiltrække AI-virksomheder ved en i hovedsagen slap regulering.
› Singapore	› Ingen egentlig regulering – men der er udviklet frivillige governance frameworks
› Sydkorea	› Ingen specifik regulering af AI, men regler om hvordan man får adgang til AI-teknologi. Landet udvikler også nye standarder i.f.t. håndteringen af ophavsret
› Emiraterne	› Ingen specifikke regler, men de første til at etablere et AI-ministerie, som skal sikre at udviklingen af AI sker på en AI-venlig måde
› UK	› Ingen specifikke regler, men der lægges op til kontekst- og sektorspecifik regulering
› US	› Ingen specifikke regler, men flere omfattende regelsæt er stillet i forslag

Hvis det går galt alligevel ...

EU har fremsat forslag til to reguleringer, som skal sikre adgang til kompensation, hvis AI systemer forårsager skader:

Et nyt produktansvarsdirektiv

Proposal for a directive of the European Parliament and of the Council on liability for defective products

Et separat direktiv om AI ansvar

Proposal for a Directive on adapting non contractual civil liability rules to artificial intelligence



Produktansvar for software & datatab som en skade

En opdatering af produktansvarsdirektivet fra 1985 skal tilpasse reglerne den digitale tidsalder, bl.a. ved at gøre det klart, at software er et produkt, og at datatab eller -ødelæggelse udgør en skade



Manglende cybersikkerhed som en "defekt"

Vurderingen af, om et produkt er "defekt", skal inkludere produktets digitale elementer, fx forbindelse til andre produkter eller netværk, "self-learning" elementer, og krav til digitale produkter, fx i relation til cybersikkerhed



Editionsregler og lempelse af bevisbyrden

For at gøre det lettere at underbygge et erstatningskrav, vil de nye regler indføre editionsregler for udbydere af komplekse digitale produkter og lempe bevisbyrden for kausalitet.

Omfavn AI fornuftigt

AI er kommet for at blive, men det skal stadig ikke anvendes ukritisk, som med alle andre former for teknologi.

Tag stilling til AI

Udarbejd retningslinjer så medarbejderne ved hvordan de skal forholde sig til brugen af AI, og for at kickstarte vejledning og uddannelse.

Vurder behov for tiltag og gør klar til regulering

Selvom der ikke findes AI-specifik lovgivning endnu, så kommer det, og under alle omstændigheder giver AI anledning til nye overvejelser indenfor databeskyttelse, IP og cyber. Skab og vedligehold overblik så der er klar til AI Act.

Hold jer ajour

AI udvikler sig hurtigt, og det er derfor afgørende at holde sig opdateret løbende. Tilsvarende er det afgørende, at medarbejderne uddannes i korrekt brug af de løsninger, som løbende blive tilgængelige på markedet.

Hvad gør vi?



Retningslinjer og strategi

Ledelse og mennesker

Strategi, retning og forankring
Uddannelse og kultur
Tværfagligt perspektiv

Organisatoriske foranstaltninger

Medarbejderhåndbog og lignende politikker med en AI-specifik vinkel
Kontrol og håndhævelse

Tekniske foranstaltninger?

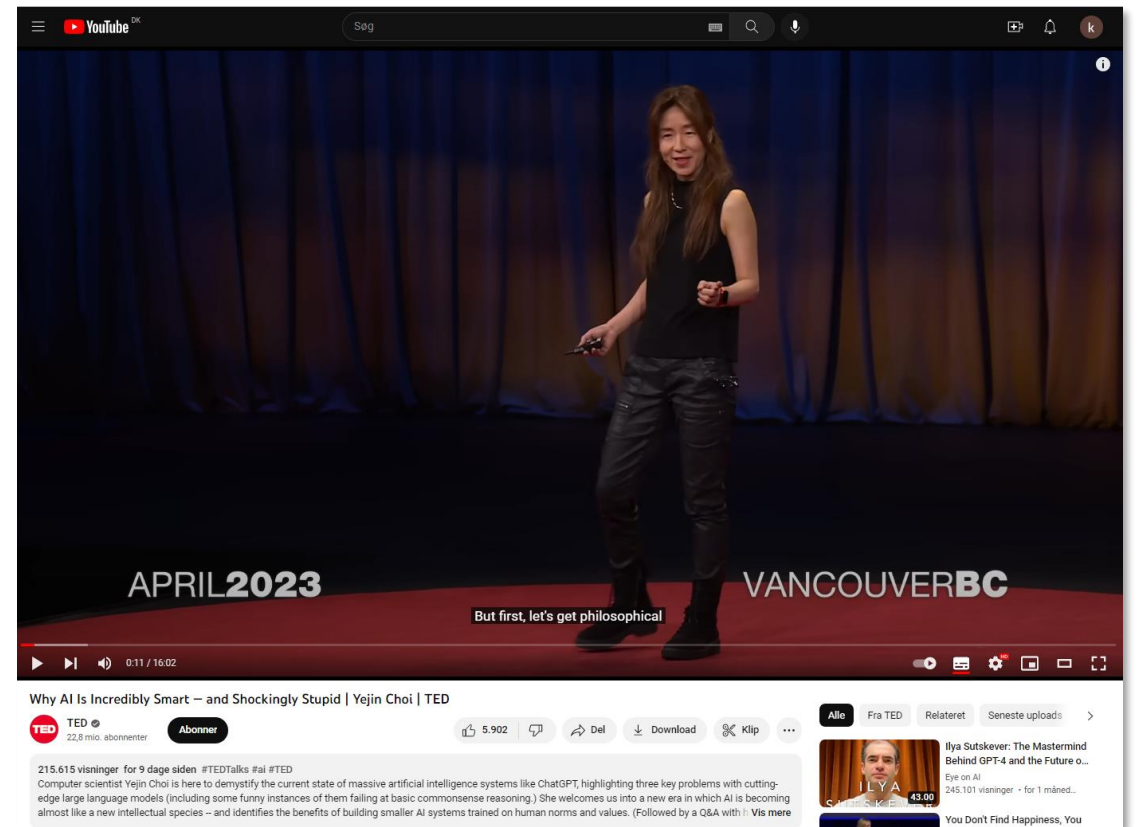
Blokering, filtre, agenter, logning?

1. Det bør være tilladt at anvende AI – men med omtanke.
2. Vær opmærksom på vilkårene for den tjeneste, der bruges
3. Generativ AI er ikke en erstatning for at tænke selv.
4. Løbende opmærksomhed på interne retningslinjer m.v., og opfordring til at række ud ved tvivl.

5. Fortrolighed må ikke blive kompromitteret.
6. Risiko for, at der ikke opnås immaterialretlig beskyttelse af outputtet – eller for krænkelse
7. Hav altid øje for rettmæssige begrænsninger, når du sender og modtager indhold.
8. Undlad eller anonymisér personoplysninger.

Bliver vi erstattet af generativ AI i morgen?

“How would you feel about an AI lawyer that aced the bar exam, yet randomly failed at such basic common sense?”



<https://www.youtube.com/watch?v=SvBR0OGT5VI>

Spørgsmål?

