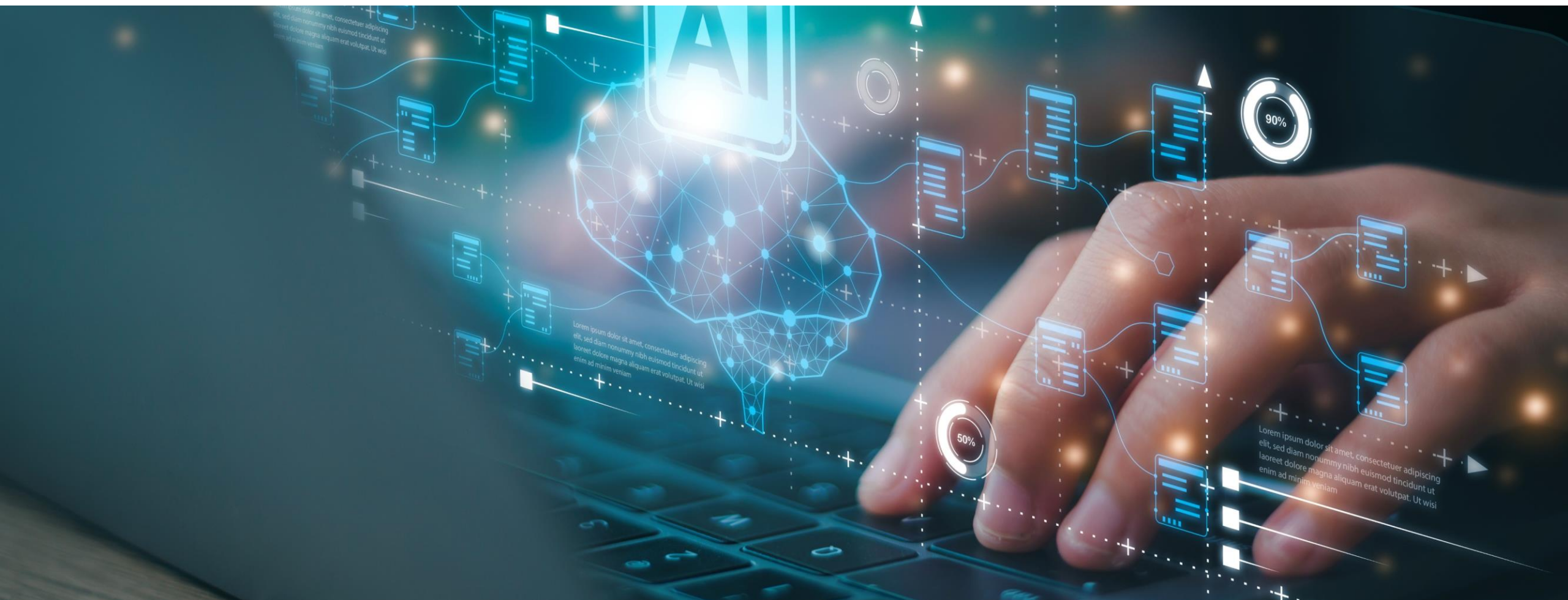


JURIDISK FORENING

Praktisk anvendelse af kunstig intelligens i juridiske arbejdsfunktioner



PROGRAM (FØR PAUSE)

16.00 – 16.30: Ankomst og netværk

16.30 – 16.45: Hvordan kan generelle AI-robotter fungere som juridisk hjælpeværkøjer?
v/ dr.jur. Mads Bryde Andersen

16.45 – 17.00: Karnov AI Legal Assistant (KAILA)
v/ Michael Herbing, Head of Literature, Karnov Group

17.00 – 17.15: AI-assistenten fra Djøfs Forlag
v/ udviklingschef Jens-Christian Jensen, Djøf Forlag

17.15 – 17.30: Hvordan bruges AI i offentlig virksomhed Danmark?
v/ Postdoctoral Researcher Aysel Eybil Kucuksu, iCourts, University of Copenhagen

17.30-17:45: Pause m. let mad og drikke



PROGRAM (EFTER PAUSE)

17.30 – 17:45: Pause m. let mad og drikke

17.45 – 18:00: Hvilke retlige begrænsninger vil AI-forordningen lægge for brugen af AI i privat og offentlig virksomhed? *v/ professor, dr.jur. Henrik Udsen*

18.00 – 18:20: Hvilke spørgsmål rejser AI-brug efter persondataretlige regler?
v/cand.jur. og sikkerhedsrådgiver Allan Frank, Datatilsynet

18.20 – 18:40: Procesretlige og etiske overvejelser ved dommeres brug af AI
v/ landsdommer Mette Lyster Knudsen, Østre Landsret

18.40 – 19.00: Etiske og sikkerhedsmæssige spørgsmål ved brug af AI i advokatvirksomhed
v/ områdedirektør for Forretningsudvikling & IT Louise Krarup, Poul Schmith/Kammeradvokaten

19.00: Tak for i dag



Hvordan kan generelle AI-robotter fungere som juridiske hjælpeværktøjer?

Juridisk Forening

mandag den 28. oktober 2024

Professor, dr.jur. Mads Bryde Andersen

mads@jur.ku.dk

KØBENHAVNS UNIVERSITET



Baggrunden for det følgende

- Lægmandsbrug af
 - ChatGPT (gratis)
 - ChatGPT Plus (betalbar, 20 USD/md.)
 - Chat and Ask AI (betalbar, 60 USD/årligt)
 - Microsoft Copilot Enterprise (via Københavns Universitets licens)
 - DeepL (betalbar – månedlig afgift afhængigt af antal oversættelser)
- Ikke yderligere “forbrugervejledning” (tidsrammer)
- Kun eksempler på anvendelighed

Generelle iagttagelser

- *Generel advarsel:* Systemerne er fyldt med forkerte oplysninger, bortforklaringer og dårlige undskyldninger ("meget menneskelige")
- Der er en grund til, at det hedder "chat". Bliv ved med at præcisere
- Tal gerne engelsk, hvis informationssøgningen forudsættes at benytte engelske kilder
- Tro ikke på dårlige undskyldninger
- Forsøg flere applikationer
- Regn ikke med noget (herunder privatlivsgarantier)

Bemærk logo-forvirring

- Chat GPT's logo



- Chat and Ask AI's logo



Følgende aftestninger foretaget (med karakter på 5-skala)

- Redegørelser for gældende ret (2/5 – afhængigt af dokumentgrundlag)
- Hjælp til aftalekoncipering (4)
- Hjælp til tekstanalyse (5)
- Hjælp til identifikation af argumenter (5)
- Hjælp til afprøvning af argumenter (4)
- Hjælp til oversættelser (5 – navnlig DeepL)

Redegørelser for gældende ret

- **Spørgsmål:** Kan Danmark udtræde af den europæiske menneskerettighedskonvention uden at krænke sine forpligtelser i medfør af EU-traktaterne?
- **Spørgsmål:** En politiker blev for 20 år siden dømt for et udsagn, som dengang blev dømt som racistisk. Nu har han gentaget udsagnet, fordi det i dag - efter politikerens opfattelse – er legitimt at fremføre sådanne synspunkter. Skal politikerens straffes igen?

Generel hjælp til argumentation

- **Spørgsmål:** Hvilke argumenter taler generelt for og imod legalisering af aktiv dødshjælp?

Hjælp til aftalekoncipering

- **Skriv en licensaftale**, hvorved indehaveren af et patent på en kemisk substans giver en produktionsvirksomhed ret til at benytte patentet i sin produktion. Hvis der skal tages stilling til principielle spørgsmål, før du kan skrive en sådan aftale, så afklar dem gerne forinden?
- Nærmere detaljer: 1: Ikke-eksklusiv licens. 2: begrænset til Danmark. 3: Samme varighed som patenttiden 4: Royalty 5: Kun til brug ved fremstilling af produktet "x". 6. Ingen kvalitetskontrol. 7: Ingen ret til overdragelse af licensen
- Er der risiko for, at din tekst krænker ophavsretten til en eksisterende licensaftale?

Tekstanalyse af bøger, fx Lærebog i Obligationsret I

- **Spørgsmål:** *Mener forfatteren til denne bog, at der består et såkaldt "kontrolansvar" i dansk obligationsret - og hvad går dette ansvar i givet fald ud på?*
- **Svar:** I den pågældende bog diskuterer forfatteren det såkaldte "kontrolansvar" i relation til både dansk og international obligationsret. Forfatteren forklarer, at dette ansvar udløses af misligholdelsen selv, uanset om debitor har haft kontrol over årsagen til misligholdelsen. Debitor kan dog fritages for ansvar, hvis vedkommende kan bevise, at den upåregnelige og uovervindelige begivenhed, som forårsager tabet, lå uden for hans kontrol. Dette ansvar anvendes eksempelvis i internationale købsretlige relationer (CISG) og er gradvist ved at påvirke dansk indenlandsk obligationsret **【8:0†source】**. Kontrolansvaret differentierer sig fra culpereglen, idet det i nogle situationer tillader fritagelse fra ansvar, hvis debitor beviser, at begivenheden lå uden for deres kontrol. Eksempler på dette er hovedleverandørens ansvar for underleverandørens mangler, som ofte betragtes som værende inden for hovedleverandørens kontrol **【8:1†source】**.

Og videre (i samme bog)

- **Spørgsmål:** *Mener forfatteren til bogen, at der findes en grundsætning om "force majeure" i dansk ret?*
- **Svar:** Forfatteren til bogen nævner, at det er tvivlsomt, om der kan udledes en generel obligationsretlig grundsætning om force majeure i dansk ret. Der er dog anerkendelse af, at force majeure kan fritage en debitor fra ansvar i tilfælde, hvor misligholdelsen skyldes uforudsete og uovervindelige begivenheder uden for debitorens kontrol. Desuden diskuterer bogen, hvordan retsvirkningerne af force majeure afhænger af den konkrete aftale eller lovgivningen, såsom Købelovens § 24 (KBL § 24), der fritager debitor for erstatningspligt ved force majeure i købsforhold **【8:2+source】** **【8:5+source】** .

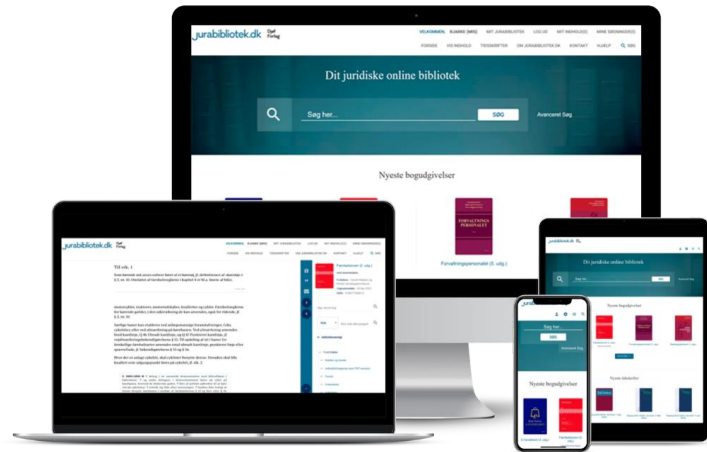
Praksissøgning i lovkommentarer

- **Spørgsmål:** På grundlag af den vedhæftede, kommenterede, udgave af retsplejeloven ønsker jeg at kende **betingelserne for udpegning af sagkyndige dommere til Sø- og Handelsretten**. Derudover ønsker jeg at vide, om der stilles andre krav til disse dommers inhabilitet (forstået som fravær af interessekonflikter), end der gør for andre dommere.
- **Spørgsmål:** findes der eksempler fra **retspraksis** (se navnlig noterne til loven), som belyser kravene til de sagkyndige dommers inhabilitet?
- **Spørgsmål:** Skriv gerne disse svar sammen i **et lille notat**, som jeg gerne vil modtage i Word.

Jurabibliotek i fremtiden

Hvad vil vi opnå?

- Synliggøre omkring 1.000 forfatteres indhold
- Slå to systemer sammen til et
- Forbedre søgning



En tanke:

- Skal man altid søge “opsigelsesvarsel funktionær” eller kunne man bare spørge i klart sprog “Hvad er opsigelsesvarslet for en funktionær”?
- Kunne vi bruge det der “GPT” til det?

RAG

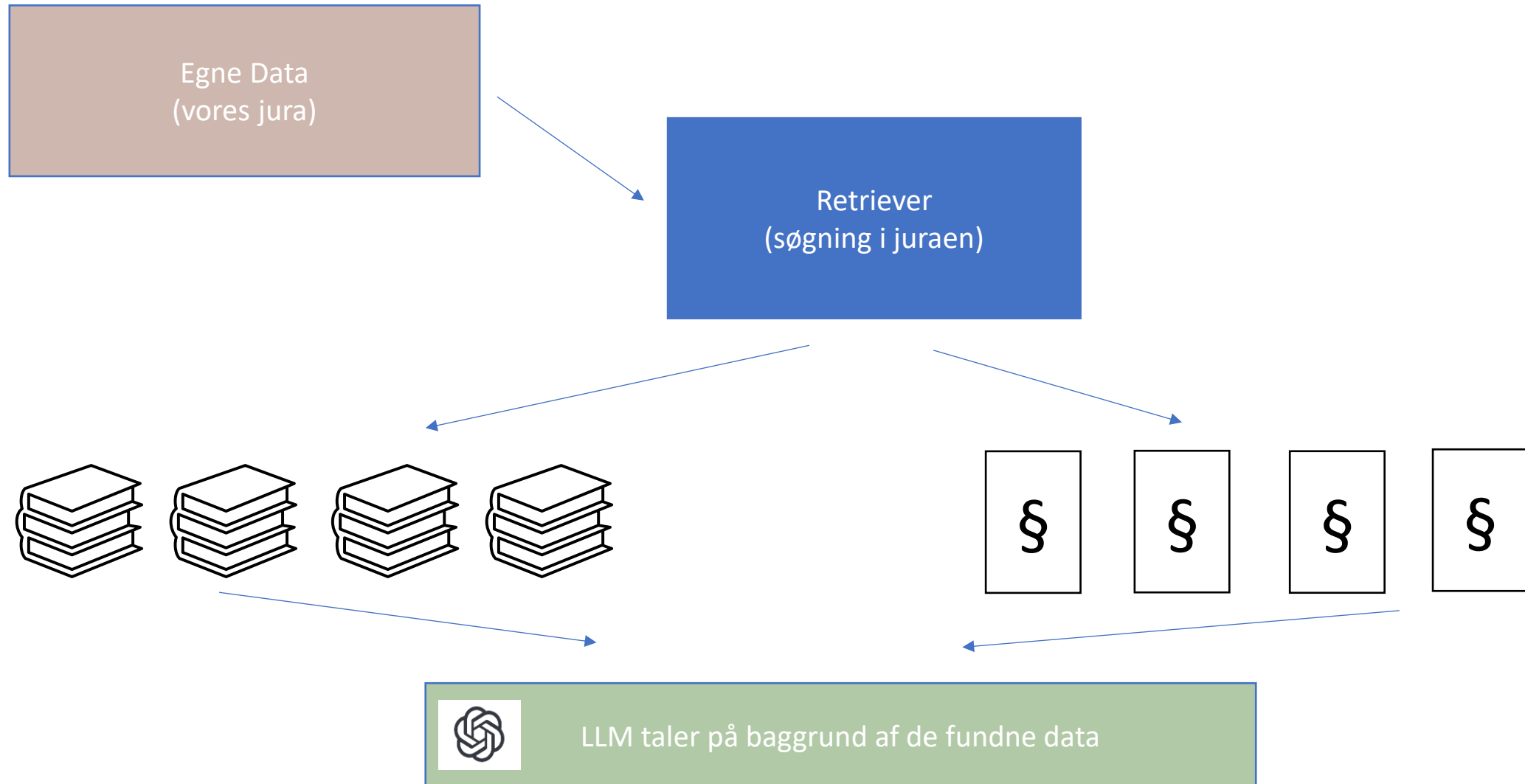
Retrieval-Augmented Generation

- **Retrieval:** Det at hente dokumenter (fra egen database) ...
- **Augmented:** ... til af forbedre
- **Generation:** ... genereringen (af tekst) ved brug af en LLM

De fleste AI-løsninger, der bygges i dag inden for *legal tech*, er en slags RAG

Idéen er, om man kan bruge AI'ens snakkeevner på et kurateret indhold

RAG fortsat



Hvilke data fodrer vi RAG'en med?

- **Jurabøger** *Kun seneste udgave*
- **Danske love** *Konsolideret*
- **Danske bekendtgørelser** *Konsolideret*

Hvilke data benytter vi endnu ikke?

- Artikler
- Forarbejder
- Afgørelser
- Vedledninger, cirkulærer, EU-retlig lovgivning og afgørelser

Hver slags har sine egne udfordringer

Hvad virker?

Hegnet ind	<i>Assistenten svarer kun på baggrund af kurateret indhold</i>
Opdateret*	<i>Indholdet holdes opdateret</i>
Kildeangivelse	<i>Vi tvinger assistenten til at angive kilder så man selv kan se efter om man er enig</i>

Hvorfor virker det?

Vores data er tabulerede

Alt indhold er parset ind i småbidder og ligger i en relationel database

Egne embeddings

Vi har lært modellen dansk juridisk sprog. Hvilke begreber er beslægtede

Prompt engineering

Vi har brugt en del tid på at få assistenten til at svare mere som en jurist

Eksempler på hvad der skal forbedres

Problem	Løsning
One shot <i>Jurister arbejder jo ikke sådan, at vi altid giver svaret på en gang</i>	Dialog <i>Det vil være godt, hvis den af og til stiller modspørgsmål for at kunne give et bedre svar</i>
For specifik <i>Den svarer af og til på specifikke undtagelser, hvor der er et mere generelt svar</i>	Generelle svar <i>Vi vil som udgangspunkt tvinge den til at finde det mest generelle svar, hvor der også er mere specifikke</i>
Selvsikker <i>Den er stadig lidt for selvfed</i>	Tvivi <i>Svar skal være lidt mindre skråsikre</i>
Ufuldstændige svar <i>Svarene er ikke altid fuldstændige</i>	Større context window <i>Vi giver den faktisk meget lidt at arbejde med. Vi kunne give den ca. 20 gange mere</i>
Flere kilder <i>Der er ofte svar i mange flere bøger men vi nævner få</i>	Større context window <i>Igen handler det om, at vi ikke retriever nok</i>
Checke egne svar <i>Den checker ikke sine egne svar</i>	Kontrol <i>Når modellerne bliver hurtigere, er der tid til, at vi kan fodre dem med deres egne svar og bede dem checke, om svaret underbygges i kilderne</i>

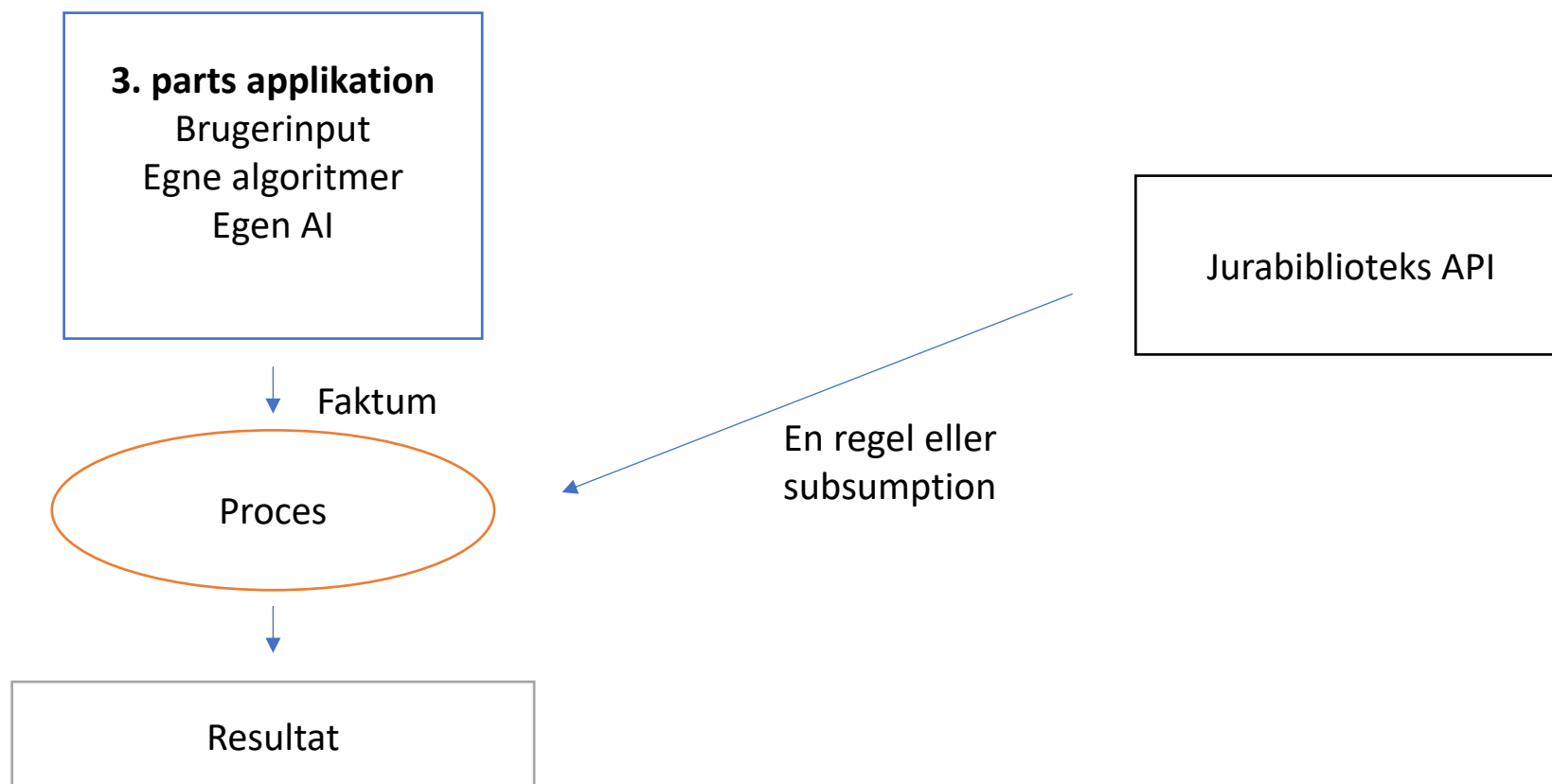
Andre anvendelser af AI i forlaget

- AI på flere retskilder
- AI i API (Application Programming Interface)
- Læringsmål før kapitler
- Opsummering af kapitler
- Testspørgsmål til kapitler
- Oplæsning af bøger
- Semantisk søgning
- Paradigmer
- Kontraktgennemgang

Noget er på test-stadiet, noget er slet ikke bygget

API

Jura til maskiner



KARNOV AI LEGAL ASSISTANT (KAILA)

*V/ MICHAEL HERBING, HEAD OF LITERATURE,
KARNOV GROUP*



Kunstig intelligens i offentlig virksomhed

Aysel Küçüksu, postdoc, ph.d.
Aysel.eybil.kucuksu@jur.ku.dk

Zuzanna Godzimirska, lektor, ph.d.

iCourts, Centre of Excellence for International
Courts and Governance
Det Juridiske Fakultet



[DATABASEN](#)
Søg efter projekter

[METODE](#)
Blæg om databasen

[VIDEN OG INSPIRATION](#)
Læs om AI og menneskerettigheder


ÅBENHED

KUNSTIG INTELLIGENS I DET OFFENTLIGE

Danmarks første database om brugen af kunstig intelligens i det offentlige.

[Søg i databasen](#)

Seneste projekter i databasen



ETIAS

ETIAS (European Travel Information and Authorisation System) er et EU-system, der kræver forhåndsgodkendelse for visumfritagne rejsende til Schengen området.

📅 Planlægges taget i brug 📅 2025

🌐 Udlændinge og asyl 🌐 EU

Profilering ▲▲▲▲



RefCase

RefCase et beslutningsstøttende værktøj til optimering af ansøgning- og sagsbehandlingsprocesserne omkring kropsbårne hjælpemidler efter servicelovens § 112.

📅 i brug 📅 2023

🌐 Sagsbehandling 🌐 Regionalt

▲▲▲▲



SIS

De nationale myndigheder som politiet og grænsevagterne kan indlæse og søge i indberetninger om eftersøgte personer og genstande i én fælles database.

📅 i brug 📅 1995

🌐 Udlændinge og asyl 🌐 EU

Biometrisk klassifikation ▲▲▲▲

Har i et Projekt?

Her på siden kan du anmelde et kunstig intelligens projekt i det offentlige. Kravet er at du kan fungere som kontaktperson og besvare på spørgsmål om systemet.

Indsend projekt

> [Søg i databasen](#)

Hvad bruges kunstig intelligens til i det offentlige?

Filtrer databasen efter formål:

🔍 Profilering >
🗂️ Klassifikation >
🛡️ Kvalitetssikring >
📊 Effektivisering >

Oversigt

- Definition av kunstig intelligens
- Hvor og hvem bruker kunstig intelligens?
- Hva brukes kunstig intelligens til?
- Tre eksempler fra databasen



Definitioner

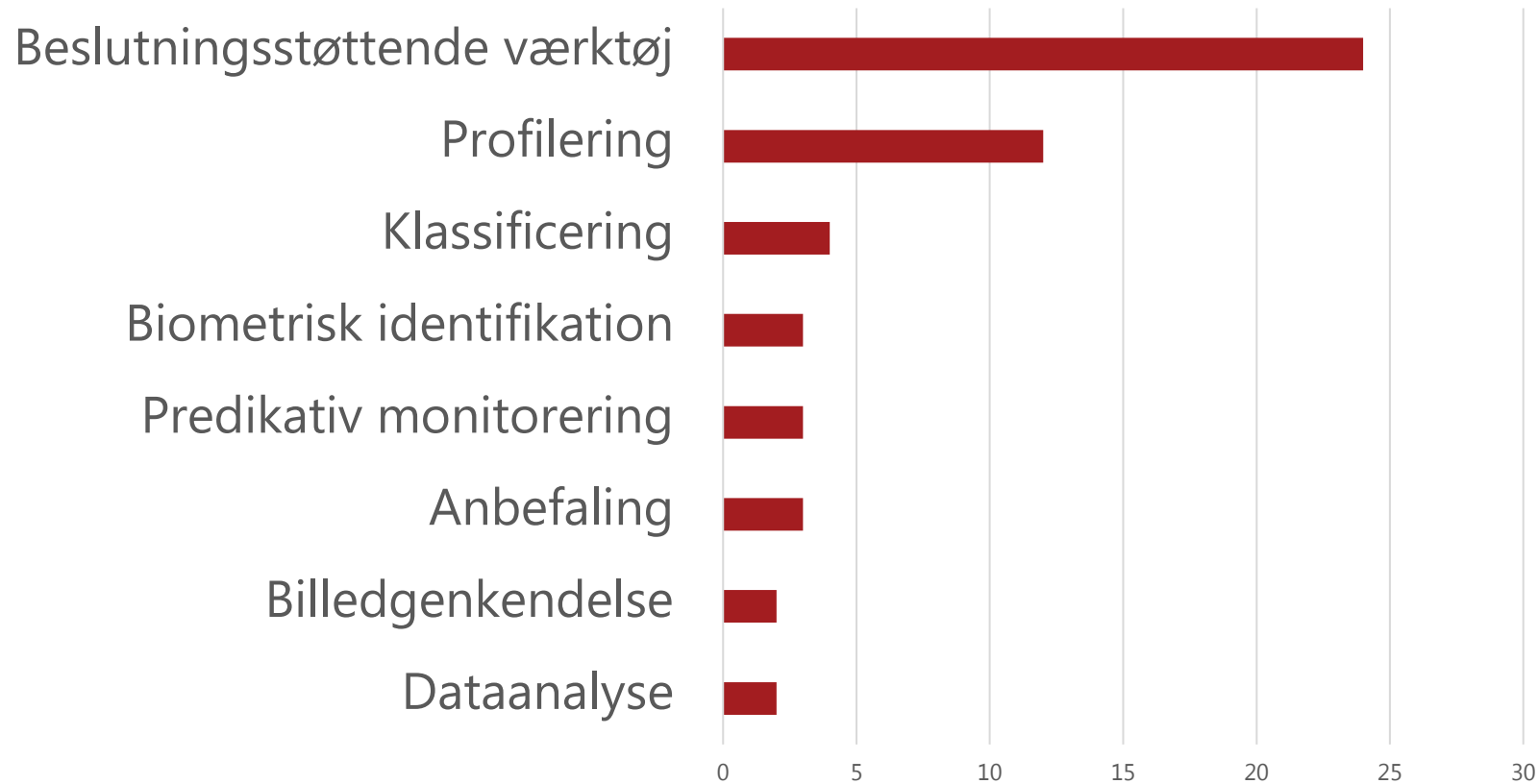
Et »AI-system« er et **maskinbaseret** system, som er udformet med henblik på at fungere med en varierende grad af **autonomi**, og som efter idriftsættelsen kan udvise en **tilpasningsevne**, og som til eksplicite eller implicite mål af det input, det modtager, udleder, hvordan det kan **generere output** såsom forudsigelser, indhold, anbefalinger eller beslutninger, som kan påvirke fysiske eller virtuelle miljøer.

Artikel 3, AI forordningen

Typer af kunstig intelligens

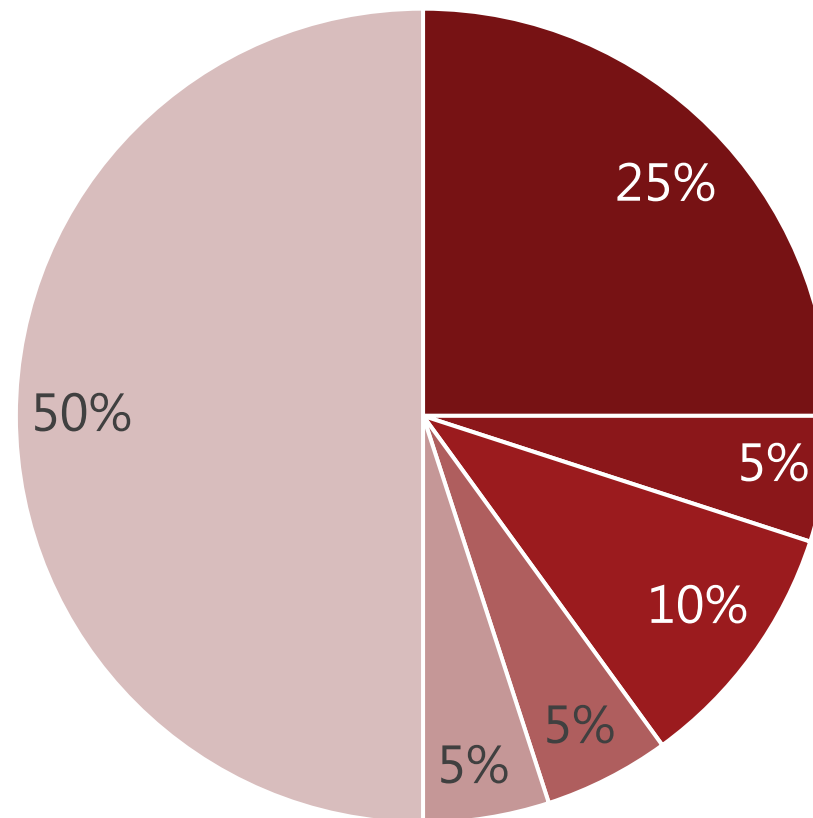
1. Profilering: indsamle oplysninger anvendes til at lave profiler af en person til at forudse eksempelvis adfærd eller fremtidige behov.
2. Dataanalyse: trekker ut innsikter fra store datamengder.
3. Maskinlæring: analyserer store datamengder, finner mønstre, og på baggrund af disse producerer f.eks. egne anbefalinger.
4. Naturlig språkbehandling: brukes til å forstå og generere menneskelig språk.
5. Bilde- og ansiktsgjenkjenning: brukes f.eks. for å identifisere personer i offentlige rom eller analysere medisinske bilder.
6. Beslutningsstøttesystemer: bidrager med beslutningsanbefalinger til offentlige ansatte basert på overnevnte metoder.

Hvad bruges kunstig intelligens til i det offentlige i Danmark?

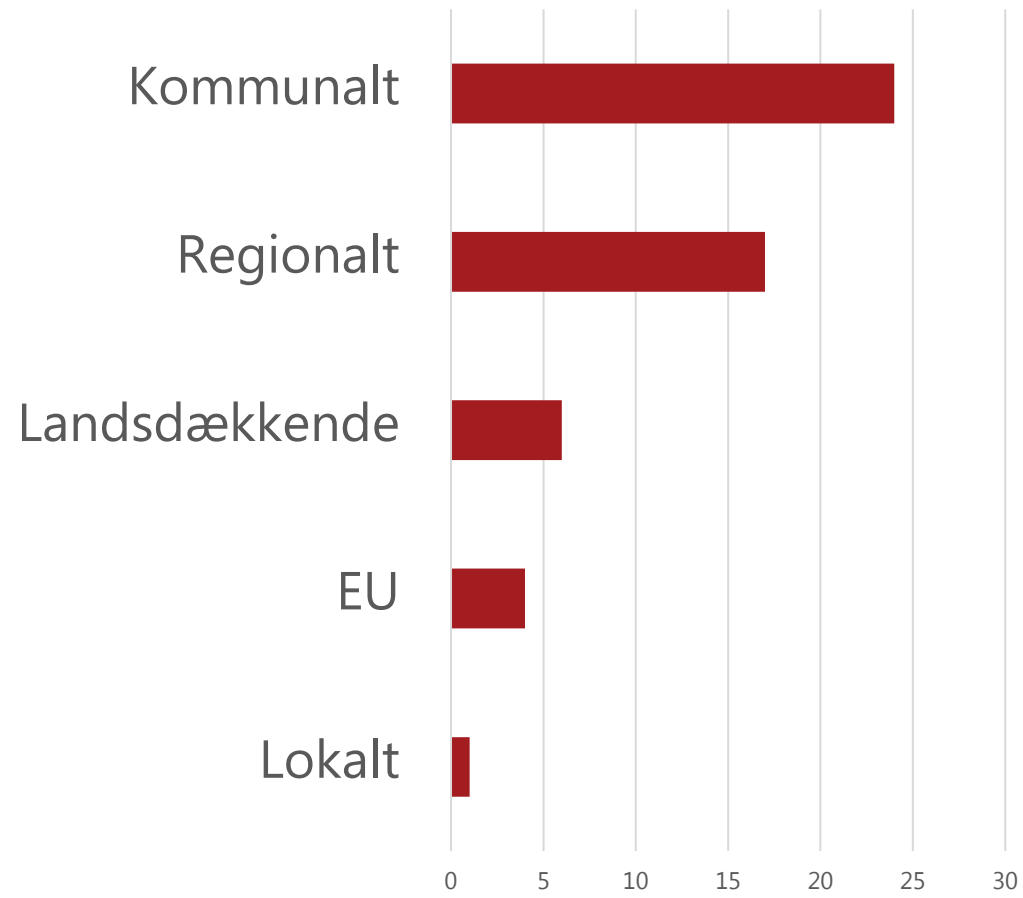


Variasjon blandt beslutningsstøttende KI-systemer

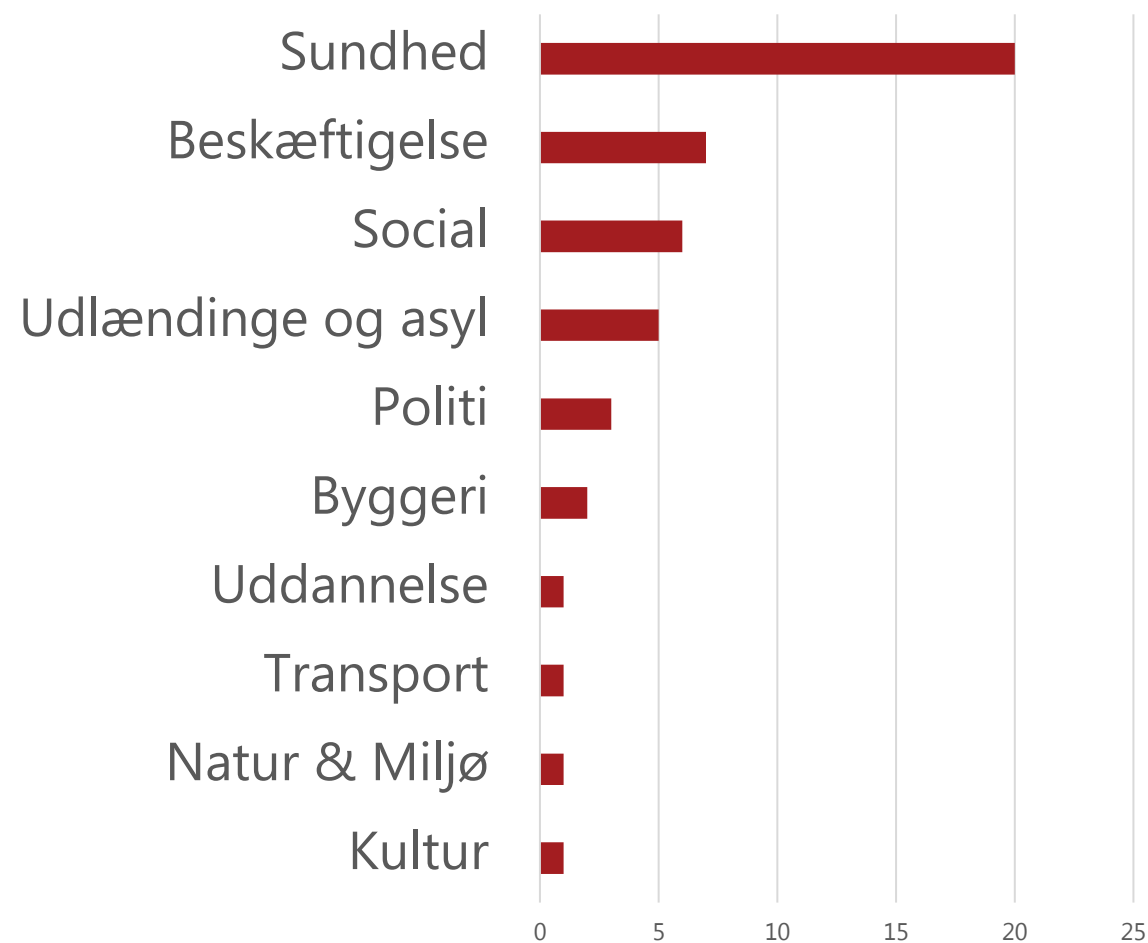
- Diagnostisering og beslutningsstøtte
- Anbefaling og beslutningsstøtte
- Profilering, anbefaling og beslutningsstøtte
- Sagsbehandling, dataanalyse og beslutningsstøtte
- Klassificering og beslutningsstøtte
- Beslutningsstøtte



Hvor brukes der kunstig intelligens?



På hvilke områder forsøg(t)es kunstig intelligens tatt i bruk?



AI-drevet chat- og voicebot (Kommune Kiri)



- Fælleskommunalt project siden 2019
- Avanceret machine-learning-teknologi
- Bygger på norske erfaringer, hvor 80 norske kommuner bruger chatbotten 'Kommune Kari'

Kilde: Roskilde Kommune

Øget erkendelse af hjertestop ved brug af machine learningmodel

- Skal bruges i Region Hovedstadens Akutberedskab
- Beslutningsstøttende værktøj
- Diagnostisering

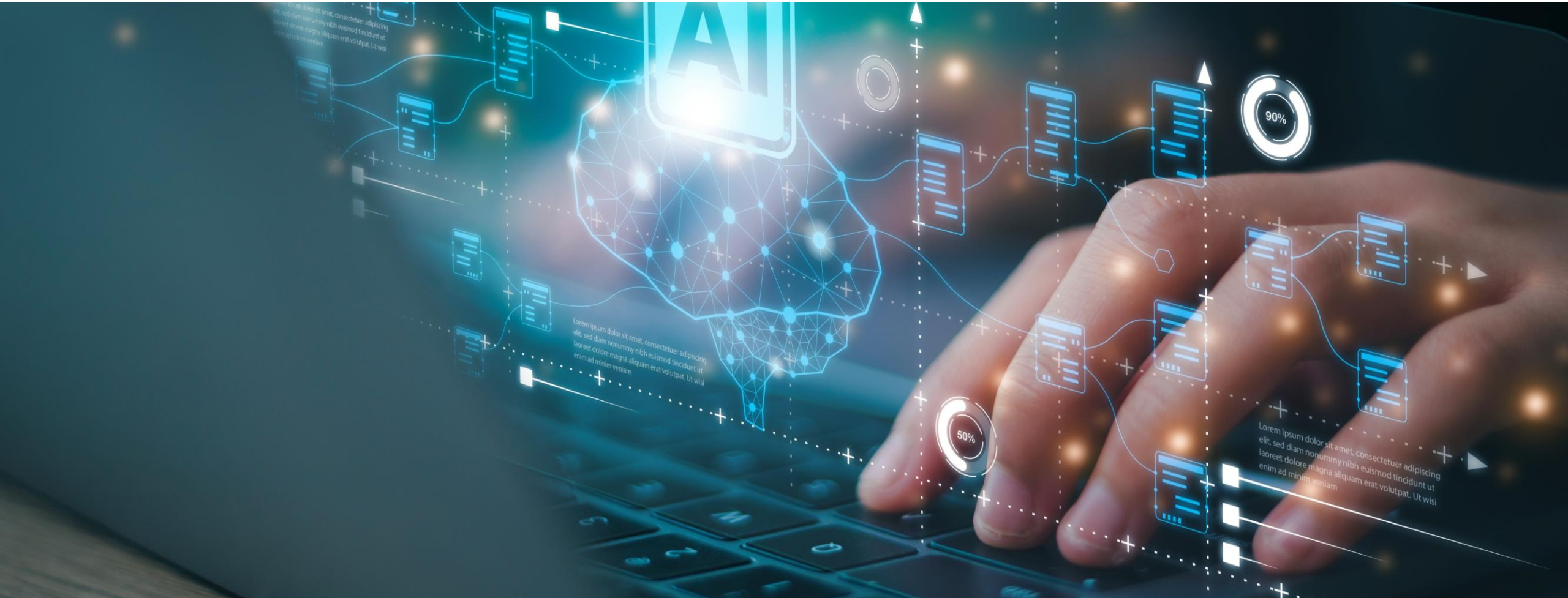


Profileringsværktøj til bekjempelse av langtidsledighet (ASTA)

- Profileringsværktøj
- Brukt af Københavns Kommune
- Lukket i 2022



PAUSE



AI-forordningen

Henrik Udsen

KØBENHAVNS UNIVERSITET





Den Europæiske Unions
Tidende

DA
L-udgaven

2024/1689

12.7.2024

EUROPA-PARLAMENTETS OG RÅDETS FORORDNING (EU) 2024/1689

af 13. juni 2024

om harmoniserede regler for kunstig intelligens og om ændring af forordning (EF) nr. 300/2008, (EU) nr. 167/2013, (EU) nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 og (EU) 2019/2144 samt direktiv 2014/90/EU, (EU) 2016/797 og (EU) 2020/1828 (forordningen om kunstig intelligens)

(EØS-relevant tekst)

EUROPA-PARLAMENTET OG RÅDET FOR DEN EUROPÆISKE UNION HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde, særlig artikel 16 og 114,

under henvisning til forslag fra Europa-Kommissionen,

efter fremsendelse af udkast til lovgivningsmæssig retsakt til de nationale parlamenter,



Den Europæiske Unions
Tidende

DA
L-udgaven

2024/1689

12.7.2024

EUROPA-PARLAMENTETS OG RÅDETS FORORDNING (EU) 2024/1689

af 13. juni 2024

om harmoniserede regler for kunstig intelligens og om ændring af forordning
nr. 167/2013, (EU) nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 og (EU) 2014/90/EU, (EU) 2016/797 og (EU) 2020/1828 (forordningen om k

(EØS-relevant tekst)

EUROPA-PARLAMENTET OG RÅDET FOR DEN EUROPÆISKE UNION HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde, særlig artikel

under henvisning til forslag fra Europa-Kommissionen,

efter fremsendelse af udkast til lovgivningsmæssig retsakt til de nationale parlamenter,



EUROPA-
KOMMISSIONEN

Bruxelles, den 21.4.2021
COM(2021) 206 final

2021/0106 (COD)

Forslag til

EUROPA-PARLAMENTETS OG RÅDETS FORORDNING

**OM HARMONISEREDE REGLER FOR KUNSTIG INTELLIGENS (RETSAKTEN
OM KUNSTIG INTELLIGENS) OG OM ÆNDRING AF VISSE AF UNIONENS
LOVGIVNINGSMÆSSIGE RETSAKTER**

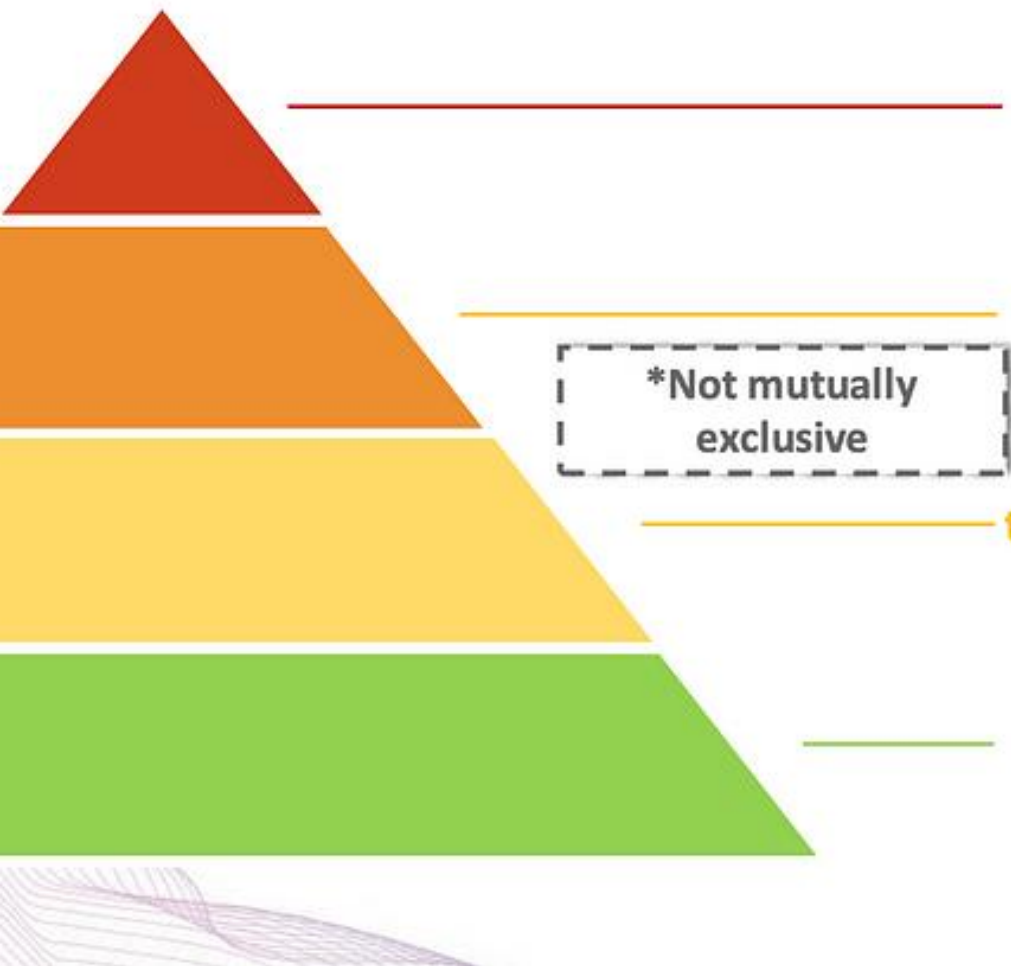
{SEC(2021) 167 final} - {SWD(2021) 84 final} - {SWD(2021) 85 final}

Hvad er AI-forordningen, og hvad er den ikke?

- AI-forordningen er en risikoregulering: fastsætter krav for at undgå og nedbringe risici knyttet til AI
- AI-forordningen regulerer ikke andre retlige spørgsmål, f.eks. om brug af ophavsretligt beskyttede værker eller personoplysninger (GDPR)

Forordningens definition af "AI"

»AI-system«: et maskinbaseret system, som er udformet med henblik på at fungere med en varierende grad af autonomi, og som efter idriftsættelsen kan udvise en tilpasningsevne, og som til eksplicitte eller implicitte mål af det input, det modtager, udleder, hvordan det kan generere output såsom forudsigelser, indhold, anbefalinger eller beslutninger, som kan påvirke fysiske eller virtuelle miljøer



Unacceptable risk

e.g. social scoring

Prohibited

High risk

e.g. recruitment, medical devices

Permitted subject to compliance with AI requirements and ex-ante conformity assessment

*Not mutually exclusive

AI with specific

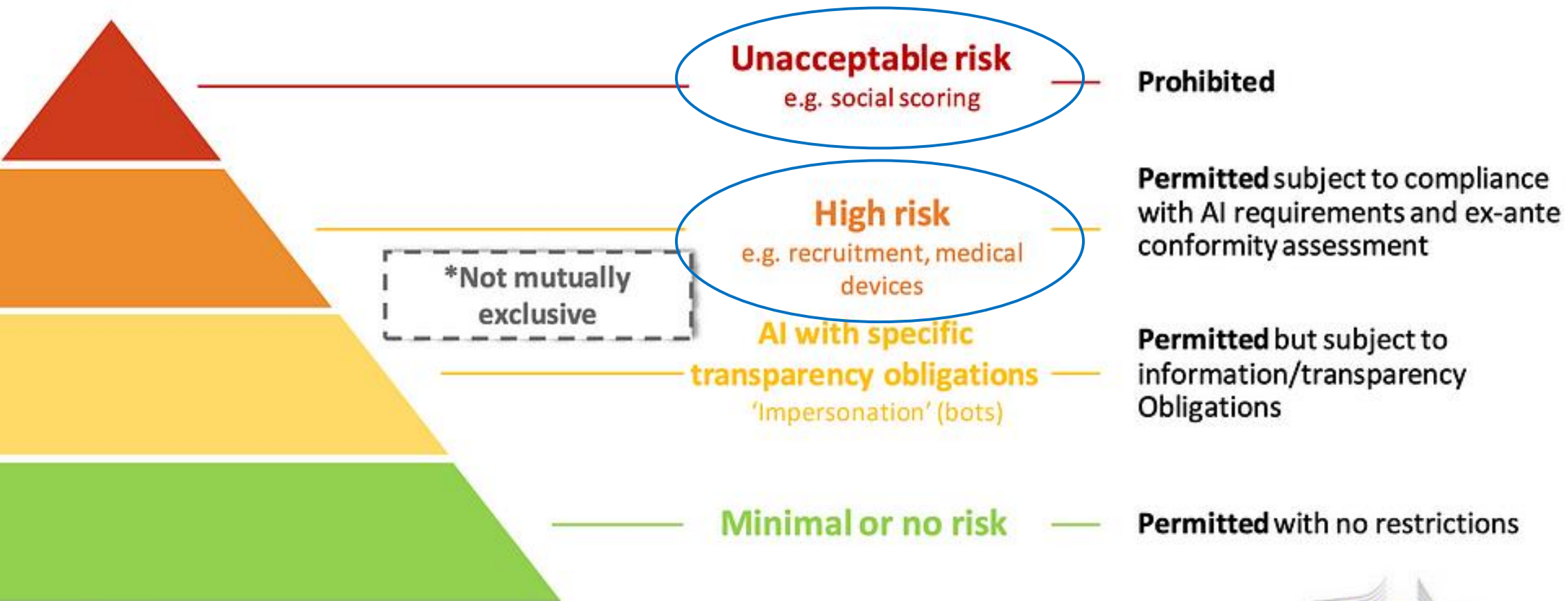
transparency obligations

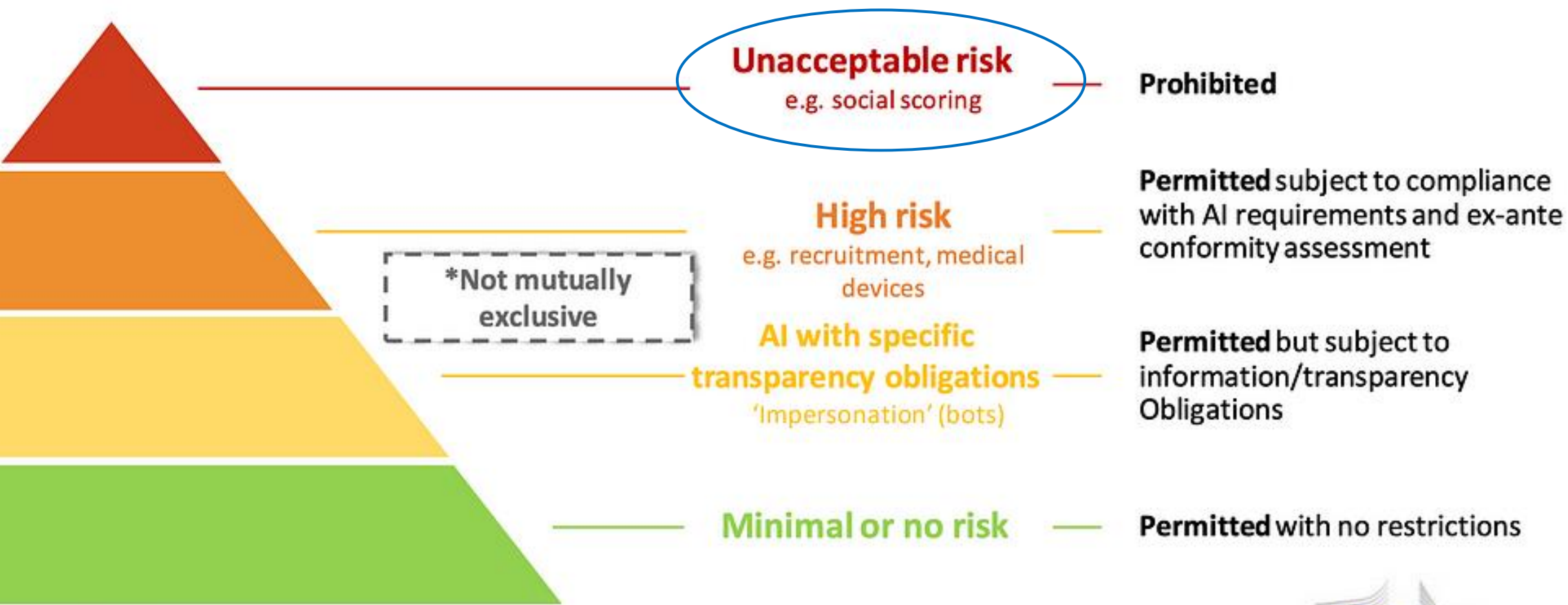
'Impersonation' (bots)

Permitted but subject to information/transparency Obligations

Minimal or no risk

Permitted with no restrictions





Art. 5 – Forbudte former for AI-praksis

Adfærdsmanipulation med betydelig skade

- a) omsætning, ibrugtagning eller anvendelse af et AI-system, der anvender subliminale teknikker, der rækker ud over den menneskelige bevidsthed, eller bevidst manipulerende eller vildledende teknikker med henblik på eller med det resultat i væsentlig grad at fordreje en persons eller en gruppe af personers adfærd ved betydeligt at hæmme dennes evne til at træffe informerede beslutninger, hvilket får dem til at træffe en beslutning, som de ellers ikke ville have truffet, på en måde, der forvolder eller med rimelig sandsynlighed vil forvolde den pågældende person, en anden person eller en gruppe af personer betydelig skade

Udnyttelse af sårbarheder med betydelig skade

- b) omsætning, ibrugtagning eller anvendelse af et AI-system, der hos en fysisk person eller en specifik gruppe af personer udnytter sårbarheder på grundlag af alder, handicap eller en særlig social eller økonomisk situation med henblik på eller med det resultat i væsentlig grad at fordreje den pågældende persons eller en til gruppen hørende persons adfærd på en måde, der forvolder eller med rimelig sandsynlighed vil forvolde den pågældende person eller en anden person betydelig skade

Bedømmelse af social adfærd – skadelige eller ugunstig behandling

- c) omsætning, ibrugtagning eller anvendelse af AI-systemer til evaluering eller klassificering af fysiske personer eller grupper af personer over en given periode på grundlag af deres sociale adfærd eller kendte, udledte eller forudsagte personlige egenskaber eller personlighedstræk, således at den sociale bedømmelse fører til et af eller begge følgende udfald:

Sandsynlighedsvurdering – fremtidig kriminalitet

- d) omsætning, ibrugtagning til dette specifikke formål eller anvendelse af et AI-system til at foretage risikovurderinger af fysiske personer for at vurdere eller forudsige risikoen for, at en fysisk person begår en strafbar handling, hvilket alene er baseret på profilering af en fysisk person eller en vurdering af deres personlighedstræk og personlige egenskaber; dette forbud finder ikke anvendelse på AI-systemer, der anvendes til at understøtte den menneskelige vurdering af en persons involvering i en kriminel aktivitet, som allerede er baseret på objektive og verificerbare kendsgerninger, der er direkte knyttet til en kriminel aktivitet

Ansigtsgenkendelsesdatabaser – ikkemåltrettet indsamling fra internet og kameraovervågning

- e) omsætning, ibrugtagning til dette specifikke formål eller anvendelse af AI-systemer, der opretter eller udvider ansigtsgenkendelsesdatabaser gennem ikkemåltrettet indsamling af ansigtsbilleder fra internettet eller kameraovervågning

Følelsedetektion – arbejdspladser og uddannelsesinstitutioner

- f) omsætning, ibrugtagning til dette specifikke formål eller anvendelse af AI-systemer til at udlede følelser hos en fysisk person på arbejdspladser og uddannelsesinstitutioner, undtagen hvis anvendelsen af AI-systemet er tilsigtet at blive bragt i omsætning af medicinske eller sikkerhedsmæssige årsager

Individuel biometrisk kategorisering - følsomme oplysninger

- g) omsætning, ibrugtagning til dette specifikke formål eller anvendelse af systemer til biometrisk kategorisering, som kategoriserer fysiske personer individuelt på grundlag af deres biometriske data med henblik på at udlede deres race, politiske anskuelser, fagforeningsmedlemskab, religiøse eller filosofiske overbevisning, seksuelle forhold eller seksuelle orientering; dette forbud omfatter ikke mærkning eller filtrering af lovligt indhentede biometriske datasæt såsom billeder på grundlag af biometriske data eller kategorisering af biometriske data på retshåndhævelsesområdet

Biometrisk fjernidentifikation i realtid på offentlige steder mhp. retshåndhævelse

- h) anvendelse af systemer til biometrisk fjernidentifikation i realtid på offentlige steder med henblik på retshåndhævelse, medmindre og i det omfang en sådan anvendelse er strengt nødvendig til et af følgende formål:



Unacceptable risk

e.g. social scoring

Prohibited

High risk

e.g. recruitment, medical devices

Permitted subject to compliance with AI requirements and ex-ante conformity assessment

***Not mutually exclusive**

AI with specific

transparency obligations

'Impersonation' (bots)

Permitted but subject to information/transparency Obligations

Minimal or no risk

Permitted with no restrictions

Høj risiko-systemer - overordnet

- Udtømmende opregning i forordningen af, hvad der udgør høj risiko-systemer (med mulighed for Kommissionen til at udvide listen)
- To typer af høj risiko-systemer
 - AI-systemet omfattet af den EU-produktsikkerhedsregulering, der er opregnet i forordningens bilag I, enten fordi AI-systemet indgår som en sikkerhedskomponent i produktet, eller fordi AI-systemet i sig selv er et produkt
 - AI-systemet er omfattet af opregningen i forordningens bilag III
- Nærmere krav knyttet til udvikling og brug af høj risiko-systemer

Høj risiko-systemer - overordnet

- Udtømmende opregning i forordningen af, hvad der udgør høj risiko-systemer (med mulighed for Kommissionen til at udvide listen)
- To typer af høj risiko-systemer
 - AI-systemet omfattet af den EU-produktsikkerhedsregulering, der er opregnet i forordningens bilag I, enten fordi AI-systemet indgår som en sikkerhedskomponent i produktet, eller fordi AI-systemet i sig selv er et produkt
 - **AI-systemet er omfattet af opregningen i forordningens bilag III**
- **Nærmere krav knyttet til udvikling og brug af høj risiko-systemer**

Høj risiko-systemer – bilag III (art. 6, stk. 2)

Biometri

- Biometrisk fjernidentifikation
- Biometrisk kategorisering på baggrund af følsomme oplysninger (ikke individuelt)
- Følelsedetektion

Kritisk infrastruktur

- Sikkerhedskomponenter i forvaltning og drift af kritisk digital infrastruktur, veje og forsyning

Uddannelse og erhvervsuddannelse

- Adgang og fordeling
- Evaluering og bedømmelse
- Eksamenskontrol

HR og tildeling af opgaver

- Rekruttering og udvælgelse
- Forfremmelse, afskedigelse og andre beslutninger

Offentlige ydelser og visse private tjenester

- Adgang til væsentlige offentlige ydelser
- Kreditvurdering
- Livs- og sygeforsikring
- Vurdering og prioritering nødopkald/situationer

Retshåndhævelse

- Risiko for at blive offer for forbrydelse
- Løgnedetektion
- Vurdering af bevismateriale i straffesager
- Sandsynlighedsvurdering mv. – kriminel adfærd
- Profilering - straffesager

Migrationsstyring, asyl og grænsekontrol

- Løgnedetektion
- Risikovurderinger
- Behandling af asyl, visum og ophold
- ID

Retspleje og demokratiske processer

- Juridisk afgørelsesvirksomhed
- Påvirkning af valgprocesser

Høj risiko-systemer – bilag III (art. 6, stk. 2)

Biometri

- Biometrisk fjernidentifikation
- Biometrisk kategorisering på baggrund af følsomme oplysninger (ikke individuelt)
- Følelsedetektion

Kritisk infrastruktur

- Sikkerhedskomponenter i forvaltning og drift af kritisk digital infrastruktur, veje og forsyning

Uddannelse og erhvervsuddannelse

- Adgang og fordeling
- Evaluering og bedømmelse
- Eksamenskontrol

HR og tildeling af opgaver

- Rekruttering og udvælgelse
- Forfremmelse, afskedigelse og andre beslutninger

1. Biometri, for så vidt som dets anvendelse er tilladt i henhold til relevant EU-ret eller national ret:

a) systemer til biometrisk fjernidentifikation.

Dette omfatter ikke AI-systemer, der er tilsigtet biometrisk verifikation, og hvis eneste formål er at bekræfte, at en bestemt fysisk person er den person, vedkommende hævder at være

b) AI-systemer, der er tilsigtet biometrisk kategorisering i henhold til følsomme eller beskyttede egenskaber eller karakteristika på grundlag af udledning af disse egenskaber eller karakteristika

c) AI-systemer, der er tilsigtet følelsesgenkendelse.

- Risiko for at blive offer for forbrydelse
- Løgnedetektion
- Vurdering af bevismateriale i straffesager
- Sandsynlighedsvurdering mv. – kriminel adfærd
- Profilering - straffesager

Migrationsstyring, asyl og grænsekontrol

- Løgnedetektion
- Risikovurderinger
- Behandling af asyl, visum og ophold
- ID

Retspleje og demokratiske processer

- Juridisk afgørelsesvirksomhed
- Påvirkning af valgprocesser

Høj risiko-systemer – bilag III (art. 6, stk. 2)

Biometri

- Biometrisk fjernidentifikation
- Biometrisk kategorisering på baggrund af følsomme oplysninger (ikke individuelt)
- Følelsesdetektion

Kritisk infrastruktur

- Sikkerhedskomponenter i forvaltning og drift af kritisk digital infrastruktur, veje og forsyning

Uddannelse og erhvervsuddannelse

- Adgang og fordeling
- Evaluering og bedømmelse
- Eksamenskontrol

HR og tildeling af opgaver

- Rekruttering og udvælgelse
- Forfremmelse, afskedigelse og andre beslutninger

Offentlige ydelser og visse private tjenester

- Adgang til væsentlige offentlige ydelser
- Kreditvurdering
- Livs- og sygeforsikring
- Vurdering og prioritering nødopkald/situationer

2. Kritisk infrastruktur: AI-systemer, der tilsigtes anvendt som sikkerhedskomponenter i forvaltningen og driften af kritisk digital infrastruktur, vejtrafik eller forsyning af vand, gas, varme og elektricitet.

- Løgnedetektion
- Vurdering af bevismateriale i straffesager
- Sandsynlighedsvurdering mv. – kriminel adfærd
- Profilering - straffesager

Migrationsstyring, asyl og grænsekontrol

- Løgnedetektion
- Risikovurderinger
- Behandling af asyl, visum og ophold
- ID

Retspleje og demokratiske processer

- Juridisk afgørelsesvirksomhed
- Påvirkning af valgprocesser

Høj risiko-systemer – bilag III (art. 6, stk. 2)

Biometri

- Biometrisk fjernidentifikation
- Biometrisk kategorisering på baggrund af følsomme oplysninger (ikke individuelt)
- Følelsesdetektion

Kritisk infrastruktur

- Sikkerhedskomponenter i forvaltning og drift af kritisk digital infrastruktur, veje og forsyning

Uddannelse og erhvervsuddannelse

- Adgang og fordeling
- Evaluering og bedømmelse
- Eksamenskontrol

HR og tildeling af opgaver

- Rekruttering og udvælgelse
- Forfremmelse, afskedigelse og andre beslutninger

Offentlige ydelser og visse private tjenester

- Adgang til væsentlige offentlige ydelser
- Kreditvurdering
- Livs- og sygeforsikring
- Vurdering og prioritering nødopkald/situationer

Retshåndhævelse

- Risiko for at blive offer for forbrydelse
- Løgnedetektion
- Vurdering af bevismateriale i straffesager
- Sandsynlighedsvurdering mv. – kriminel adfærd
- Profilerings - straffesager

3. Uddannelse og erhvervsuddannelse:

- a) AI-systemer, der tilsigtes anvendt til at bestemme fysiske personers adgang til eller optagelse eller deres fordeling på uddannelsesinstitutioner på alle niveauer
- b) AI-systemer, der tilsigtes anvendt til at evaluere læringsresultater, herunder når disse resultater anvendes til at styre fysiske personers læringsproces på uddannelsesinstitutioner på alle niveauer
- c) AI-systemer, der tilsigtes anvendt til at bedømme det nødvendige uddannelsesniveau, som den enkelte vil få eller vil kunne få adgang til, i forbindelse med eller inden for uddannelsesinstitutioner på alle niveauer
- d) AI-systemer, der tilsigtes anvendt til at overvåge og opdage forbudt adfærd blandt studerende under prøver i forbindelse med eller inden for uddannelsesinstitutioner på alle niveauer.

- Påvirkning af valgprocesser

Høj risiko-systemer – bilag III (art. 6, stk. 2)

Biometri

- Biometrisk fjernidentifikation
- Biometrisk kategorisering på baggrund af følsomme oplysninger (ikke individuelt)
- Følelsedetektion

Kritisk infrastruktur

- Sikkerhedskomponenter i forvaltning og drift af kritisk digital infrastruktur, veje og forsyning

Uddannelse og erhvervsuddannelse

- Adgang og fordeling
- Evaluering og bedømmelse
- Eksamenskontrol

HR og tildeling af opgaver

- Rekruttering og udvælgelse
- Forfremmelse, afskedigelse og andre beslutninger

Offentlige ydelser og visse private tjenester

- Adgang til væsentlige offentlige ydelser
- Kreditvurdering
- Livs- og sygeforsikring
- Vurdering og prioritering nødopkald/situationer

Retshåndhævelse

- Risiko for at blive offer for forbrydelse
- Løgnedetektion
- Vurdering af bevismateriale i straffesager
- Sandsynlighedsvurdering mv. – kriminel adfærd
- Profilering - straffesager

Migrationsstyring, asyl og grænsekontrol

- Løgnedetektion
- Risikovurderinger
- Behandling af asyl, visum og ophold

4. Beskæftigelse, forvaltning af arbejdstagere og adgang til selvstændig virksomhed:

- a) AI-systemer, der tilsigtes anvendt til rekruttering eller udvælgelse af fysiske personer, navnlig til at indrykke målrettede jobannoncer, analysere og filtrere jobansøgninger og evaluere kandidater
- b) AI-systemer, der tilsigtes anvendt til at træffe beslutninger, der påvirker vilkårene for arbejdsrelaterede forhold, forfremmelse eller afskedigelse i arbejdsrelaterede kontraktforhold, til at fordele opgaver på grundlag af individuel adfærd eller personlighedstræk eller personlige egenskaber eller til at overvåge og evaluere personers præstationer og adfærd i sådanne forhold.

Høj risiko-systemer – bilag III (art. 6, stk. 2)

5. Adgang til og benyttelse af væsentlige private tjenester og væsentlige offentlige tjenester og ydelser:

- a) AI-systemer, der tilsigtes anvendt af offentlige myndigheder eller på vegne af offentlige myndigheder til at vurdere fysiske personers berettigelse til væsentlige offentlige bistandsydelser og -tjenester, herunder sundhedstjenester, samt til at tildele, nedsætte, tilbagekalde eller kræve tilbagebetaling af sådanne ydelser og tjenester
- b) AI-systemer, der tilsigtes anvendt til at evaluere fysiske personers kreditværdighed eller fastslå deres kreditvurdering, med undtagelse af AI-systemer, der anvendes til at afsløre økonomisk svig
- c) AI-systemer, der tilsigtes anvendt til at foretage risikovurdering og prisfastsættelse for så vidt angår fysiske personer i forbindelse med livs- og sygeforsikring
- d) AI-systemer, der er tilsigtet at evaluere og klassificere nødopkald fra fysiske personer eller til at blive anvendt til at sende beredskabstjenester i nødsituationer eller til at tildele prioriteter i forbindelse hermed, herunder udrykning af politi, brandslukning og lægehjælp samt patientsorteringssystemer for førstehjælp

Uddannelse og erhvervsuddannelse

- Adgang og fordeling
- Evaluering og bedømmelse
- Eksamenskontrol

HR og tildeling af opgaver

- Rekruttering og udvælgelse
- Forfremmelse, afskedigelse og andre beslutninger

Offentlige ydelser og visse private tjenester

- Adgang til væsentlige offentlige ydelser
- Kreditvurdering
- Livs- og sygeforsikring
- Vurdering og prioritering nødopkald/situationer

Retshåndhævelse

- Risiko for at blive offer for forbrydelse
- Løgnedetektion
- Vurdering af bevismateriale i straffesager
- Sandsynlighedsvurdering mv. – kriminel adfærd
- Profilering - straffesager

Migrationsstyring, asyl og grænsekontrol

- Løgnedetektion
- Risikovurderinger
- Behandling af asyl, visum og ophold
- ID

Retspleje og demokratiske processer

- Juridisk afgørelsesvirksomhed
- Påvirkning af valgprocesser

Høj risiko-systemer – bilag III (art. 6, stk. 2)

Biometri

- Biometrisk fjernidentifikation
- Biometrisk kategorisering på baggrund af følsomme oplysninger (ikke individuelt)
- Følelsesdetektion

6. Retshåndhævelse, for så vidt som deres anvendelse er tilladt i henhold til relevant EU-ret eller national ret:

- AI-systemer, der tilsigtes anvendt af eller på vegne af retshåndhævende myndigheder eller af EU-institutioner, -organer, -kontorer eller -agenturer til støtte for retshåndhævende myndigheder eller på deres vegne til at vurdere risikoen for, at en fysisk person bliver offer for strafbare handlinger
- AI-systemer, der tilsigtes anvendt af eller på vegne af retshåndhævende myndigheder eller af EU-institutioner, -organer, -kontorer eller -agenturer til støtte for retshåndhævende myndigheder som polygrafer eller lignende værktøjer
- AI-systemer, der tilsigtes anvendt af eller på vegne af retshåndhævende myndigheder eller af EU-institutioner, -organer, -kontorer eller -agenturer til støtte for retshåndhævende myndigheder til at vurdere pålideligheden af bevismateriale i forbindelse med efterforskning eller retsforfølgning af strafbare handlinger
- AI-systemer, der tilsigtes anvendt af retshåndhævende myndigheder eller på deres vegne eller af EU-institutioner, -organer, -kontorer eller -agenturer til støtte for retshåndhævende myndigheder til at vurdere risikoen for, at en fysisk person begår eller på ny begår lovovertrædelser, der ikke udelukkende er baseret på profilering af fysiske personer som omhandlet i artikel 3, stk. 4, i direktiv (EU) 2016/680, eller til at vurdere fysiske personers eller grupper personlighedstræk og personlige egenskaber eller tidligere kriminelle adfærd
- AI-systemer, der tilsigtes anvendt af eller på vegne af retshåndhævende myndigheder eller af EU-institutioner, -organer, -kontorer eller -agenturer til støtte for retshåndhævende myndigheder til profilering af fysiske personer som omhandlet i artikel 3, stk. 4, i direktiv (EU) 2016/680 i forbindelse med afsløring, efterforskning eller retsforfølgning af strafbare handlinger.

beslutninger

Offentlige ydelser og visse private tjenester

- Adgang til væsentlige offentlige ydelser
- Kreditvurdering
- Livs- og sygeforsikring
- Vurdering og prioritering nødopkald/situationer

Retshåndhævelse

- Risiko for at blive offer for forbrydelse
- Løgnedetektion
- Vurdering af bevismateriale i straffesager
- Sandsynlighedsvurdering mv. – kriminel adfærd
- Profilering - straffesager

Migrationsstyring, asyl og grænsekontrol

- Løgnedetektion
- Risikovurderinger
- Behandling af asyl, visum og ophold
- ID

Retspleje og demokratiske processer

- Juridisk afgørelsesvirksomhed
- Påvirkning af valgprocesser

Høj risiko-systemer – bilag III (art. 6, stk. 2)

Biometri

- Biometrisk fjernidentifikation
- Biometrisk kategorisering på baggrund af følsomme oplysninger (ikke individuelt)
- Følelsedetektion

7. Migrationsstyring, asylforvaltning og grænsekontrol, for så vidt som deres anvendelse er tilladt i henhold til relevant EU-ret eller national ret:

- AI-systemer, der tilsigtes anvendt af eller på vegne af kompetente offentlige myndigheder eller af EU-institutioner, -organer, -kontorer eller -agenturer som polygrafer eller lignende værktøjer
- AI-systemer, der tilsigtes anvendt af eller på vegne af kompetente offentlige myndigheder eller af EU-institutioner, -organer, -kontorer eller -agenturer til at vurdere en risiko, herunder en sikkerhedsrisiko, en risiko for irregulær migration eller en sundhedsrisiko, som udgøres af en fysisk person, der har til hensigt at rejse ind i eller er indrejst i en medlemsstat
- AI-systemer, der tilsigtes anvendt af eller på vegne af kompetente offentlige myndigheder eller af EU-institutioner, -organer, -kontorer eller -agenturer til at bistå kompetente offentlige myndigheder i behandlingen af ansøgninger om asyl, visum eller opholdstilladelser og hertil relaterede klager med henblik på at fastslå, om de fysiske personer, der ansøger, er berettigede, herunder tilhørende vurdering af pålideligheden af bevismateriale
- AI-systemer, der tilsigtes anvendt af eller på vegne af kompetente offentlige myndigheder eller af EU-institutioner, -organer, -kontorer eller -agenturer i forbindelse med migrationsstyring, asylforvaltning eller grænsekontrol med henblik på at opdage, genkende eller identificere fysiske personer, bortset fra kontrol af rejselegitimation.

HR og tildeling af opgaver

- Rekruttering og udvælgelse
- Forfremmelse, afskedigelse og andre beslutninger

Offentlige ydelser og visse private tjenester

- Adgang til væsentlige offentlige ydelser
- Kreditvurdering
- Livs- og sygeforsikring
- Vurdering og prioritering nødopkald/situationer

Retshåndhævelse

- Risiko for at blive offer for forbrydelse
- Løgnedetektion
- Vurdering af bevismateriale i straffesager
- Sandsynlighedsvurdering mv. – kriminel adfærd
- Profilering - straffesager

Migrationsstyring, asyl og grænsekontrol

- Løgnedetektion
- Risikovurderinger
- Behandling af asyl, visum og ophold
- ID

Retspleje og demokratiske processer

- Juridisk afgørelsesvirksomhed
- Påvirkning af valgprocesser

Høj risiko-systemer – bilag III (art. 6, stk. 2)

Biometri

- Biometrisk fjernidentifikation
- Biometrisk kategorisering på baggrund af følsomme oplysninger (ikke individuelt)
- Følelsesdetektion

Kritisk infrastruktur

- Sikkerhedskomponenter i forvaltning og drift af kritisk digital infrastruktur, veje og forsyning

Uddannelse og erhvervsuddannelse

- Adgang og fordeling
- Evaluering og bedømmelse

Offentlige ydelser og visse private tjenester

- Adgang til væsentlige offentlige ydelser
- Kreditvurdering
- Livs- og sygeforsikring
- Vurdering og prioritering nødopkald/situationer

Retshåndhævelse

- Risiko for at blive offer for forbrydelse
- Løgnedetektion
- Vurdering af bevismateriale i straffesager
- Sandsynlighedsvurdering mv. – kriminel adfærd
- Profilering - straffesager

Migrationsstyring, asyl og grænsekontrol

- Løgnedetektion
- Risikovurderinger
- Behandling af asyl, visum og ophold
- ID

8. Retspleje og demokratiske processer:

- a) AI-systemer, der tilsigtes anvendt af judicielle myndigheder eller på deres vegne til at bistå en judiciel myndighed med at undersøge og fortolke fakta og retten og anvende retten på konkrete sagsforhold eller til at blive anvendt på en lignende måde i forbindelse med alternativ tvistbilæggelse
- b) AI-systemer, der tilsigtes anvendt til at påvirke resultatet af et valg eller en folkeafstemning eller fysiske personers stemmeadfærd i forbindelse med udøvelsen af deres stemme ved valg eller folkeafstemninger. Dette omfatter ikke AI-systemer, hvis output fysiske personer ikke er direkte eksponeret for, såsom værktøjer, der anvendes til at organisere, optimere eller strukturere politiske kampagner ud fra et administrativt eller logistisk synspunkt.

Retspleje og demokratiske processer

- Juridisk afgørelsesvirksomhed
- Påvirkning af valgprocesser

Høj risiko-systemer – bilag III (art. 6, stk. 2)

Biometri

- Biometrisk fjernidentifikation
- Biometrisk kategorisering på baggrund af følsomme oplysninger (ikke individuelt)
- Følelsesdetektion

(61) Visse AI-systemer, der er tilsigtet anvendelse inden for retspleje og i demokratiske processer, bør klassificeres som højrisiko i betragtning af deres potentielt betydelige indvirkning på demokratiet, retsstatsprincippet, individets frihedsrettigheder samt retten til adgang til effektive retsmidler og retten til en retfærdig rettergang. Navnlig for at imødegå risikoen for bias, fejl og uigennemsigtighed bør de AI-systemer, der tilsigtes anvendt af judicielle myndigheder eller på deres vegne for at bistå judicielle myndigheder med at fortolke fakta og lovgivningen og anvende lovgivningen på konkrete sagsforhold, klassificeres som højrisiko. AI-systemer, der tilsigtes anvendt af alternative tvistbilæggelsesorganer til disse formål, bør også betragtes som højrisiko, når resultaterne af den alternative tvistbilæggelsesprocedure har retsvirkninger for parterne. Anvendelsen af AI-værktøjer kan understøtte, men bør ikke erstatte dommernes beslutningskompetence eller retsvæsenets uafhængighed, da den endelige beslutningstagning fortsat skal være en menneskedrevet aktivitet. Klassificeringen af AI-systemer som højrisiko bør dog ikke omfatte AI-systemer, der kun tilsigtes supplerende administrative aktiviteter, som ikke har indflydelse på den egentlige retspleje i de enkelte sager, som f.eks. anonymisering eller pseudonymisering af retsafgørelser, dokumenter eller data, kommunikation mellem personale eller administrative opgaver.

- Evaluering og bedømmelse

8. Retspleje og demokratiske processer:

- AI-systemer, der tilsigtes anvendt af judicielle myndigheder eller på deres vegne til at bistå en juridisk myndighed med at undersøge og fortolke fakta og retten og anvende retten på konkrete sagsforhold eller til at blive anvendt på en lignende måde i forbindelse med alternativ tvistbilæggelse
- AI-systemer, der tilsigtes anvendt til at påvirke resultatet af et valg eller en folkeafstemning eller fysiske personers stemmeadfærd i forbindelse med udøvelsen af deres stemme ved valg eller folkeafstemninger. Dette omfatter ikke AI-systemer, hvis output fysiske personer ikke er direkte eksponeret for, såsom værktøjer, der anvendes til at organisere, optimere eller strukturere politiske kampagner ud fra et administrativt eller logistisk synspunkt.

Offentlige ydelser og visse private tjenester

- Adgang til væsentlige offentlige ydelser
- Kreditvurdering
- Livs- og sygeforsikring
- Vurdering og prioritering nødopkald/situationer

Retshåndhævelse

- Risiko for at blive offer for forbrydelse
- Løgnedetektion
- Vurdering af bevismateriale i straffesager
- Sandsynlighedsvurdering mv. – kriminel adfærd
- Profilering - straffesager

Migrationsstyring, asyl og grænsekontrol

- Løgnedetektion
- Risikovurderinger
- Behandling af asyl, visum og ophold
- ID

Retspleje og demokratiske processer

- Juridisk afgørelsesvirksomhed
- Påvirkning af valgprocesser

Høj risiko-systemer – bilag III (art. 6, stk. 2)

Biometri

- Biometrisk fjernidentifikation
- Biometrisk kategorisering på baggrund af følsomme oplysninger (ikke individuelt)
- Følelsedetektion

Kritisk infrastruktur

- Sikkerhedskomponenter i forvaltning og drift af kritisk digital infrastruktur, veje og forsyning

Uddannelse og erhvervsuddannelse

- Adgang og fordeling
- Evaluering og bedømmelse
- Eksamenskontrol

HR og tildeling af opgaver

- Rekruttering og udvælgelse
- Forfremmelse, afskedigelse og andre beslutninger

Offentlige ydelser og visse private tjenester

- Adgang til væsentlige offentlige ydelser
- Kreditvurdering
- Livs- og sygeforsikring
- Vurdering og prioritering nødopkald/situationer

Retshåndhævelse

- Risiko for at blive offer for forbrydelse
- Løgnedetektion
- Vurdering af bevismateriale i straffesager
- Sandsynlighedsvurdering mv. – kriminel adfærd
- Profilering - straffesager

Migrationsstyring, asyl og grænsekontrol

- Løgnedetektion
- Risikovurderinger
- Behandling af asyl, visum og ophold
- ID

Retspleje og demokratiske processer

- Juridisk afgørelsesvirksomhed
- Påvirkning af valgprocesser

Krav ved udvikling af høj risiko-systemer

- Risikostyring, art. 9
- Data og datastyring, art. 10
- Teknisk dokumentation, art. 11
- Registrering (logging), art. 12
- Gennemsigtighed og brugsanvisning, art. 13
- Menneskeligt tilsyn, art. 14
- Nøjagtighed, robusthed, cybersikkerhed, art. 15

Krav ved udvikling af høj risiko-systemer

- Risikostyring, art. 9
- Data og datastyring, art. 10
- Teknisk dokumentation, art. 11
- Registrering (logging), art. 12
- Gennemsigthed og brugsanvisning, art. 13
- Menneskeligt tilsyn, art. 14
- Nøjagtighed, robusthed, cybersikkerhed, art. 15

Artikel 9 Risikostyringsystem	
1.	Hvad angår højrisiko-AI-systemer oprettes og gennemføres der et risikostyringsystem, som dokumenteres og vedligeholdes.
2.	Risikostyringsystemet skal forstås som en kontinuerlig iterativ proces, der er planlagt og løber i hele højrisiko-AI-systemets livscyklus, og som kræver regelmæssig systematisk gennemgang og opdatering. Det omfatter følgende trin: <ul style="list-style-type: none">a) kortlægning og analyse af kendte og med rimelighed forudsigelige risici, som højrisiko-AI-systemet kan udgøre for sundheden, sikkerheden eller de grundlæggende rettigheder, når højrisiko-AI-systemet anvendes i overensstemmelse med dets tilbagelagte formålb) vurdering og evaluering af de risici, der kan opstå, når højrisiko-AI-systemet anvendes i overensstemmelse med dets tilbagelagte formål og ved fejlanvendelse, der med rimelighed kan forudsesc) evaluering af andre risici, der kan opstå, på grundlag af analyse af data indsamlet fra systemet til overvågning efter omsætningen, jf. artikel 72d) vedtagelse af passende og målrettede risikostyringsforanstaltninger, der har til formål at imødegå de risici, der er identificeret i henhold til litra a)
3.	De i denne artikel omhandlede risici vedrører kun dem, der med rimelighed kan afbødes eller fjernes gennem udviklingen eller vedligeholdelsen af højrisiko-AI-systemet eller tilvejebringelsen af tilstrækkelige tekniske oplysninger.
4.	De i stk. 2, litra d), omhandlede risikostyringsforanstaltninger tager behørigt hensyn til virkningerne og eventuelle interaktioner som følge af den kombinerede anvendelse af kravene i denne afdeling med henblik på at minimere risikoen mere effektivt og samtidig opnå en passende balance i gennemførelsen af foranstaltningerne til opfyldelse af disse krav.
5.	De i stk. 2, litra d), omhandlede risikostyringsforanstaltninger er af en sådan art, at de relevante resterende risici, der er forbundet med hver fase, samt den samlede resterende risiko ved højrisiko-AI-systemerne vurderes at være acceptabel.
I fastlæggelsen af de mest hensigtsmæssige risikostyringsforanstaltninger sikres følgende:	
a)	fjernelse eller begrænsning af de risici, der er identificeret og evalueret i henhold til stk. 2, i det omfang det er teknisk muligt, gennem passende udformning og udvikling af højrisiko-AI-systemet
b)	om nødvendigt gennemførelse af passende foranstaltninger til afbedning og kontrol, som imødegår risici, der ikke kan fjernes
6.	Højrisiko-AI-systemer afprøves med henblik på at identificere de mest hensigtsmæssige og målrettede risikostyringsforanstaltninger. Afprøvnin g sikrer, at højrisiko-AI-systemer yder konsistent i overensstemmelse med deres tilbagelagte formål og overholder de krav, der er fastsat i denne afdeling.
7.	Afprøvningsprocedurerne kan omfatte afprøvnin g under faktiske forhold i overensstemmelse med artikel 60.
8.	Afprøvnin g af højrisiko-AI-systemer foretages på et hvilket som helst tidspunkt under hele udviklingsprocessen, så efter hvad der er relevant, og under alle omstændigheder inden de bringes i omsætning eller ibrugtages. Afprøvnin g foretages på grundlag af på forhånd definerede parametre og sandsynligheds tærskler, der er passende i forhold til det tilbagelagte formål med højrisiko-AI-systemet.
9.	Ved gennemførelsen af det risikostyringsystem, der er fastsat i stk. 1-7, tager udbydere hensyn til, om der i betragtning af det tilbagelagte formål med højrisiko-AI-systemet er sandsynlighed for, at det har en negativ indvirkning på personer under 18 år og i relevant omfang på andre sårbare grupper.
10.	For udbydere af højrisiko-AI-systemer, der er underlagt krav vedrørende interne risikostyringsprocesser i henhold til andre relevante bestemmelser i EU-retten, kan de aspekter, der er fastsat i stk. 1-9, være en del af eller kombineres med de risikostyringsprocedurer, der er fastlagt i henhold til den pågældende ret.

Krav ved udvikling af høj risiko-systemer

- Risikostyring, art. 9
- Data og datastyring, art. 10
- Teknisk dokumentation, art. 11
- Registrering (logging), art. 12
- Gennemsigtighed og brugsanvisning, art. 13
- Menneskeligt tilsyn, art. 14
- Nøjagtighed, robusthed, cybersikkerhed, art. 15

Artikel 10	
Data og datastyring	
1.	De højrisiko-AI-systemer, der gør brug af teknikker, som omfatter træning af AI-modeller med data, udvikles på grundlag af trænings-, validerings- og afprøvningsdatasæt, der opfylder de kvalitetskriterier, der er omhandlet i stk. 2-5, når sådanne datasæt anvendes.
2.	Trænings-, validerings- og afprøvningsdatasæt skal være underlagt former for datastyrings- og dataforvaltningspraksis, som er tilpasset højrisiko-AI-systemets tilgodes formål. Disse former for praksis vedrører navnlig: <ol style="list-style-type: none"> de relevante valg med hensyn til udvælgelse dataindsamlingsprocesser og datasæts oprindelse og, hvis der er tale om personoplysninger, det oprindelige formål med dataindsamlingen relevant dataforberedelsesbehandling såsom annotation, mærkning, rensning, opdatering, berigelse og aggregering formuleringen af amalgamer, navnlig med hensyn til de oplysninger, som datasæts skal måle og repræsentere en vurdering af tilgængeligheden, manglen og egigheden af de datasæt, der er nødvendige undersøgelse med hensyn til mulige bias, der sandsynligvis vil påvirke personers sundhed og sikkerhed, have negativ indvirkning på de grundlæggende retigheder eller føre til forskelsbehandling, som er forbudt i henhold til EU-rammen, navnlig hvis dataoutput påvirker input til fremtidige operationer passende foranstaltninger til at påvise, forebygge og afbøde de mulige bias, der er identificeret i henhold til litra f) kortlægning af relevante datakæder eller datastrømlængder, som forhindrer overholdelse af denne forordning, og hvordan de kan afhjælpes.
3.	Trænings-, validerings- og afprøvningsdatasæt skal i betragtning af det tilgodes formål være relevante, tilstrækkelige repræsentative og i videst muligt omfang fejlfrie og faldvarmde. De skal have de tilstrækkelige statistiske egenskaber, herunder, hvis det er relevant, med hensyn til de personer eller grupper af personer, på hvilke højrisiko-AI-systemet tilgodes anvendt. Disse egenskaber kan opfyldes for de enkelte datasæt eller for en kombination heraf.
4.	I datasæt tages det, i det omfang det er nødvendigt i lyset af deres tilgodes formål, hensyn til de egenskaber eller elementer, der er særlige for den specifikke geografiske, kontekstuelle, adfærdsmæssige eller funktionelle ramme, inden for hvilken højrisiko-AI-systemet tilgodes anvendes.
5.	I det omfang det er strengt nødvendigt for at sikre, at bias i forbindelse med højrisiko-AI-systemer påvises og korrigeres i overensstemmelse med denne artikels stk. 2, litra f) og g), kan udbydere af sådanne systemer undtagelsesvis behandle særlige kategorier af personoplysninger, med forbehold af passende sikkerhedsforanstaltninger med hensyn til fysiske personers grundlæggende retigheder og frihed. Ud over bestemmelserne i forordning (EU) 2016/679 og (EU) 2018/1725 samt direktiv (EU) 2016/680 skal følgende betingelser overholdes for at udføre en sådan behandling: <ol style="list-style-type: none"> påvisning og korrektion af bias kan ikke opnås effektivt ved behandling af andre data, herunder symmetiske eller anonymiserede data de særlige kategorier af personoplysninger er underlagt tekniske begrænsninger for vidensanvendelse af personoplysninger og de mest avancerede sikkerhedsforanstaltninger og foranstaltninger til beskyttelse af privatlivt liv, herunder pseudonymisering de særlige kategorier af personoplysninger er underlagt foranstaltninger, der skal sikre, at de behandlede personoplysninger er sikret, beskyttet og omfattes af passende sikkerhedsforanstaltninger, herunder streng kontrol og dokumentation af adgangen, for at undgå misbrug og sikre, at kun autoriserede personer har adgang til disse personoplysninger med passende fortrolighedsforpligtelser de særlige kategorier af personoplysninger må ikke transmittes til, overføres til eller på anden måde stilles til andre parter de særlige kategorier af personoplysninger slettes, når bias er blevet korrigeret, eller når opbevaringsperioden for personoplysningerne udløbet, alt efter hvad der indtræffer først foretagelserne over behandlingsaktiviteter i henhold til forordning (EU) 2016/679 og (EU) 2018/1725 samt direktiv (EU) 2016/680 indeholder en begrundelse for, hvorfor behandlingen af særlige kategorier af personoplysninger var strengt nødvendig for at opdage og korrigere bias, og hvorfor dette mål ikke kunne nås ved behandling af andre data.
6.	Ved udvikling af højrisiko-AI-systemer, der ikke gør brug af teknikker, der omfatter træning af AI-modeller, finder stk. 2-5 kun anvendelse på afprøvningsdatasæts.

Krav ved udvikling af høj risiko-systemer

- Risikostyring, art. 9
- Data og datastyring, art. 10
- **Teknisk dokumentation, art. 11**
- Registrering (logging), art. 12
- Gennemsigtighed og brugsanvisning
- Menneskeligt tilsyn, art. 14
- Nøjagtighed, robusthed, cybersikkerhed, art. 15

Artikel 11

Teknisk dokumentation

1. Den tekniske dokumentation for et højrisiko-AI-system udarbejdes, inden systemet bringes i omsætning eller ibrugtages, og holdes ajour.

Den tekniske dokumentation udarbejdes således, at den påviser, at højrisiko-AI-systemet overholder de krav, der er fastsat i denne afdeling, og at de oplysninger, der er nødvendige for at vurdere AI-systemets overholdelse af disse krav, gives på en klar og forståelig måde til de nationale kompetente myndigheder og bemyndigede organer. Den skal som minimum indeholde de i bilag IV fastsatte elementer. SMV'er, herunder iværksættervirksomheder, kan fremlægge de elementer i den tekniske dokumentation, der er anført i bilag IV, på en forenklet måde. Med henblik herpå udarbejder Kommissionen en forenklet formular for teknisk dokumentation, der er målrettet små virksomheders og mikrovirksomheders behov. Hvis en SMV, herunder en iværksættervirksomhed, vælger at fremlægge de oplysninger, der kræves i bilag IV, på en forenklet måde, anvender den formularen, der er omhandlet i dette stykke. Bemyndigede organer skal acceptere formularen med henblik på overensstemmelsesvurderingen.

2. Hvis et højrisiko-AI-system tilknyttet et produkt, der er omfattet af den i bilag I, afsnit A, anførte EU-harmoniseringslovgivning, bringes i omsætning eller ibrugtages, udarbejdes der et enkelt sæt teknisk dokumentation, der indeholder alle de oplysninger, der er fastsat i stk. 1, samt de oplysninger, der kræves i henhold til disse retsakter.

3. Kommissionen tillægges beføjelser til at vedtage delegerede retsakter i overensstemmelse med artikel 97 for at ændre bilag IV, hvis det i lyset af den tekniske udvikling er nødvendigt for, at den tekniske dokumentation giver alle de oplysninger, der er nødvendige for at vurdere, om systemet overholder de krav, der er fastsat i denne afdeling.

Krav ved udvikling af høj risiko-systemer

- Risikostyring, art. 9
- Data og datastyring, art. 10
- Teknisk dokumentation, art. 11
- **Registrering (logning), art. 12**
- Gennemsigthed og brugsanvisning
- Menneskeligt tilsyn, art. 14
- Nøjagtighed, robusthed, cybersikkerhed

Artikel 12	
Registrering	
1.	Højrisiko-AI-systemer skal teknisk muliggøre automatisk registrering af hændelser (-logfiler-) under systemets levetid.
2.	For at sikre en passende grad af sporbarhed i højrisiko-AI-systemets funktion i forhold til systemets tilsigtede formål skal logningskapaciteten muliggøre registrering af hændelser, der er relevante for: a) identifikation af situationer, der kan medføre, at højrisiko-AI-systemet udgør en risiko som omhandlet i artikel 79, stk. 1, eller en væsentlig ændring b) lettelse af overvågningen efter omsætningen, jf. artikel 72, og c) overvågning af driften af højrisiko-AI-systemer, jf. artikel 26, stk. 5.
3.	For så vidt angår de højrisiko-AI-systemer, der er omhandlet i bilag III, punkt 1, litra a), omfatter logningskapaciteten som minimum: a) registrering af tidsperioden for hver anvendelse af systemet (startdato og -klokkeslæt samt slutdato og -klokkeslæt for hver anvendelse) b) den referencedatabase, med hvilken systemet har sammenholdt inputdata c) de inputdata, som i søgningen har givet et match d) identifikation af de fysiske personer, der er involveret i verifikationen af resultaterne, jf. artikel 14, stk. 5.

Krav ved udvikling af høj risiko-system

- Risikostyring, art. 9
- Data og datastyring, art. 10
- Teknisk dokumentation, art. 11
- Registrering (logging), art. 12
- Gennemsigtighed og brugsanvisning, art. 13
- Menneskeligt tilsyn, art. 14
- Nøjagtighed, robusthed, cybersikkerhed, art.

Artikel 13

Gennemsigtighed og formidling af oplysninger til idriftsætterne

1. Højrisiko-AI-systemer udformes og udvikles på en sådan måde, at deres drift er tilstrækkelig gennemsigtig til, at idriftsætterne kan fortolke et systems output og anvende det korrekt. Der sikres en passende type og grad af gennemsigtighed med henblik på at opnå overholdelse af de relevante udbyder- og idriftsætterforpligtelser, der er fastsat i afdeling 3.
2. Højrisiko-AI-systemer ledsages af en brugsanvisning i et passende digitalt format eller på anden vis, som indeholder kortfattede, fuldstændige, korrekte og klare oplysninger, som er relevante, tilgængelige og forståelige for idriftsætterne.
3. Brugsanvisningen skal som minimum indeholde følgende oplysninger:
 - a) identitet på og kontaktoplysninger for udbyderen og dennes eventuelle bemyndigede repræsentant
 - b) højrisiko-AI-systemets egenskaber, kapacitet og begrænsninger for dets ydeevne, herunder:
 - i) det tilsigtede formål
 - ii) det niveau af nøjagtighed, herunder systemets parametre, robusthed og cybersikkerhed, jf. artikel 15, i forhold til hvilket højrisiko-AI-systemet er afprøvet og valideret, og som kan forventes, samt alle kendte og forudsigelige omstændigheder, der kan have indvirkning på det forventede niveau af nøjagtighed, robusthed og cybersikkerhed
 - iii) alle kendte eller forudsigelige omstændigheder i forbindelse med anvendelse af højrisiko-AI-systemet i overensstemmelse med dets tilsigtede formål eller ved fejlanvendelse, der med rimelighed kan forudses, der kan medføre risici for sundhed og sikkerhed eller grundlæggende rettigheder, jf. artikel 9, stk. 2
 - iv) hvis det er relevant, højrisiko-AI-systemets tekniske kapacitet og egenskaber til at give oplysninger, som er relevante for at forklare dets output
 - v) hvis det er relevant, dets ydeevne for så vidt angår de specifikke personer eller grupper af personer, på hvilke systemet tilsigtes anvendt
 - vi) hvis det er relevant, specifikationer for inputdataene eller andre relevante oplysninger med hensyn til de anvendte trænings-, validerings- og afprøvningsdatasæt under hensyntagen til højrisiko-AI-systemets tilsigtede formål
 - vii) hvis det er relevant, oplysninger, der sætter idriftsætterne i stand til at fortolke højrisiko-AI-systemets output og anvende det korrekt
 - c) eventuelle ændringer af højrisiko-AI-systemet og dets ydeevne, som udbyderen på forhånd har fastsat på tidspunktet for den indledende overensstemmelsesvurdering
 - d) foranstaltninger til menneskeligt tilsyn, jf. artikel 14, herunder de tekniske foranstaltninger, der er indført for at lette idriftsætternes fortolkning af højrisiko-AI-systemers output
 - e) de nødvendige beregningskrafts- og hardwareressourcer, højrisiko-AI-systemets forventede levetid og eventuelle nødvendige vedligeholdelses- og plejeforanstaltninger, herunder deres hyppighed, for at sikre, at AI-systemet fungerer korrekt, herunder med hensyn til softwareopdateringer
 - f) hvis det er relevant, en beskrivelse af de mekanismer, der er medtaget i højrisiko-AI-systemet, og som giver idriftsætterne mulighed for på korrekt vis at indsamle, lagre og fortolke logfilerne i overensstemmelse med artikel 12.

Krav ved udvikling af høj risiko-systemer

- Risikostyring, art. 9
- Data og datastyring, art. 10
- Teknisk dokumentation, art. 11
- Registrering (logging), art. 12
- Gennemsigtighed og brugsanvisning, art. 13
- **Menneskeligt tilsyn, art. 14**
- Nøjagtighed, robusthed, cybersikkerhed

Artikel 14	
Menneskeligt tilsyn	
1.	Højrisiko-AI-systemer udformes og udvikles på en sådan måde, berunder med passende menneske-maskine-grænsefladeværktøjer, at fysiske personer effektivt kan overvåge dem i den periode, hvor de er i brug.
2.	Menneskeligt tilsyn har til formål at forebygge eller minimere de risici for sundhed, sikkerhed eller grundlæggende rettigheder, der kan opstå, når et højrisiko-AI-system anvendes i overensstemmelse med dets tilsigtede formål eller under forhold med fejlanvendelse, der med rimelighed kan forudses, navnlig hvis sådanne risici fortsat består trods anvendelsen af andre krav, der er fastsat i denne afdeling.
3.	Tilsynsforanstaltningerne skal stå i et rimeligt forhold til risiciene, graden af autonomi og den kontekst, som højrisiko-AI-systemet anvendes i, og sikres ved hjælp af en af eller samtlige følgende typer foranstaltninger:
a)	foranstaltninger, der er fastlagt og, hvis det er teknisk muligt, indbygget i højrisiko-AI-systemet fra udbyderens side, inden systemet bringes i omsætning eller ibrugtages
b)	foranstaltninger, der er fastlagt af udbyderen, inden højrisiko-AI-systemet bringes i omsætning eller ibrugtages, og som er egnede til at blive gennemført af driftsætteren.
4.	Med henblik på gennemførelsen af stk. 1, 2 og 3 leveres højrisiko-AI-systemet til driftsætteren på en sådan måde, at det er muligt for fysiske personer, der har fået til opgave at varetage menneskeligt tilsyn, alt efter hvad der er relevant og forholdsmæssigt, at:
a)	forstå højrisiko-AI-systemets relevante kapacitet og begrænsninger korrekt og være i stand til at overvåge dets drift på behørig vis, herunder med henblik på at opdage og håndtere uregelmæssigheder, funktionsforstyrrelser og uventet ydeevne
b)	være opmærksomme på den mulige tendens til automatisk eller i overdreven grad af forlade sig på output frembragt af et højrisiko-AI-system (automatiseringsbias), navnlig for så vidt angår højrisiko-AI-systemer, der anvendes til at give oplysninger eller anbefalinger til afgørelser, der skal træffes af fysiske personer
c)	fortolke højrisiko-AI-systemets output korrekt under hensyntagen til f.eks. de tilgængelige fortolkningsværktøjer og -metoder
d)	beslutte i en særlig situation ikke at anvende højrisiko-AI-systemet eller på anden måde se bort fra, tilslidesætte eller omgøre outputtet fra højrisiko-AI-systemet
e)	gribe ind i højrisiko-AI-systemets drift eller afbryde systemet ved hjælp af en »stopknap« eller en lignende procedure, som gør det muligt at afbryde systemet i en sikker tilstand.
5.	For så vidt angår de højrisiko-AI-systemer, der er omhandlet i bilag III, punkt 1, litra a), sikrer de foranstaltninger, der er omhandlet i denne artikels stk. 3, desuden, at driftsætteren ikke foretager noget tiltag eller træffer nogen beslutninger på grundlag af en identifikation, der følger af systemet, medmindre denne identifikation er blevet verificeret og bekræftet særskilt af mindst to fysiske personer med den nødvendige kompetence, uddannelse og myndighed.
Kravet om særskilt verifikation foretaget af mindst to fysiske personer finder ikke anvendelse på højrisiko-AI-systemer, der anvendes med henblik på retshåndhævelse, migrationsstyring, grænsekontrol og asylforvaltning, hvis anvendelsen af dette krav efter EU-retten eller national ret skønnes uforholdsmæssig.	

Krav ved udvikling af høj risiko-systemer

- Risikostyring, art. 9
- Data og datastyring, art. 10
- Teknisk dokumentation, art. 11
- Registrering (logging), art. 12
- Gennemsigthed og brugsanvisning, art. 13
- Menneskeligt tilsyn, art. 14
- **Nøjagtighed, robusthed, cybersikkerhed, art. 15**

Artikel 15

Nøjagtighed, robusthed og cybersikkerhed

1. Højrisiko-AI-systemer udformes og udvikles på en sådan måde, at de opnår et passende niveau af nøjagtighed, robusthed og cybersikkerhed, og at de i disse henseender yder konsistent i hele deres livscyklus.
2. For at håndtere de tekniske aspekter af, hvordan de passende niveauer af nøjagtighed og robusthed, der er fastsat i stk. 1, og andre relevante ydeevneparametre måles, tilskynder Kommissionen, alt efter hvad der er relevant, i samarbejde med relevante interessenter og organisationer såsom metrologi- og benchmarkingmyndigheder til udvikling af benchmarks og målemetoder.
3. Højrisiko-AI-systemers niveau og relevante parametre med hensyn til nøjagtighed angives i den ledsagende brugsanvisning.
4. Højrisiko-AI-systemer skal være så modstandsdygtige som muligt over for fejl, svigt og uoverensstemmelser, der kan forekomme i systemet eller i det miljø, som systemet fungerer i, navnlig på grund af systemets interaktion med fysiske personer eller andre systemer. I denne henseende træffes der tekniske og organisatoriske foranstaltninger.

Højrisiko-AI-systemers robusthed kan opnås ved hjælp af tekniske redundansløsninger, som kan omfatte backupplaner eller «fail-safe plans».

De højrisiko-AI-systemer, der fortsætter med at lære efter at være bragt i omsætning eller ibrugtaget, udvikles på en sådan måde med henblik på i videst muligt omfang at fjerne eller reducere risikoen for, at eventuelt output behæftet med bias påvirker input i fremtidige operationer (feedbackløjer), og sikre, at sådanne feedbackløjer behørigt imødegås ved hjælp af passende albedende foranstaltninger.

5. Højrisiko-AI-systemer skal være modstandsdygtige over for uautoriserede tredjeparters forsøg på at ændre deres anvendelse, output eller ydeevne ved at udnytte systemsårbarheder.

De tekniske løsninger, der har til formål at sikre cybersikkerhed i forbindelse med højrisiko-AI-systemer, skal stå i et passende forhold til de relevante omstændigheder og risiciene.

De tekniske løsninger til afhjælpning af AI-specifikke sårbarheder omfatter, alt efter hvad der er relevant, foranstaltninger til at forebygge, opdage, reagere på, afværge og kontrollere angreb, der søger at manipulere træningsdatasættet (dataforgiftning), eller forhåndstrænede komponenter, der anvendes i træning (modelforgiftning), input, der er udformet til at få AI-modellen til at begå fejl (ondsindede eksempler eller modelunddragelse), fortrolighedsangreb eller modelfejl.

Krav til idriftsættere af høj risiko-systemer

Artikel 26

Forpligtelser for idriftsættere af højrisiko-AI-systemer

1. Idriftsættere af højrisiko-AI-systemer træffer passende tekniske og organisatoriske foranstaltninger for at sikre, at de anvender disse systemer i overensstemmelse med den brugsanvisning, der ledsager systemerne, jf. stk. 3 og 6.
2. Idriftsættere overdrager varetagelsen af det menneskelige tilsyn til fysiske personer, der har den nødvendige kompetence, uddannelse og myndighed samt den nødvendige støtte.
3. Forpligtelserne i stk. 1 og 2 berører ikke andre idriftsætterforpligtelser i henhold til EU-retten eller national ret eller idriftsætterens frihed til at tilrettelægge sine egne ressourcer og aktiviteter med henblik på at gennemføre de af udbyderen angivne foranstaltninger til menneskeligt tilsyn.
4. Uden at dette berører stk. 1 og 2, og i det omfang idriftsætteren udøver kontrol over inputdataene, sikrer denne idriftsætter, at inputdataene er relevante og tilstrækkeligt repræsentative med henblik på højrisiko-AI-systemets tilsigtede formål.
5. Idriftsættere overvåger driften af højrisiko-AI-systemet på grundlag af brugsanvisningen og underretter, hvis det er relevant, udbyderne i overensstemmelse med artikel 72. Hvis idriftsættere har grund til at mene, at anvendelsen af højrisiko-AI-systemet i overensstemmelse med anvisningerne kan resultere i, at AI-systemet udgør en risiko som omhandlet i artikel 79, stk. 1, underretter de uden unødigt ophold udbyderen eller distributøren og den relevante markedsovervågningsmyndighed og stiller anvendelsen af dette system i bero. Hvis idriftsættere har konstateret en alvorlig hændelse, underretter de også omgående først udbyderen og dernæst importøren eller distributøren og de relevante markedsovervågningsmyndigheder om den pågældende hændelse. Hvis idriftsætteren ikke er i stand til at kontakte udbyderen, finder artikel 73 tilsvarende anvendelse. Denne forpligtelse omfatter ikke følsomme operationelle data fra idriftsættere af AI-systemer, som er retshåndhævende myndigheder.

For idriftsættere, der er finansielle institutioner, som er underlagt krav vedrørende deres interne ledelse, ordninger eller processer i henhold til EU-retten om finansielle tjenesteydelser, anses overvågningsforpligtelsen i første afsnit for at være opfyldt ved overholdelse af reglerne om ordninger, processer og mekanismer for intern ledelse i henhold til den relevante ret om finansielle tjenesteydelser.

6. Idriftsættere af højrisiko-AI-systemer opbevarer de logfiler, der genereres automatisk af det pågældende højrisiko-AI-system, i det omfang sådanne logfiler er under deres kontrol, i en periode, der er passende i forhold til det tilsigtede formål med højrisiko-AI-systemet, på mindst seks måneder, medmindre andet er fastsat i gældende EU-ret eller national ret, navnlig EU-retten om beskyttelse af personoplysninger.

Idriftsættere, der er finansielle institutioner, som er underlagt krav vedrørende deres interne ledelse, ordninger eller processer i henhold til EU-retten om finansielle tjenesteydelser, beholder logfilerne som en del af den dokumentation, der

Artikel 27

Konsekvensanalyse vedrørende grundlæggende rettigheder for højrisiko-AI-systemer

1. Inden idriftsættelse af et højrisiko-AI-system omhandlet i artikel 6, stk. 2, undtagen højrisiko-AI-systemer, der tilsigtes anvendt på det område, der er anført i bilag III, punkt 2, foretager idriftsættere, der er offentligtretlige organer eller private enheder, der leverer offentlige tjenester, og idriftsættere af de højrisiko-AI-systemer, der er omhandlet i bilag III, punkt 5, litra b) og c), en analyse af konsekvensen for grundlæggende rettigheder, som anvendelsen af et sådant system kan medføre. Med henblik herpå foretager idriftsætterne en konsekvensanalyse bestående af:
 - a) en beskrivelse af idriftsætterens processer, i hvilke højrisiko-AI-systemet vil blive anvendt i overensstemmelse med dets tilsigtede formål
 - b) en beskrivelse af den periode og hyppighed, inden for hvilken hvert højrisiko-AI-system tilsigtes anvendt
 - c) de kategorier af fysiske personer og grupper, som forventes at blive påvirket af dets anvendelse i den specifikke kontekst
 - d) de specifikke risici for skade, der sandsynligvis vil påvirke de kategorier af fysiske personer eller grupper af personer, som er identificeret i henhold til dette stykkes litra c), under hensyntagen til oplysningerne fra udbyderen, jf. artikel 13
 - e) en beskrivelse af gennemførelsen af foranstaltninger til menneskeligt tilsyn i overensstemmelse med brugsanvisningen
 - f) de foranstaltninger, der skal træffes, hvis disse risici opstår, herunder ordningerne for intern ledelse og klagemekanismer.

Forpligtelser for udbydere af AI-modeller til almen brug

Artikel 53

Forpligtelser for udbydere af AI-modeller til almen brug

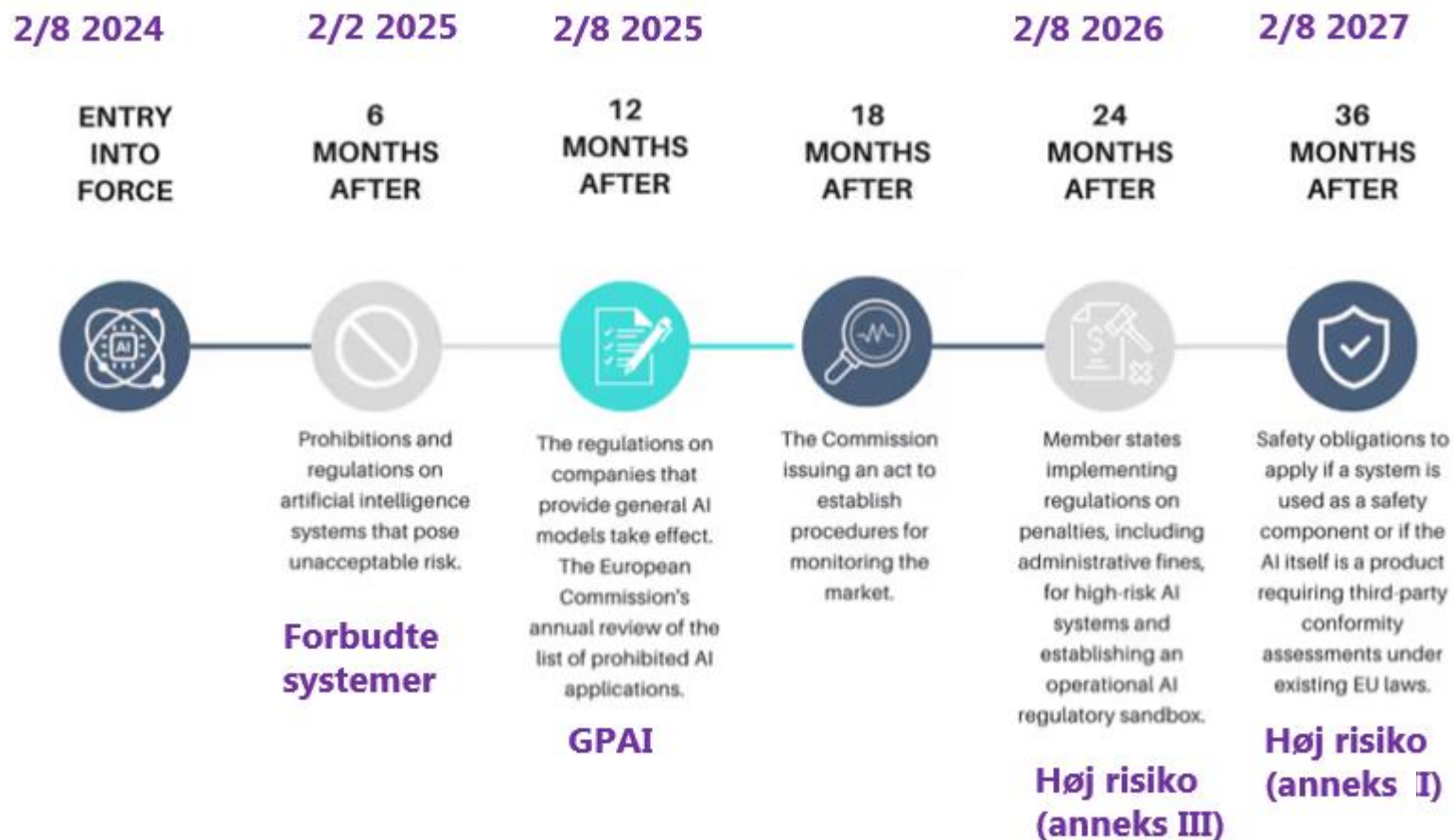
1. Udbydere af AI-modeller til almen brug skal:
 - a) udarbejde og løbende ajourføre den tekniske dokumentation til modellen, herunder dens trænings- og afprøvningsproces og resultaterne af evalueringen af den, som mindst skal indeholde de oplysninger, der er fastsat i bilag XI, med henblik på efter anmodning at forelægge den for AI-kontoret og de nationale kompetente myndigheder
 - b) udarbejde og løbende ajourføre oplysninger og dokumentation og stille disse til rådighed for udbydere af AI-systemer, som har til hensigt at integrere AI-modellen til almen brug i deres AI-systemer. Uden at det berører behovet for at respektere og beskytte intellektuelle ejendomsrettigheder og fortrolige forretningsoplysninger eller forretningshemmeligheder i overensstemmelse med EU-retten og national ret, skal oplysningerne og dokumentationen:
 - i) give udbydere af AI-systemer mulighed for at få en god forståelse af kapaciteterne og begrænsningerne i AI-modellen til almen brug og overholde deres forpligtelser i henhold til denne forordning, og
 - ii) som minimum indeholde de i bilag XII fastsatte elementer
 - c) indføre en politik, der overholder EU-retten om ophavsret og beslægtede rettigheder, navnlig med henblik på at identificere og overholde, herunder ved hjælp af de nyeste teknologier, et forbehold vedrørende rettigheder, der udtrykkes i henhold til artikel 4, stk. 3, i direktiv (EU) 2019/790
 - d) udarbejde og offentliggøre en tilstrækkeligt detaljeret sammenfatning om det indhold, der anvendes til træning af AI-modellen til almen brug, i overensstemmelse med en skabelon, der leveres af AI-kontoret.
2. Forpligtelserne i stk. 1, litra a) og b), finder ikke anvendelse på udbydere af AI-modeller, der frigives i henhold til en gratis open source-licens, der giver mulighed for adgang til, anvendelse, ændring og distribution af modellen, og hvis parametre, herunder vægtene, oplysningerne om modelarkitekturen og oplysningerne om modelanvendelsen, gøres offentligt tilgængelige. Denne undtagelse finder ikke anvendelse på AI-modeller til almen brug med systemiske risici.
3. Udbydere af AI-modeller til almen brug samarbejder om nødvendigt med Kommissionen og de nationale kompetente myndigheder i forbindelse med udøvelsen af deres kompetencer og beføjelser i henhold til denne forordning.
4. Udbydere af AI-modeller til almen brug kan basere sig på praksiskodekser som omhandlet i artikel 56 for at påvise overholdelse af forpligtelserne i nærværende artikels stk. 1, indtil der er offentliggjort en harmoniseret standard. Overholdelse af europæiske harmoniserede standarder giver udbydere formodning om overensstemmelse, i det omfang disse standarder dækker disse forpligtelser. Udbydere af AI-modeller til almen brug, som ikke overholder en godkendt praksiskodeks, eller som ikke overholder en europæisk harmoniseret standard, skal påvise alternative passende måder for overensstemmelse med henblik på Kommissionens vurdering.
5. For at lette overholdelsen af bilag XI, navnlig punkt 2, litra d) og e), i nævnte bilag, tillægges Kommissionen beføjelser til at vedtage delegerede retsakter i overensstemmelse med artikel 97 for at præcisere måle- og beregningsmetoder med henblik på at muliggøre sammenlignelig og verificerbar dokumentation.
6. Kommissionen tillægges beføjelser til at vedtage delegerede retsakter i overensstemmelse med artikel 97, stk. 2, for at ændre bilag XI og XII i lyset af den teknologiske udvikling.
7. Alle de oplysninger eller al den dokumentation, der indhentes i henhold til denne artikel, herunder forretningshemmeligheder, behandles i overensstemmelse med fortrolighedsforpligtelserne fastsat i artikel 78.

Artikel 55

Forpligtelser for udbydere af AI-modeller til almen brug med systemisk risiko

1. Ud over de forpligtelser, der er opført i artikel 53 og 54, skal udbydere af AI-modeller til almen brug med systemisk risiko:
 - a) foretage modevaluering i overensstemmelse med standardiserede protokoller og værktøjer, der afspejler det aktuelle tekniske niveau, herunder gennemførelse og dokumentation af kontradiktorisk afprøvning af modellen med henblik på at identificere og afbøde systemiske risici
 - b) vurdere og afbøde mulige systemiske risici på EU-plan, herunder deres kilder, der kan skyldes udvikling, omsætning eller anvendelse af AI-modeller til almen brug med systemisk risiko
 - c) uden unødigt ophold følge, dokumentere og indberette relevante oplysninger om alvorlige hændelser og mulige korrigerende foranstaltninger til håndtering heraf til AI-kontoret og, alt efter hvad der er relevant, til de nationale kompetente myndigheder
 - d) sikre et tilstrækkeligt niveau af cybersikkerhedsbeskyttelse for AI-modellen til almen brug med systemisk risiko og modellens fysiske infrastruktur.
2. Udbydere af AI-modeller til almen brug med systemisk risiko kan basere sig på praksiskodekser som omhandlet i artikel 56 for at påvise overholdelse af forpligtelserne i nærværende artikels stk. 1, indtil der er offentliggjort en harmoniseret standard. Overholdelse af europæiske harmoniserede standarder giver udbydere formodning om overensstemmelse, i det omfang disse standarder dækker disse forpligtelser. Udbydere af AI-modeller til almen brug med systemiske risici, som ikke overholder en godkendt praksiskodeks, eller som ikke overholder en europæisk harmoniseret standard, skal påvise alternative passende måder for overensstemmelse med henblik på Kommissionens vurdering.
3. Alle de oplysninger eller al den dokumentation, der indhentes i henhold til denne artikel, herunder forretningshemmeligheder, behandles i overensstemmelse med fortrolighedsforpligtelserne fastsat i artikel 78.

Tidslinje



Kilde: Prighter

Uden for AI-forordningen

- Det kan ikke udelukkes, at høj risiko-kravene finder vej til AI-systemer, der ikke er høj risiko-systemer efter forordningen
- Og AI-forordningen er ikke eneste lovgivning, der kan være relevant, når man udvikler og bruger AI-systemer
 - GDPR vil nok i mange tilfælde (også her) være en større barriere end AI-forordningen

**HVILKE SPØRGSMÅL REJSER AI-
BRUG EFTER
PERSONDATARETLIGE REGLER?
*V/ ALLAN FRANK, DATATILSYNET***



Procesretlige og etiske overvejelser ved dommeres brug af AI

Juridisk Forening i København

Den 28. oktober 2024

Muligheder ved dommeres anvendelse af AI

typiske eksempler:

Hjælp til forskning

Bedre adgang til viden

Støtteværktøj til at træffe en afgørelse, f.eks. om strafudmåling eller den rette erhvervsleje

Øget produktivitet

Måske starte et andet sted: *Hvad er retfærdighed?*

Formel retfærdighed

Materiel retfærdighed

Fremfor fokus på teknologien (metoden/algoritmen) fokus på det helt grundlæggende:

- *Kernen i bevisretten – hvordan når vi fra a til b*
- *samspil bevisbedømmelsen og bevisbyrde – hvordan spiller retlige og faktiske formodninger ind (F.eks. Bevis for forsæt = den meningsfulde tolkning af en række handlinger)*

CEPEJ (European Commission for the Efficiency of Justice) Ethical Charter on the use of AI (2018)

- ***Principle of respect of fundamental rights***: ensuring that the design and implementation of artificial intelligence tools and services are compatible with fundamental rights
- ***Principle of non-discrimination***: specifically preventing the development or intensification of any discrimination between individuals or groups of individuals
- ***Principle of quality and security***: using certified sources and intangible data with models conceived in a multi-disciplinary manner, in a secure technological environment
- ***Principle of transparency, impartiality and fairness***: making data processing methods accessible and understandable, authorising external audits
- ***Principle of “under user control”***: precluding a prescriptive approach and ensuring that users are informed actors and in control of their choices.

Procesretlige overvejelser

Bevisførelsen direkte for den dømmende ret - Alene lægge vægt på det, der er en del af bevisførelsen

Muligheden for kontradiktion – at blive hørt

AI som redskab til protokollering af forklaringer – betydningen af gengivelsen

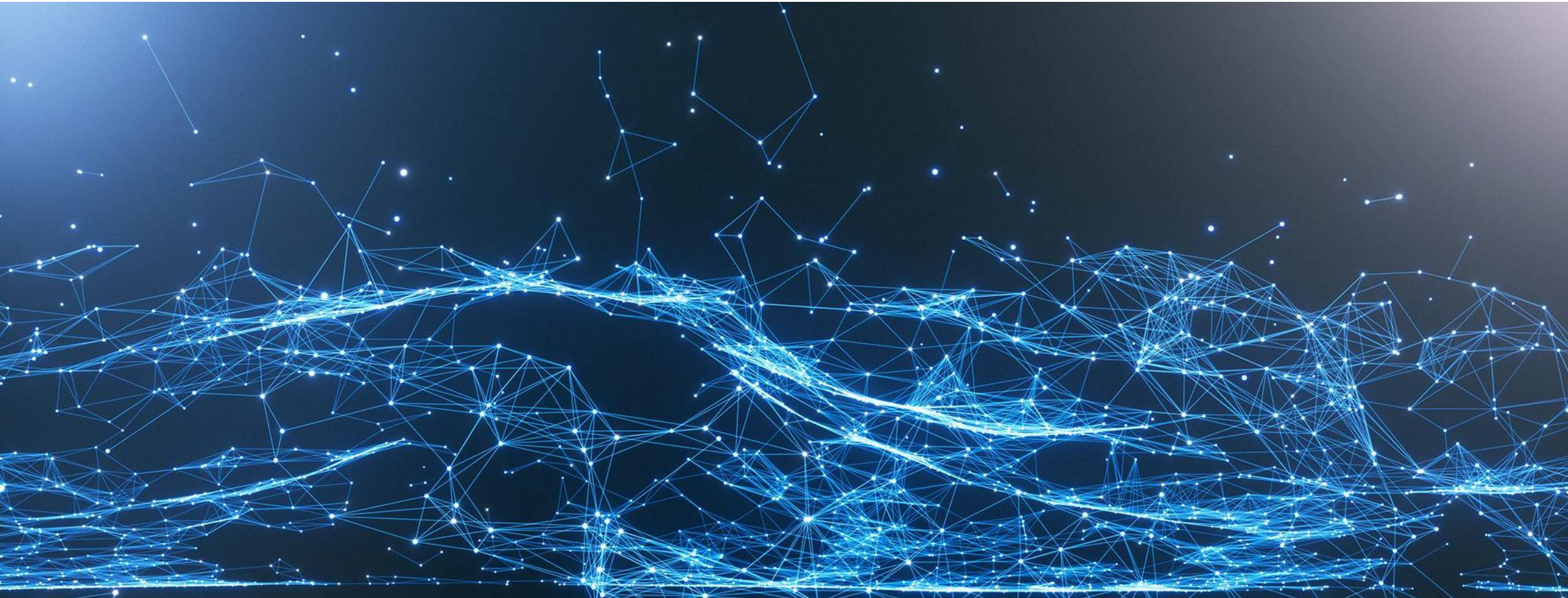
Har dommere (nok) viden om teknologi og AI – hvordan stiller jeg som dommer de rigtige spørgsmål?

- *Regler for fremlæggelse af digitale beviser?*
- *En matematisk beregning fremfor en konkret individuel vurdering*
- *Anvendelse på fastlæggelse af faktum/bevisresultat eller til at skabe overblik over allerede tilgængelig viden*

Etiske overvejelser

- Udfordres princippet om mundtlighed i straffeprocessen?
- Udfordrer AI den fri bevisbedømmelse?
 - Vægten af det enkelte bevis skjult eller uigennemsigtig?
 - Bedømmelsen af bevisernes troværdighed kan blive udfordret
 - Troværdighed ikke en egenskab hos et vidne/part, men resultatet af det samlede produkt af de spørgsmål, der stilles, og de svar, der gives
- Hvordan sikres reelt transparens?
 - Hvordan bliver et støtteværktøj en del af dommens begrundelse og resultat
- Skelne falske fra sande beviser
 - hvordan tjekker dommeren validitet- troværdigheden- af input data til algoritmer- og dermed brugbarhed en af output
 - Hvordan vurdere risiko for bias i algoritmer

OVERVEJELSER OM BRUG AF AI I ET ADVOKATHUS



KAN CHAT GPT LAVE ET UDKAST TIL ET SVARSKRIFT?

- I et pilotprojekt forsøgte vi at få ChatGPT til at lave svarskrifter i sager på et specifikt retsområde og en konkret type sager baseret på tidligere, lignende sager.
- Vi fokuserede på en "Human in the loop" tilgang for at lave kvalitetssikring undervejs i processen.
- Vi benyttede "in-context learning", hvor ChatGPT genererer svar ud fra den kontekst, den har fået gennem specifikke instruktioner (prompts) baseret på nuværende og tidligere sagsmateriale.

Interactive Svarskrift generator Svarskrift generator Document summaries

GPT version: GPT 4 Vælg sags ID: Udvidet

Chatbot

Hvad er din systemmeddelelse?

Dette er en avanceret juridisk AI-assistent, som er udviklet til at hjælpe med at generere juridiske dokumenter [redacted] ved at bruge tidligere sager som reference.

Kan du hjælpe mig med at generere et svarskrift til [redacted] som jeg arbejder på? Dokumentet skal bestå af flere dele, og jeg vil gerne håndtere disse hver for sig.

Selvfølgelig, jeg vil gerne hjælpe med at generere et svarskrift til dig [redacted] ad os starte med den første del af dokumentet. Hvad er det specifikt, du har brug for hjælp til? Er det formuleringen af en påstand, sagsfremstilling, anbringender eller noget andet?

Jeg vil gerne have, at du starter med at beskrive, hvad "sagens tema" er for denne sag.

"Sagens Tema" for denne sag er:
[redacted]

Chat besked
Spørg om ændringer, mere information eller uddybelse

Accepter svar Send Fjern sidste besked Ryd



KAN CHAT GPT LAVE ET UDKAST TIL ET SVARSKRIFT?

KONKLUSION:

- Ja, men den kan ikke lave det sprogligt præcist nok.
- Store udfordringer med konsistens.
- Til gengæld er den god til mange af de indledende steps.

Interactive Svarskrift generator | Svarkskrift generator | Document summaries

GPT version: GPT 4 | Vælg sags ID: [] | Udvidet

Chatbot

Hvad er din systemmeddelelse?

Dette er en avanceret juridisk AI-assistent, som er udviklet til at hjælpe med at generere juridiske dokumenter [] ved at bruge tidligere sager som reference.

Kan du hjælpe mig med at generere et svarskrift til [] som jeg arbejder på? Dokumentet skal bestå af flere dele, og jeg vil gerne håndtere disse hver for sig.

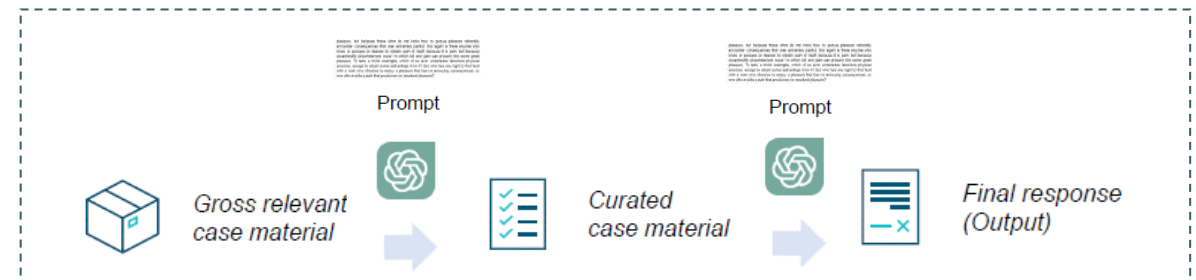
Selvfølgelig, jeg vil gerne hjælpe med at generere et svarskrift til dig [] ad os starte med den første del af dokumentet. Hvad er det specifikt, du har brug for hjælp til? Er det formuleringen af en påstand, sagsfremstilling, anbringender eller noget andet?

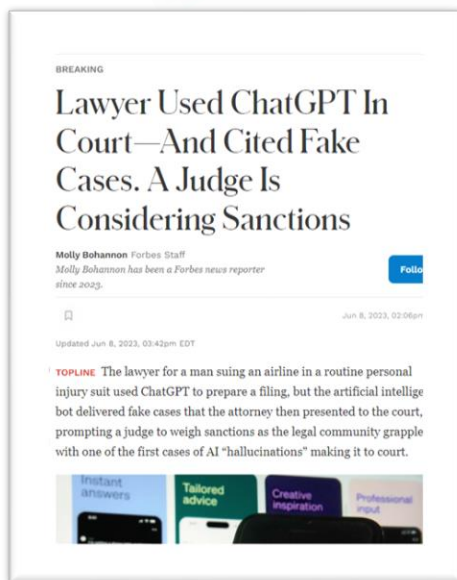
Jeg vil gerne have, at du starter med at beskrive, hvad "sagens tema" er for denne sag.

"Sagens Tema" for denne sag er:
[]

Chat besked
Spørg om ændringer, mere information eller uddybelse

Accepter svar | | |





SPROGLIG PRÆCISION OG KONSISTENS ER AFGØRENDE I JURIDISK ARBEJDE

Grundmodellerne og de generiske løsninger mangler præcision på specialtområder

- Store sprogmodeller er trænet på data, hvoraf kun en minimal mængde er dansk juridisk sprog. De forstår derfor ikke nuancerne.
- CoPilot eller ChatGPT kan sagtens løse mange administrative opgaver, men ikke præcisionsarbejdet med juridisk indhold.

Supplerende data og fine tuning er nødvendigt

- Løsninger til juridisk arbejde, er typisk fine-tunet til at forstå den juridisk kontekst bedre. Det er den "value-add" man betaler for.

Human in the loop er afgørende for at forebygge og identificere fejl og mangler

- En doven fuldmægtig bliver ikke mindre doven af at bruge AI.
- Menneskelig involvering og kvalitetssikring er den vigtigste sikkerhedsforanstaltning i brugen af AI – både i test, udvikling og daglig anvendelse.















KONKLUSION FRA KARNOVS AI WHITEPAPER 2024

”Den generelle udvikling inden for kunstig intelligens ser lige nu ud til at være præget af et integreret perspektiv, hvor teknologi og virksomheders egne data forenes i AI-løsninger, der matcher individuelle branchers krav og behov”

VI KAN IKKE FÅ ÉN AI, DER KAN DET HELE



TYPER AF, OG EKSEMPLER PÅ AI LØSNINGER FOR ADVOKATER

1 Grundmodeller				
2 AI som er/bliver integreret i generisk software			 Microsoft Copilot	
3 AI som er/bliver integreret i eksisterende legal-tech løsninger	 Share with Intelligence		 Djøf Forlag	
4 AI som er tiltænkt det juridiske arbejde generelt				 Part of Thomson Reuters
5 AI som er tiltænkt specialiserede juridiske områder eller opgaver				

VORES AI ARBEJDSFOR



MEDARBEJDERNES KOMPETENCER

Sikre de kompetencer, der er nødvendige for, at vi kan anvende AI ansvarligt og effektivt



USE CASES & TEKNOLOGIER

Fokus på konkrete use cases og teknologier, som vi løbende prioriterer og udvikler små løsninger til.



VALG AF LØSNINGER

Screening og valg af løsninger på markedet. Afgrænsede pilotforløb og vurdering af cost/benefit og arkitektur ift. skalering og integrationer..

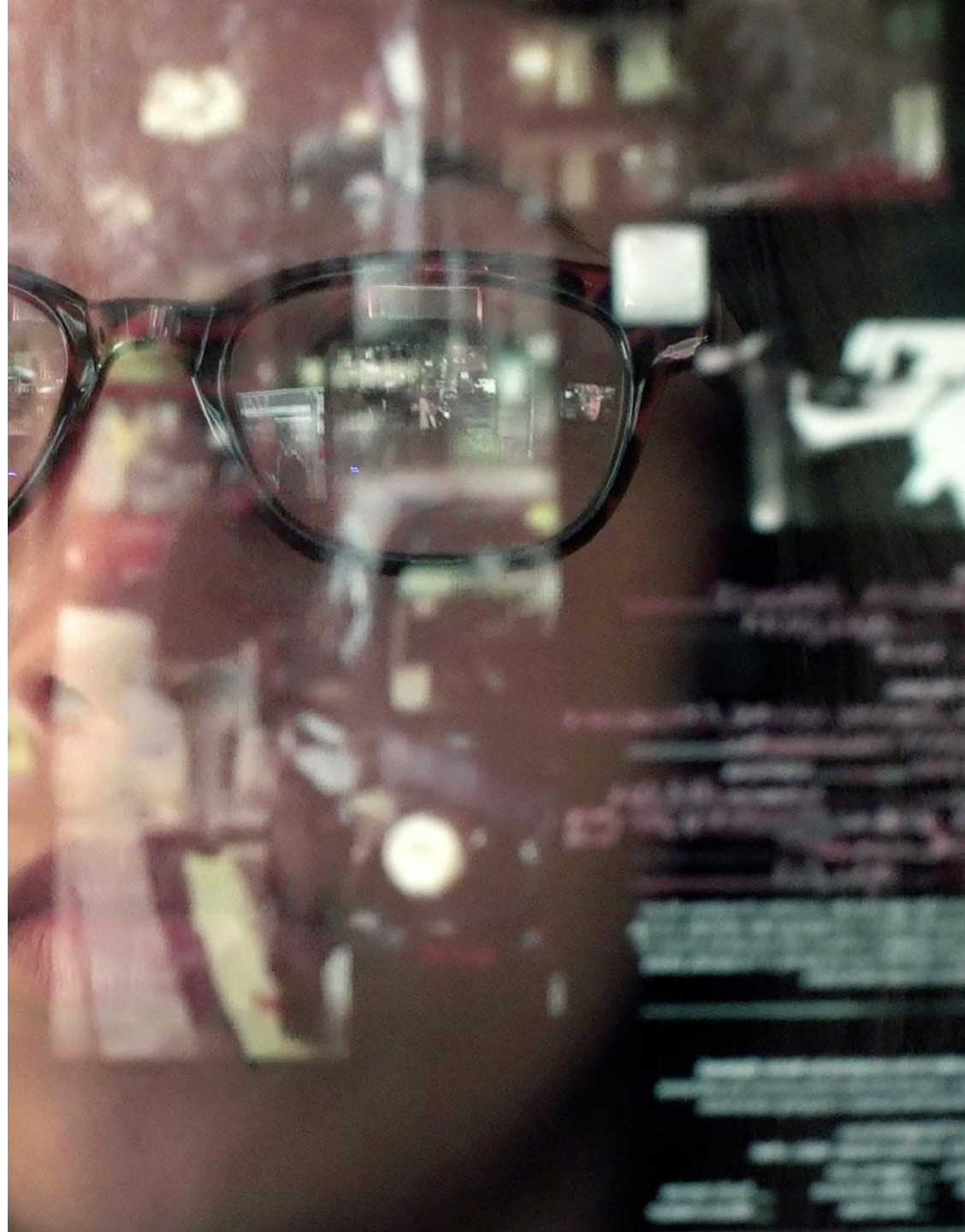


COMPLIANCE & SIKKERHED

Håndtering af de risici, der følger med anvendelsen af kunstig intelligens. Databeskyttelse, etiske overvejelser om anvendelse (må/kan/vil) og IT sikkerhed. Tæt dialog med Informationssikkerhedsudvalget.

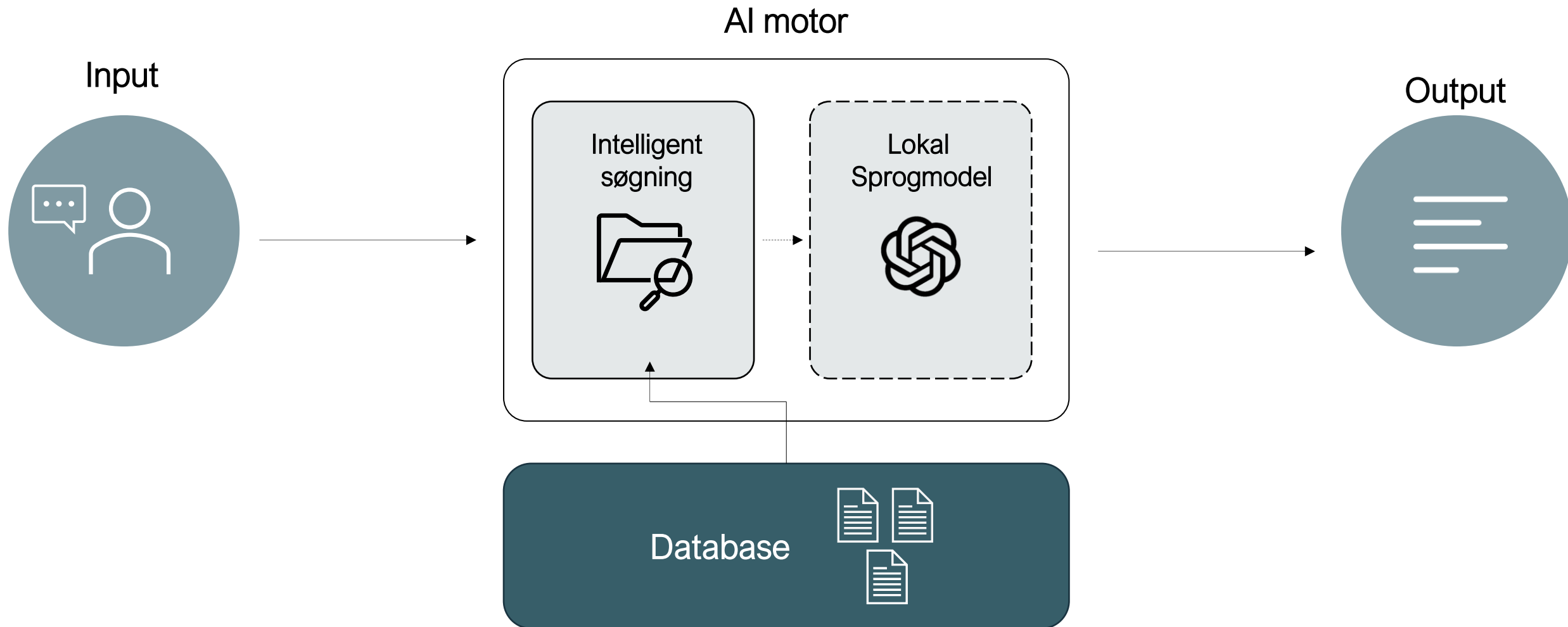
HENSYN OG PRINCIPPER

1. **Uddannelse og brugerinvolvering** - det kræver dygtige jurister at teste løsninger og validere output.
2. **Kontrol vs. tempo** - Afgrænsede use cases og faseopdelt implementering.
3. **Undgå at bruge en "hammer til en skrue"**. Gen AI hverken kan eller skal løse alt.
4. **Human in the loop** – AI understøttede arbejdsgange deles op i steps, hvor der er et menneske inde over.
5. **Tænk modulært** – udviklingen går stærkt, og vi vil undgå at være afhængige af én model eller teknologi.
6. **Høje krav til leverandører, særligt nye spillere** – Bl.a. et vågent øje for manglende transparens ift. træningsdata og "for hurtig" udvikling, f.eks. brug af problematiske 3. partsteknologier.
7. **Databeskyttelse** - GDPR, klientfortrolighed og IP.



ARKITEKTUREN I VORES EGNE LØSNINGER (RAG)

VI HAR KONTROL OVER, OG KAN UDSKIFTE DE ENKELTE KOMPONENTER



DATAKILDER OG HENSYN - JURIDISKE LØSNINGER

OFFENTLIGT TILGÆNGELIG DATA	IP-BESKYTTET DATA	EGNE DATA	KLIENTERS DATA
Eksempler: <ul style="list-style-type: none">• Lovbekendtgørelser• Cirkulærer• Vejledninger• Skrivelser• Offentlige afgørelser og domme	Eksempler: <ul style="list-style-type: none">• Indhold fra f.eks. DJØF og Karnov• Litteratur i øvrigt• Materialesamlinger på specialistområder	Eksempler <ul style="list-style-type: none">• Paradigmer• Klausuler• Interne notater og vidensdokumenter	Eksempler <ul style="list-style-type: none">• Kontrakter• Aftalegrundlag• Bestyrelsesnotater• Risikovurderinger
Frit tilgængeligt, men skal opdateres løbende.	Kan typisk kun tilgås via licens til udbyderens løsning/platform.	Særligt datakvalitet og informationssikkerhed er afgørende.	Samme hensyn som til egne data. Skal herudover beskyttes yderligere strukturelt – bl.a. ved hjælp af adgangsstyring.

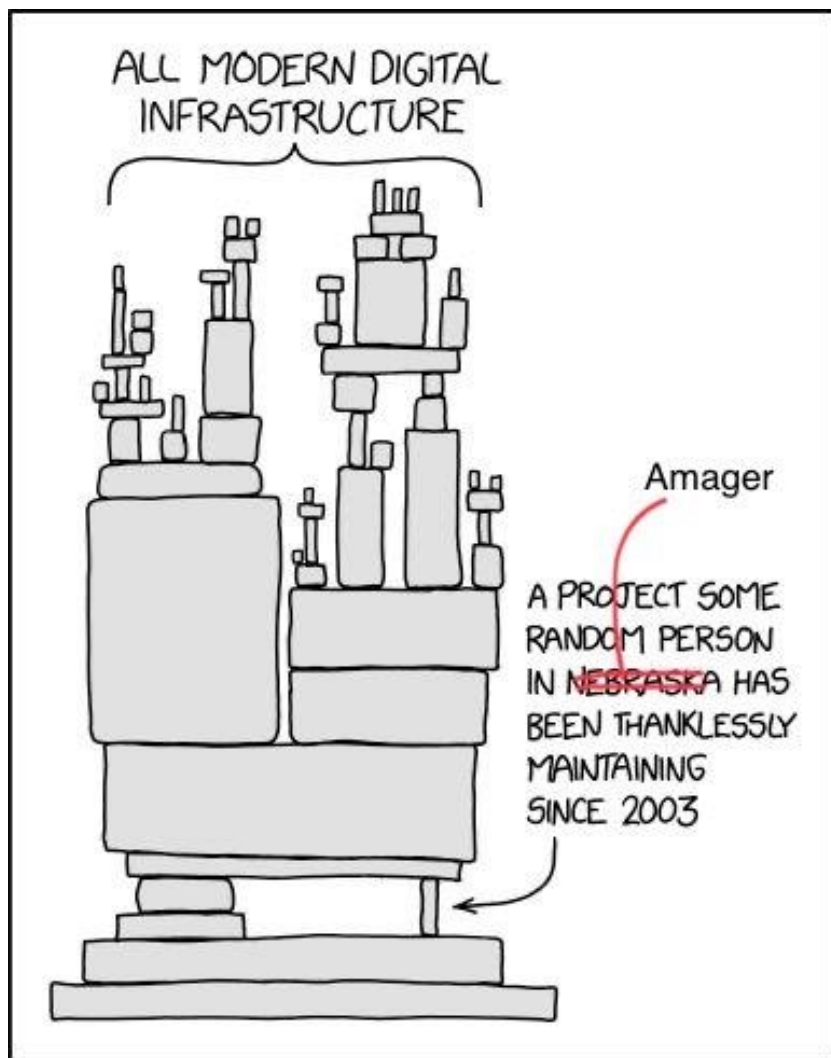
EKSEMPLER PÅ INTERNE USE CASES OG DATAKILDER

OFFENTLIGT TILGÆNGELIG DATA	IP-BESKYTTET DATA	EGNE DATA	KLIENTERS DATA
Use case 1: Søgning i afgørelser på et retsområde			
Indhold tilgængelig på en myndigheds hjemmeside	Indhold fra en materialesamling på området – efter aftale med udbyder.	Egen praksis og paradigmer på området	-
Use case 2: Arbejde med baggrund og kontraktgrundlag for et konkret, mangeårigt projekt			
-	-	-	Forarbejder, korrespondance, hovedkontrakt og delaftaler vedrørende konkret, stort byggeprojekt.
Use case 3: Find svarskrifter, som ligner en ny sag			
		Tidligere afgivede svarskrifter på området	

Tværgående funktionalitet:

Q&A, kildehenvisninger, dokument sammenligning, rettighedsstyring, feedbackfunktion

AI ER IKKE EN TRYLLESTAV



TAK FOR I DAG!

Poul Schmith har indgået aftale med VISDA, som omfatter billederne i denne præsentation.

Præsentationen og de heri indeholdte billeder er udelukkende til intern brug for modtageren og må ikke viderespredes.