

AI: Aktuelle juridiske udfordringer og muligheder

Kristian Storgaard
kst@kromannreumert.com

Potentialet er enormt!

Det er farligt – lad os forbyde det!

AI bliver vores død

Vi dør, hvis vi kommer for sent i gang!



Hvordan håndterer
vi det ansvarligt?

Advokat i karambolage med retten

Advokat fra New York brugte ChatGPT til hans juridiske undersøgelse – Fik falsk information

New York Times vs. OpenAI

Muligt fremtidigt søgsmål fra New York Times mod OpenAI

AI-indhold kan ikke beskyttes af ophavsrettigheder

Amerikansk domstol stadfæster beslutning om, at menneskelig indblanding er et “grundstenskrav” for at blive beskyttet af ophavsrettigheder

Forfattere sagsøger OpenAI for ophavsretskrænkelser

En række prominente amerikanske forfattere mener, at OpenAI uretmæssigt har brugt forfatternes værker til at træne ChatGPT.

KROMANN
REUMERT

Polen åbner privacy-undersøgelse mod ChatGPT

Ifølge en klager har ChatGPT genereret falske oplysninger om vedkommende, som ikke er blevet rettet efterfølgende

OpenAI sagsøgt for ærekrænkelser

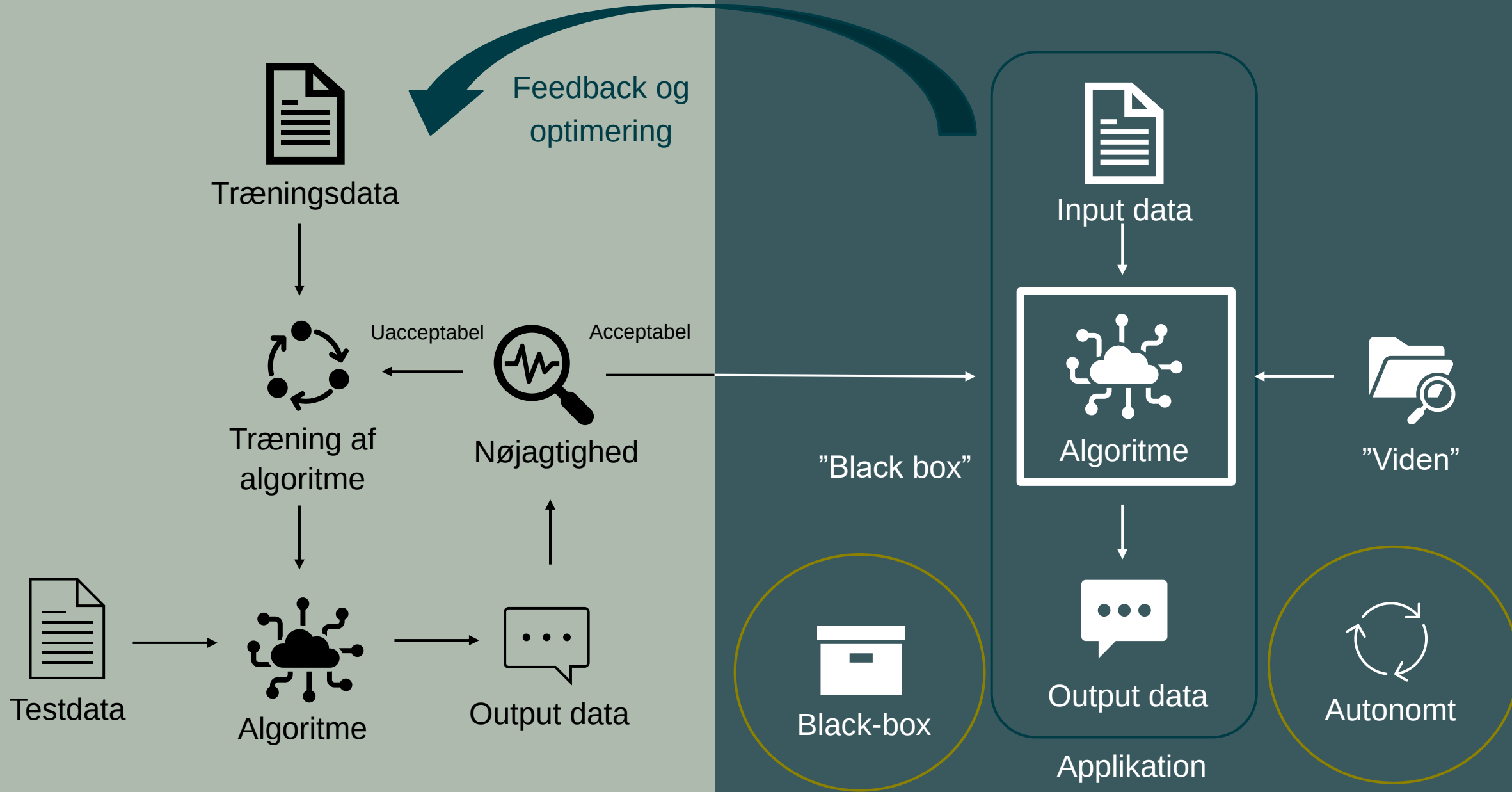
ChatGPT har genereret en falsk anklage, der beskylder en mand i U.S. for underslæb

Tesla Autopilot var ikke ansvarlig for biluheld

I hvad der angiveligt er den første sag om et uheld med delvist selvkørende biler, blev Tesla i April 2023 frifundet i en retssag i Californien.

Træning af modellen

Brug af modellen



A wave of digital regulation from EU is underway

Artificial Intelligence

- AI New Product Liability Act
- Directive
- AI Liability Directive

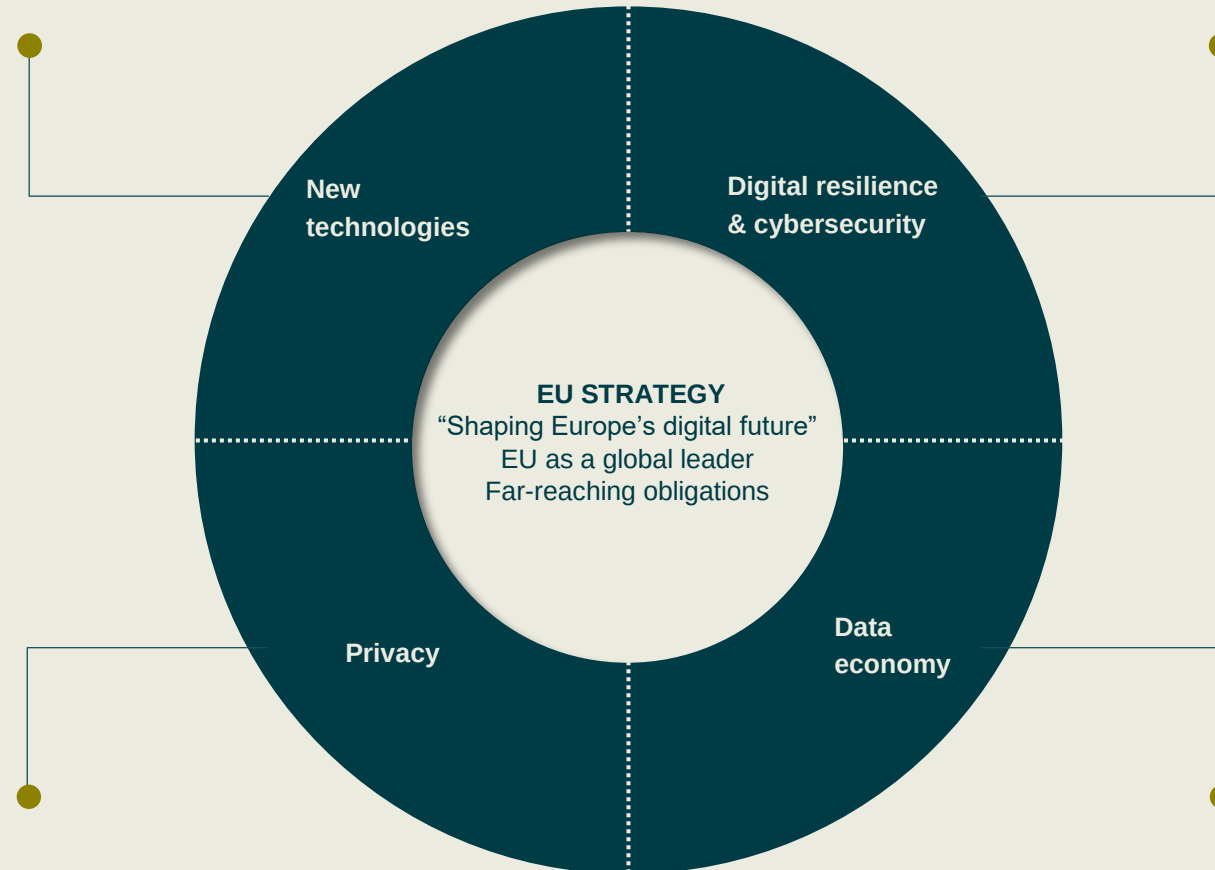
Crypto-assets

- Market in Crypto-Assets Regulation

Infrastructure

- European Chips Act
- 5G/6G

- ePrivacy Regulation
- GDPR



Organisational level

- NIS2
- DORA
- Resilience of Critical Entities

IoT products

- Cyber Resilience Act

Platforms

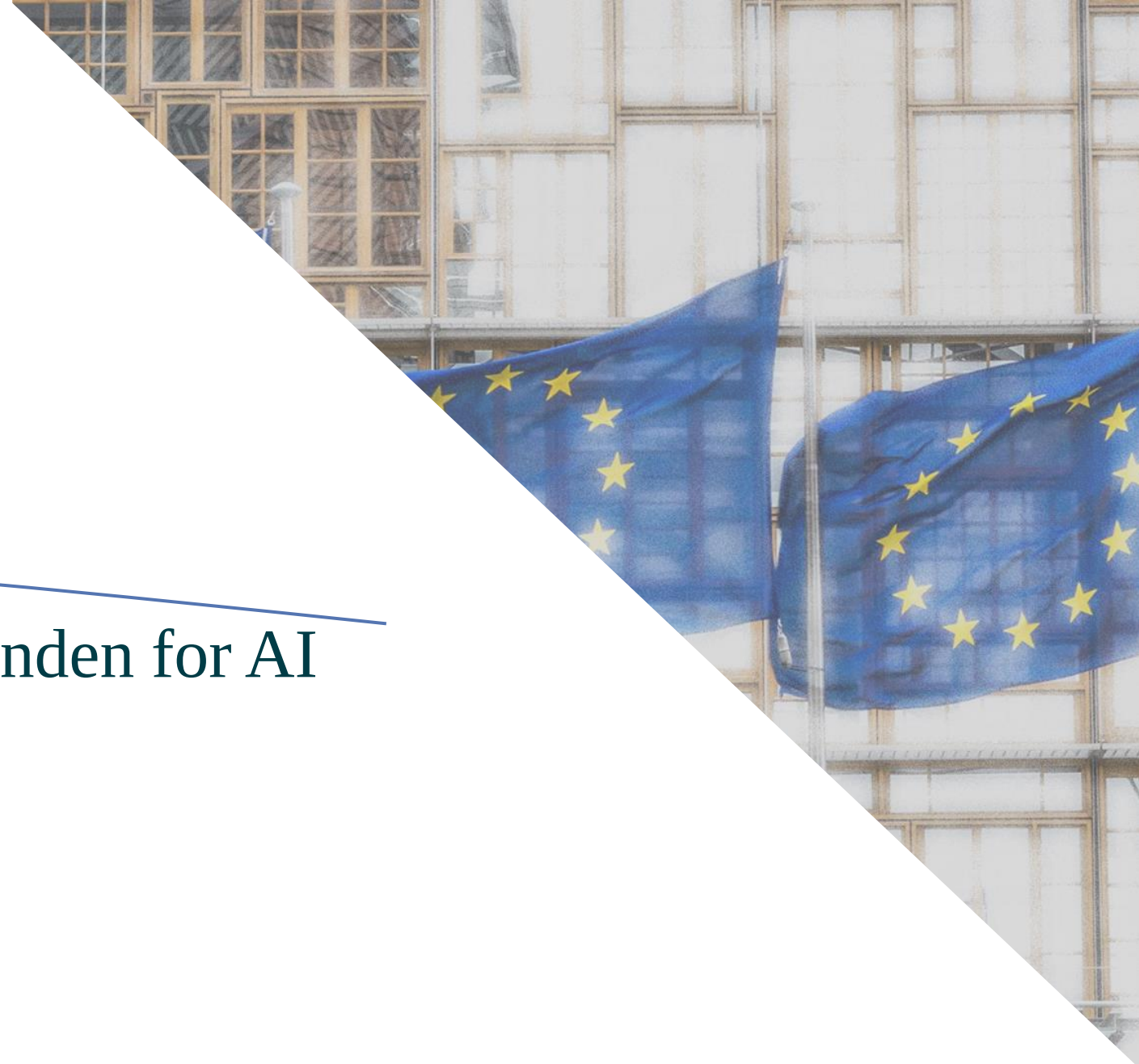
- Digital Services Act
- Digital Markets Act

Open data

- Data Governance Act
- Sector data spaces
- Data Act

”Excellence and trust”

EU vil være global leder inden for AI



AI-forordningen

”General approach”

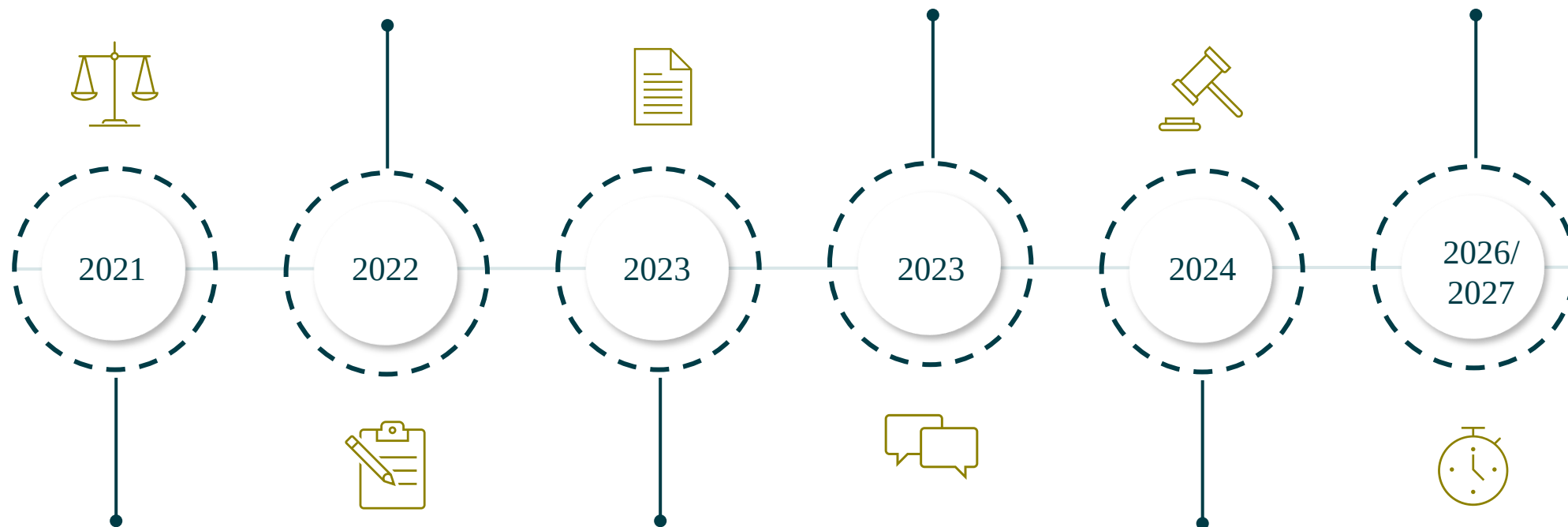
d. 6. december 2022 publicerede Rådet for Den Europæiske Union deres 'general approach' over for forordningen.

Trilogforhandlingerne

Indledning af Trilogforhandlingerne – går efter at blive færdiggjort til december 2023.

Anvendelse

Forordningen vil finde anvendelse 2-3 år efter vedtagelsen



Forslag til første regelsæt

I april 2021 foreslog Europa-Kommissionen det første EU-regelsæt for AI

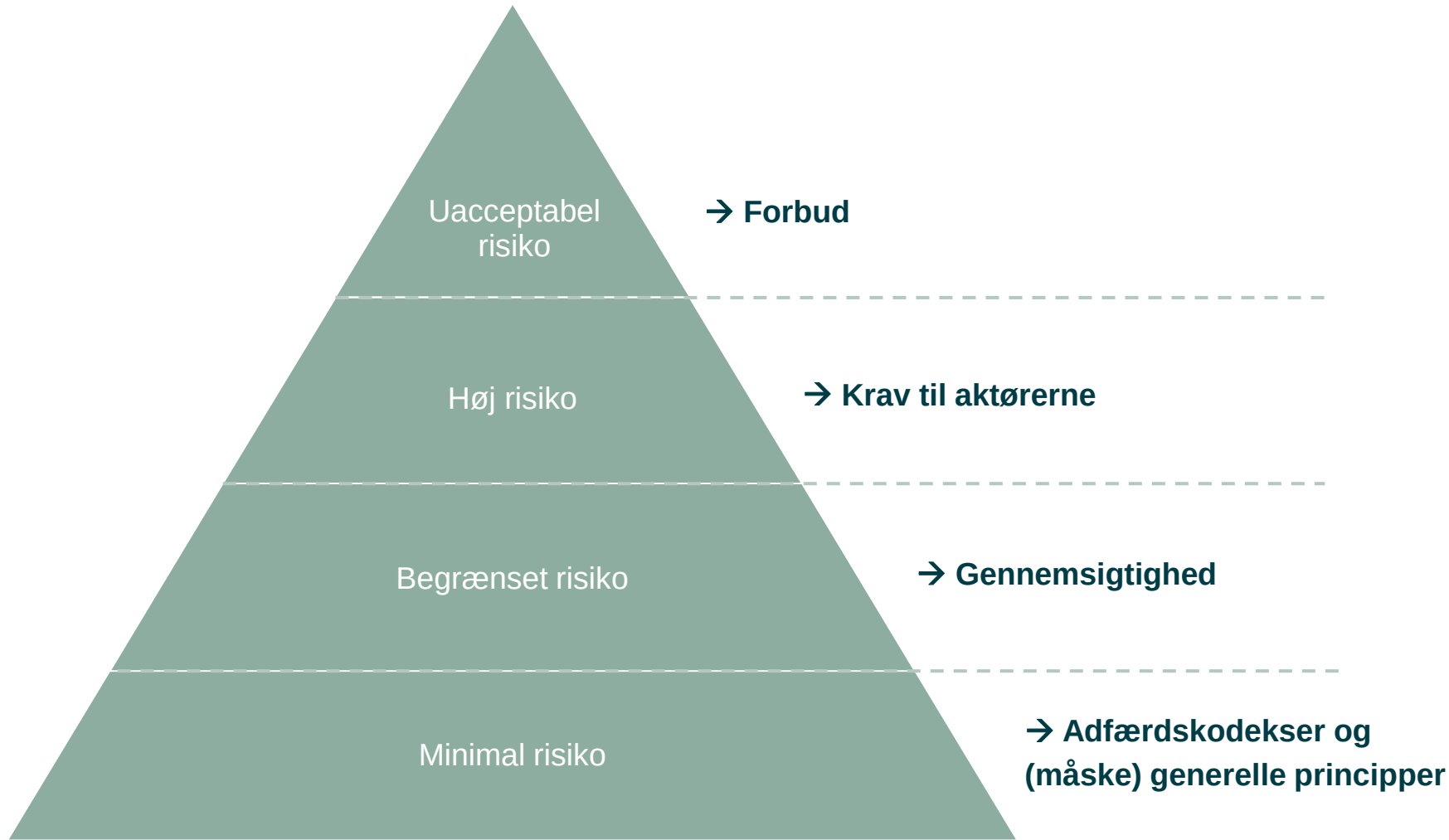
Parlamentet

Parlamentet vedtog sin holdning i 14. juni 2023

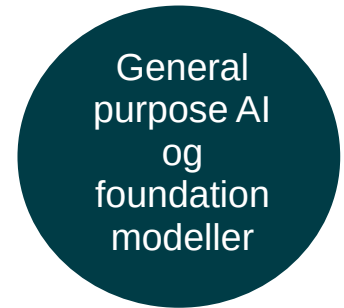
Vedtagelse

Forordningen forventes at blive vedtaget i starten af 2024.

AI-forordningen er baseret på en ”risikobaseret tilgang”



Og så kom ChatGPT...



- Specifikke krav
- Gennemsigtighed
- Summary af beskyttet træningsdata

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

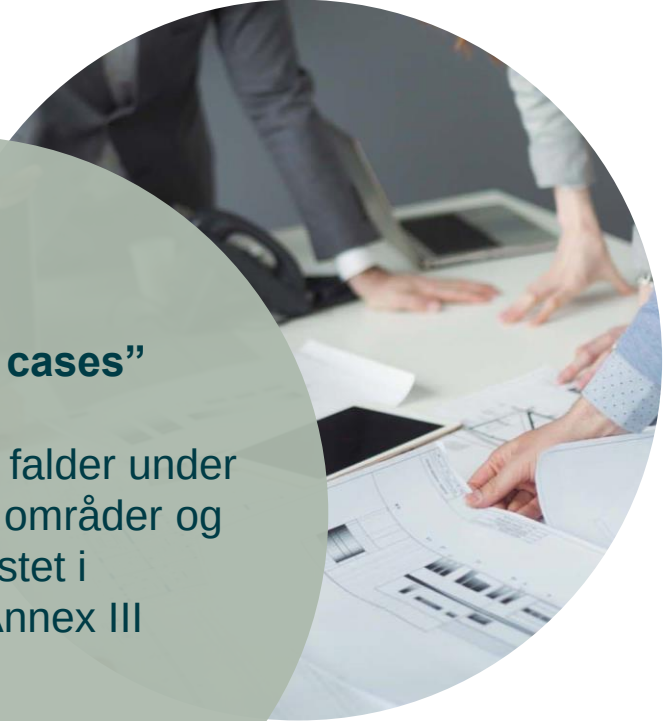
Medmindre det er strengt nødvendigt til de formål, der er oplistet i forordningen.

Hvad er “højrisiko” AI under AI-forordningen?



“Farlige produkter”

Visse produkter omfattet af EU's produktsikkerhedslovgivning, fx køretøjer, medicinsk udstyr og legetøj.



“Højrisiko use cases”

Brug af AI, som falder under et af de kritiske områder og uses cases oplistet i forordningens Annex III

Højrisko use cases i forordningens Annex III

Pkt. 1 fjernes og
indsættes i stedet
om kreditvurderinger

1. **Biometric and biometrics-based systems**
2. Management and operation of critical infrastructure
3. Education and vocational training
4. **Employment, workers management and access to self-employment**
5. Access to and enjoyment of essential private services and public services and benefits
6. Law enforcement
7. Migration, asylum and border control management
8. Administration of justice and democratic processes

(a a) AI systems intended to be used to make inferences about personal characteristics of natural persons on the basis of biometric or biometrics-based data, including emotion recognition systems, with the exception of those mentioned in Article 5;

- (a) AI systems intended to be used for recruitment or selection of natural persons, notably for placing targeted job advertisements, screening or filtering applications, evaluating candidates in the course of interviews or tests;
- (b) AI systems intended to be used to make or materially influence decisions affecting the initiation, promotion and termination of work-related contractual relationships, task allocation based on individual behaviour or personal traits or characteristics, or for monitoring and evaluating performance and behavior of persons in such relationships.

Krav til ”højrisiko” AI-systemer

- Risikostyringssystem
- Datakvalitet og datastyring
- Teknisk dokumentation
- Registrering og logging
- Gennemsigtighed og information
- Menneskeligt tilsyn
- Nøjagtighed, robusthed og cybersikkerhed

(61) Standardisation should play a key role to provide technical solutions to providers to ensure compliance with this Regulation. Compliance with harmonised standards as defined in Regulation (EU) No 1025/2012 of the European Parliament and of the Council¹ should be a means for providers to demonstrate conformity with the requirements of this Regulation. *To ensure the effectiveness of standards as policy tool*



AI-forordningen regulerer hele værdikæden

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



‘provider’ means a natural or legal person, public authority, agency or other body that develops an AI system or that has an AI system developed with a view to placing it on the market or putting it into service under its own name or trademark, whether for payment or free of charge;

Providers skal bl.a.

- › Sikre at systemet opfylder kravene til højrisiko-systemer
- › Oplyse om risikoen for bias
- › Udarbejde specifikationer for input data
- › Implementere et kvalitetsledelsessystem
- › Opbevare logs
- › Foretage/sikre overensstemmelsesvurdering af systemet
- › CE-mærke systemet
- › Registrere systemet i EU database
- › Foretage evt. korrigerende foranstaltninger
- › Samarbejde med myndighederne

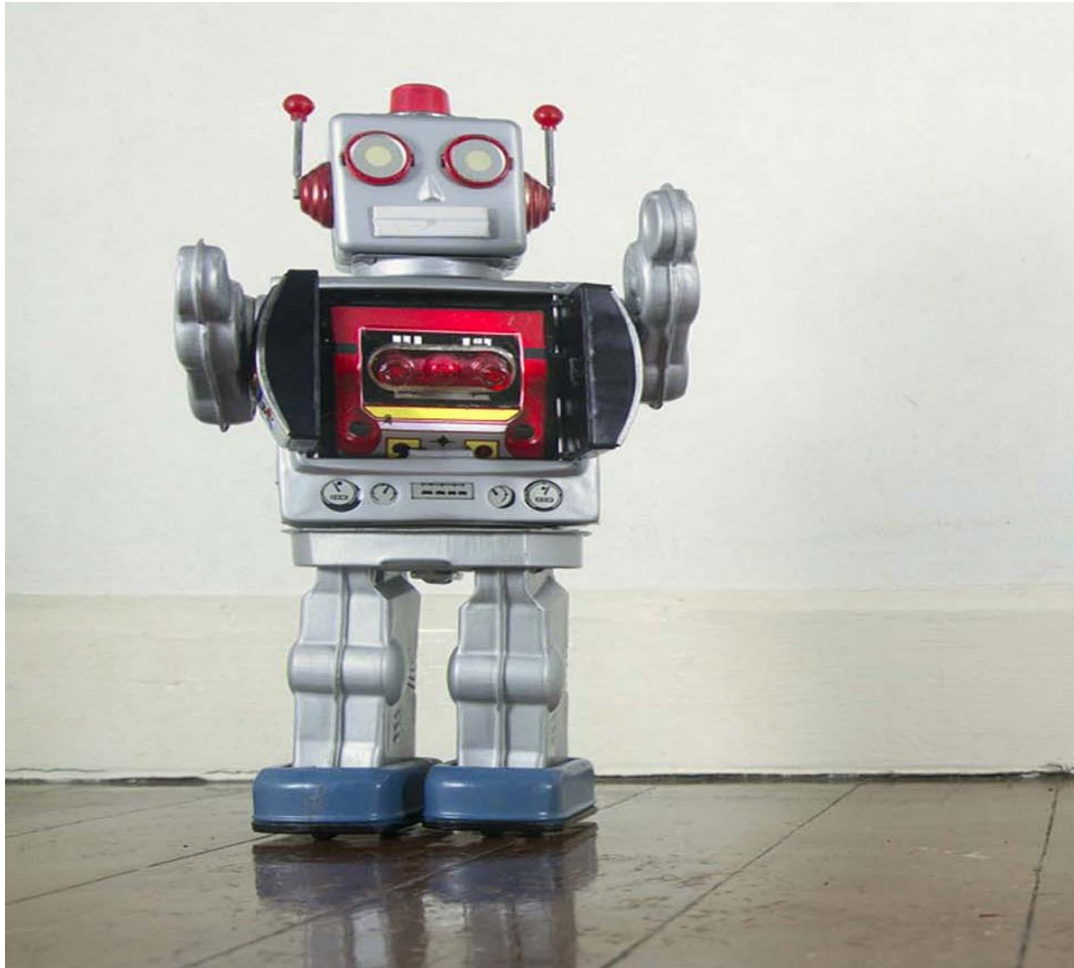


‘deployer’ means any natural or legal person, public authority, agency or other body using an AI system under its authority, except where the AI system is used in the course of a personal non-professional activity;

Deployers skal bl.a.

- › Anvende systemet som tiltænkt
- › Implementere menneskeligt tilsyn (med fornødne ressourcer og kompetencer)
- › Overvåge og opdatere sikkerhedsforanstaltninger
- › Anvende relevante og repræsentative inputdata
- › Overvåge systemet og informere om opståede risici
- › Opbevare logs (hvis under deployers kontrol)
- › Benytte informationerne om systemet til udarbejdelse af DPIA under GDPR
- › Hvis systemet benyttes til at træffe beslutninger om fysiske personer, oplyse om dette
- › Samarbejde med myndighederne
- › Udarbejde ”fundamental rights impact assessment” (FRIA)

Gennemsigtighed (begrænset risiko)



Der gælder også krav til AI-systemer, som indebærer særlige risici for imitation eller vildledning. Kravene er dog væsentligt mindre.

1. Systemer, der interagerer med mennesker

- Brugere skal oplyses om, at de interagerer med et AI-system.

2. Følelsesgenkendelse og biometrisk kategorisering

- De påvirkede skal oplyses om, at de er eksponeret for et sådan system.

3. "Deep fakes"

- Det skal oplyses, at indholdet er blevet genereret kunstigt eller manipuleret

Andre AI-systemer (minimal risiko)

Andre AI systemer bliver underlagt frivillige adfærdskodekser og (måske) også en række obligatoriske principper og krav om "AI literacy"

Article 4 a - General principles applicable to all AI systems

(fra Parlamentets forslag)

*"**All operators** falling under this Regulation shall make their **best efforts** to develop and use AI systems or foundation models in accordance with the following **general principles** ...*

*a) '**human agency and oversight**' means that AI systems shall be developed and used as a tool that serves people, respects human dignity and personal autonomy, and that is functioning in a way that can be appropriately controlled and overseen by humans;*

*b) '**technical robustness and safety**' means that AI systems shall be developed and used in a way to minimize unintended and unexpected harm as well as being robust in case of unintended problems and being resilient against attempts to alter the use or performance of the AI system so as to allow unlawful use by malicious third parties;*

*c) '**privacy and data governance**' means that AI systems shall be developed and used in compliance with existing privacy and data protection rules, while processing data that meets high standards in terms of quality and integrity;*

*d) '**transparency**' means that AI systems shall be developed and used in a way that allows appropriate traceability and explainability, while making humans aware that they communicate or interact with an AI system as well as duly informing users of the capabilities and limitations of that AI system and affected persons about their rights;*

*e) '**diversity, non-discrimination and fairness**' means that AI systems shall be developed and used in a way that includes diverse actors and promotes equal access, gender equality and cultural diversity, while avoiding discriminatory impacts and unfair biases that are prohibited by Union or national law;*

*f) '**social and environmental well-being**' means that AI systems shall be developed and used in a sustainable and environmentally friendly manner as well as in a way to benefit all human beings, while monitoring and assessing the longterm impacts on the individual, society and democracy."*



Article 4 b - AI literacy

(fra Parlamentets forslag)

*"Providers and deployers of AI systems shall take measures to ensure a **sufficient level of AI literacy of their staff and other persons** dealing with the operation and use of AI systems on their behalf ... "*



Sanktioner

30 000 000 EUR el. 6 % af
virksomhedens globale
årsomsætning

Ved overtrædelse af art. 5 og 10

20 000 000 EUR el. 4 % af
virksomhedens globale
årsomsætning

Ved overtrædelse af andre artikler

Opsamling på AI-forordningen

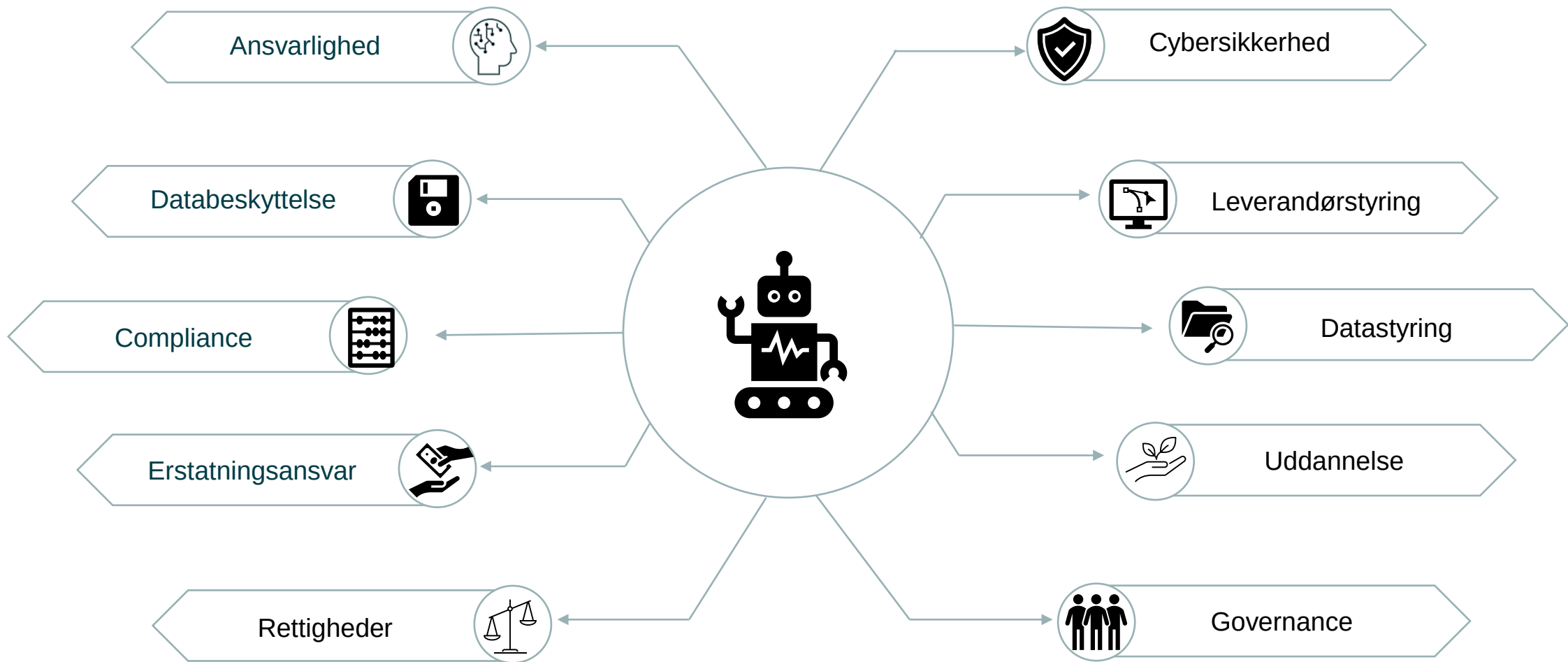
– spørgsmål og organisatoriske tiltag, som er relevante allerede i dag

Spørgsmål	Forbudt praksisser	Højrisiko kategorier	Rolle i værdikæden	Gennemsigtighedskrav
	Anvender vi AI, som kan blive omfattet af de forbudte praksisser?	Udvikler eller anvender vi højrisiko AI, eller vil vi gerne gøre det?	Kommer vi til at være provider og/eller deployer under forordningen?	Udvikler eller anvender vi AI, som kan blive underlagt krav om gennemsigtighed?
Organisatoriske tiltag	Klæd forretningen på		Sæt holdet	Hold jer opdateret
	Selvom der vil gå år, før forordningen finder anvendelse, er det nødvendigt, at ledelsen og forretningen er klar over, hvad der kommer		Forberedelse til AI-forordningen kræver forskellige kompetencer, herunder tekniske, juridiske og kommercielle samt projektstyring	Følg de afsluttende forhandlinger om forordningen samt den løbende udvikling af tekniske standarder såvel som udarbejdelsen af evt. (branchespecifikke) retningslinjer og best practices
	Start arbejdet med ansvarlig AI		Overvej behovet for en AI-politik	
	Det kan have stor værdi at begynde at arbejde med de principper for ansvarlig AI, som forordningen lægger op til, allerede nu, fx risikostyring, forklarlighed og håndtering af bias mv.		Store virksomheder er forpligtet til at rapportere om dataetik, herunder ved anvendelse af AI, og flere og flere udarbejder politikker for ansvarlig AI	

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

10 væsentligste områder



1. Ansvarlighed



Fair



Miljø



Inklusion

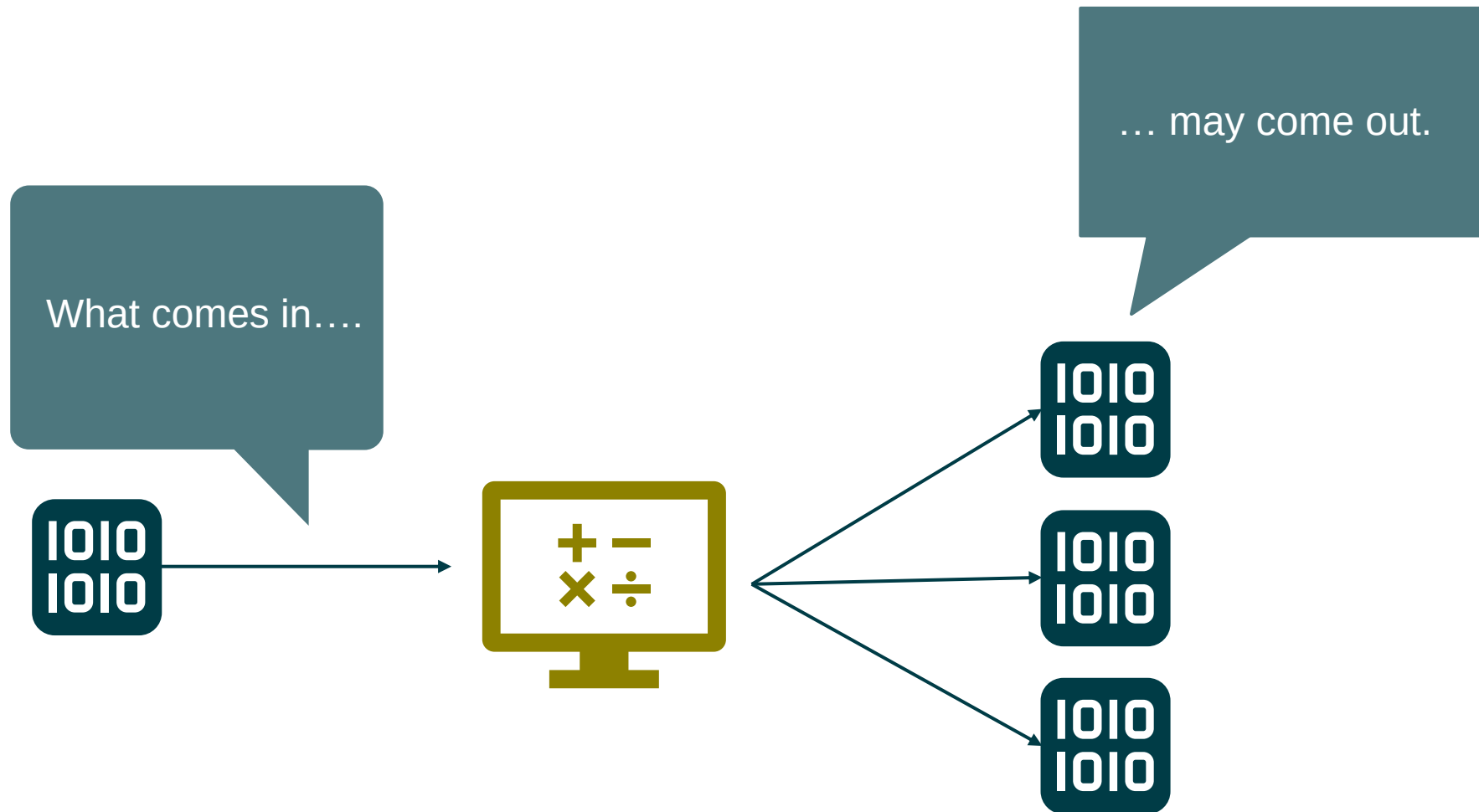


Gennemsigtighed



Ansvar

2. Databeskyttelse og fortrollighed



Fortrolighed

Indtastning af oplysninger i åbne AI-tjenester svarer stort set til offentliggørelse, hvilket udgør en risiko for virksomhedens fortrolige oplysninger og forretningshemmeligheder mv.

OpenAI terms of use

Our Use of Content. We may use Content to provide, maintain, develop, and improve our Services, comply with applicable law, enforce our terms and policies, and keep our Services safe.

Opt Out. If you do not want us to use your Content to train our models, you can opt out by following the instructions in [this Help Center article](#). Please note that in some cases this may limit the ability of our Services to better address your specific use case.

Rights You give to Midjourney

By using the Services, You grant to Midjourney, its successors, and assigns a perpetual, worldwide, non-exclusive, sublicensable no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute text, and image prompts You input into the Services, or Assets produced by the service at Your direction. This license survives termination of this Agreement by any party, for any reason.

Please note: Midjourney is an open community which allows others to use and remix Your images and prompts whenever they are posted in a public setting. By default, Your images are publically viewable and remixable. As described above, You grant Midjourney a license to allow this. If You purchase a "Pro" or "Mega" plan, You may bypass some of these public sharing defaults.

Hvad skal vi gøre?

- Overvej behovet for tekniske foranstaltninger
- Udarbejd retningslinjer for medarbejdernes brug af AI-tjenester
- Uddan medarbejderne og skab awareness omkring risici



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



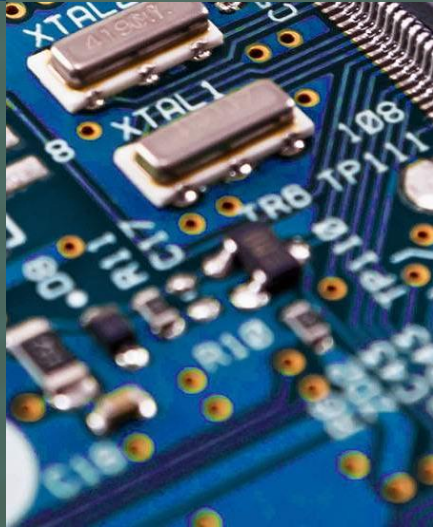
Dataansvar, risikovurdering, databehandler-aftaler, tilsyn med databehandlere.



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.

GDPR og AI

- Persondatareglerne gælder også for AI - det er også fastslået i AI-forordningen
- Visse processer er koordineret - fx i relation til DPIA og den nye "FRIA"
- Men grundlæggende gælder GDPR uændret ved siden af AI-forordningen



GRUNDLÆGGENDE PRINCIPPER

- Datakvalitet – bias i data og er modellen tilstrækkeligt trænet?
- Dataminimering – mulighed for at anvende syntetiske data?
- Den dataansvarlige skal kunne dokumentere overholdelse

BEHANDLINGSGRUNDLAG

- Hvad er rækkevidden af offentlige myndigheders lovhjemmel?
- Samtykke til AI-behandling?
- AI-behandling baseret på en interesseafvejning?

DEN REGISTREREDES RETTIGHEDER

- Der skal gives oplysning om formål relateret til AI
- Teknisk muligt at sikre retten til at blive glemt?
- Forbuddet mod automatiske individuelle afgørelser – sikre mulighed for menneskelig ingriben

GENERELLE FORPLIGTELSE

- Risikovurderinger skal opdateres eller udarbejdes i lyset af AI
- Databeskyttelse gennem design og standardindstillinger
- Databehandlertaaler skal opdateres eller udarbejdes på ny
- Konsekvensanalyser er formentlig altid et krav ved AI

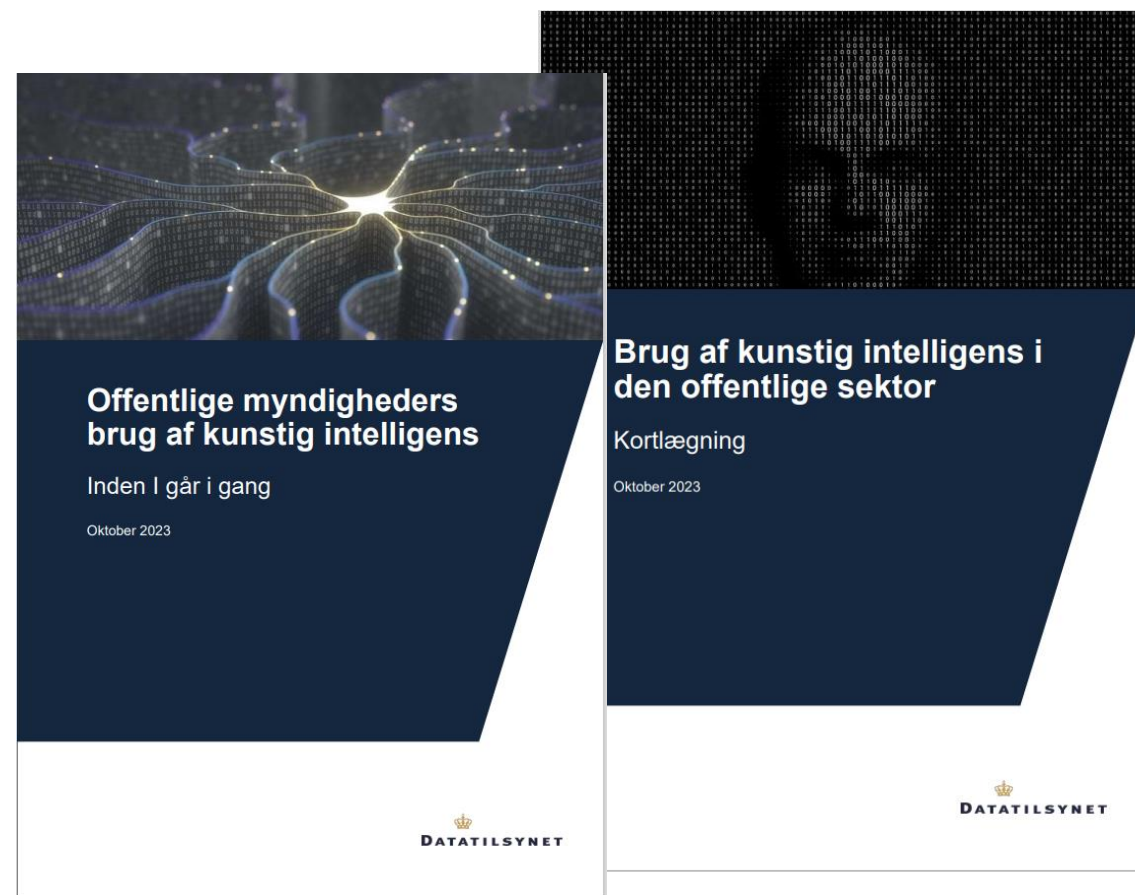


Datatilsynet: Vejledning om offentlige myndigheders brug af kunstig intelligens, oktober 2023

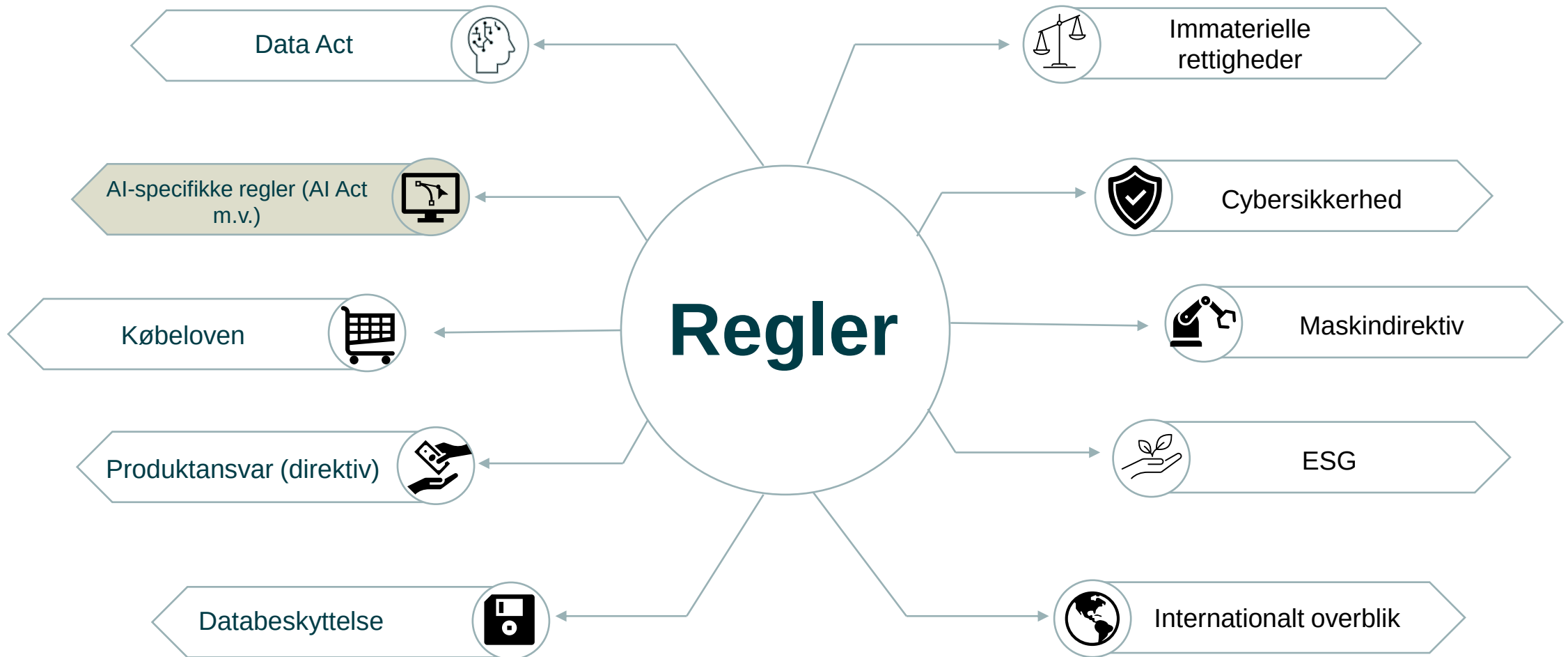
- Opmærksomhedspunkter og krav efter GDPR ved brug af AI
 - Behandlingsgrundlag
 - Konsekvensanalyse
 - Databeskyttelse gennem design og standardindstillinger
 - Automatiske afgørelser og profilering (automation bias)

➔ *Databeskyttelsesreglerne skal overholdes, uanset om behandlingen sker ved brug af AI eller et traditionelt it-system*

- Spørgeskemaundersøgelse af 191 offentlige myndigheder
 - Hvor udbredt er brugen af kunstig intelligens?
 - Hvilke juridiske overvejelser har myndighederne gjort sig?



3. Compliance



4. Erstatning

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, f.eks. forbindelse til andre produkter eller netværk, "self-learning" elementer, og krav til digitale produkter, f.eks. 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.

5. Immaterielle rettigheder



Rettigheder til input og output

Tvivlsomt i hvilket omfang outputtet kan beskyttes som en IP rettighed.

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

Hvad med beskyttelse af selve AI-systemet?



Risiko for krænkelse

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

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



Træningsdata

Adgang til at træne på baggrund af data?

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

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

Gode råd til beskyttelse af AI-generet output

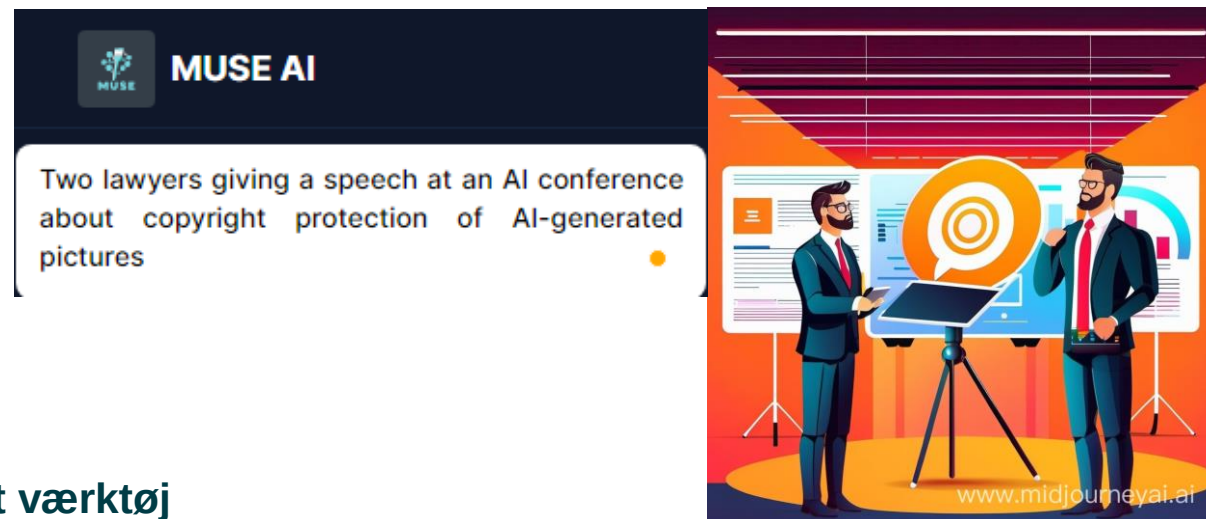


AI-teknologien anvendes som et værktøj

- Der bør foretages **konkrete, specifikke** og **kreative** valg ved valg af input (prompts).
- Ved billeder (Midjourney mv.) kan dette f.eks. være vedrørende udformningen, belysningen, billedudsnittet, vinklen eller stemningen.

AI-værket bearbejdes manuelt

- Hvis et værk genereret ved brug af AI-teknologi efterfølgende bearbejdes manuelt, kan ændringerne i sig selv være ophavsretligt beskyttet, hvis de selv er originale.
- De dele af værket, der *alene* er AI-genererede, vil derimod ikke være beskyttet.



Hvordan undgår man krænkelse ved at anvende AI-genereret indhold?



DU har ansvaret!

-

Du har som bruger af AI, ansvaret for den kommercielle brug af det generede værk – dvs. ansvar for, at resultatet ikke krænker andres rettigheder.



Kan tjenesten have ansvaret?

-

AI-tjenesten har ikke nødvendigvis ansvaret, hvis du benytter AI-genererede værker ulovligt.

6. Cybersikkerhed



Procedurer og politikker



Risikovurdering



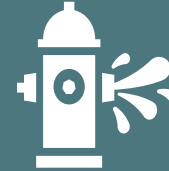
Sikkerhedsforanstaltninger



Overvågning



Data poisoning



Data leaks



Spear fishing



Adversarial attacks



Model theft



Surveillance



7. Leverandørstyring

Tænk fremad

- Data er og bliver en væsentlig "vare" – ikke kun som egen viden, men også til træning af AI
- Maskinen lærer af data – så den bliver ikke klogere end det
- **Valide data** er væsentlig kilde til at skabe "kloge" AI-systemer
- Tænk data og adgang til data ind som væsentligt aktiv i virksomhedens kontrakter
 - Egen adgang til data
 - Modparts adgang til data
 - Kvalitet og rettigheder



10. Governance



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

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.

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?



Kromann Reumert's take

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 og 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 bør aldrig erstatte brugerens egen evne til 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 rettighedsmæssige begrænsninger, når du sender og modtager indhold.
8. Undlad eller anonymisér personoplysninger.

”Det var sjovt! ... Vil du vide mere?”



Podcast

- › Ep. 4: Kunstig intelligens: en verden af muligheder og et hav af juridiske spørgsmål.
- › Findes på vores hjemmeside:
www.kromannreumert.com/viden/podcast/startup-venture-podcastserie-om-jura-startups-saeson-2



Guides og artikler

- Start-up guide | Data Privacy
- IP-retlige udfordring ved kunstig intelligens
- 10 råd til dit arbejde med ChatGPT og anden generativ AI
- ChatGPT, BING og BARD: Er din virksomhed klar til den generative AI?
- Findes på vores hjemmeside: www.kromannreumert.com/viden

Tak for i dag



Kristian Storgaard
Partner

Dir. +45 38 77 44 70
Mob. +45 20 19 74 10
kst@kromannreumert.com



Emil Hjelmsmark Orlamundt
Associate, Advokat

Dir. +45 38 77 11 73
Mob. +45 21 34 70 12
emop@kromannreumert.com

