



# Regulering af AI

## Gennemgang af AI Act

Fag: AI 502 - Etik og Privacy

Stefan Juvald Stade

# Det ingen skam at komme med på et afbud...

---



# Stefan Juvald Stade

---



Education: Cand.merc.jur. University  
of Southern Denmark (2013)



The Danish Financial Supervisory  
Authority 2013 - 2016



Focus Advokater 2016 - nu  
Legal Tech & compliance



Danske Advokaters AI Working Party  
2024 - nu



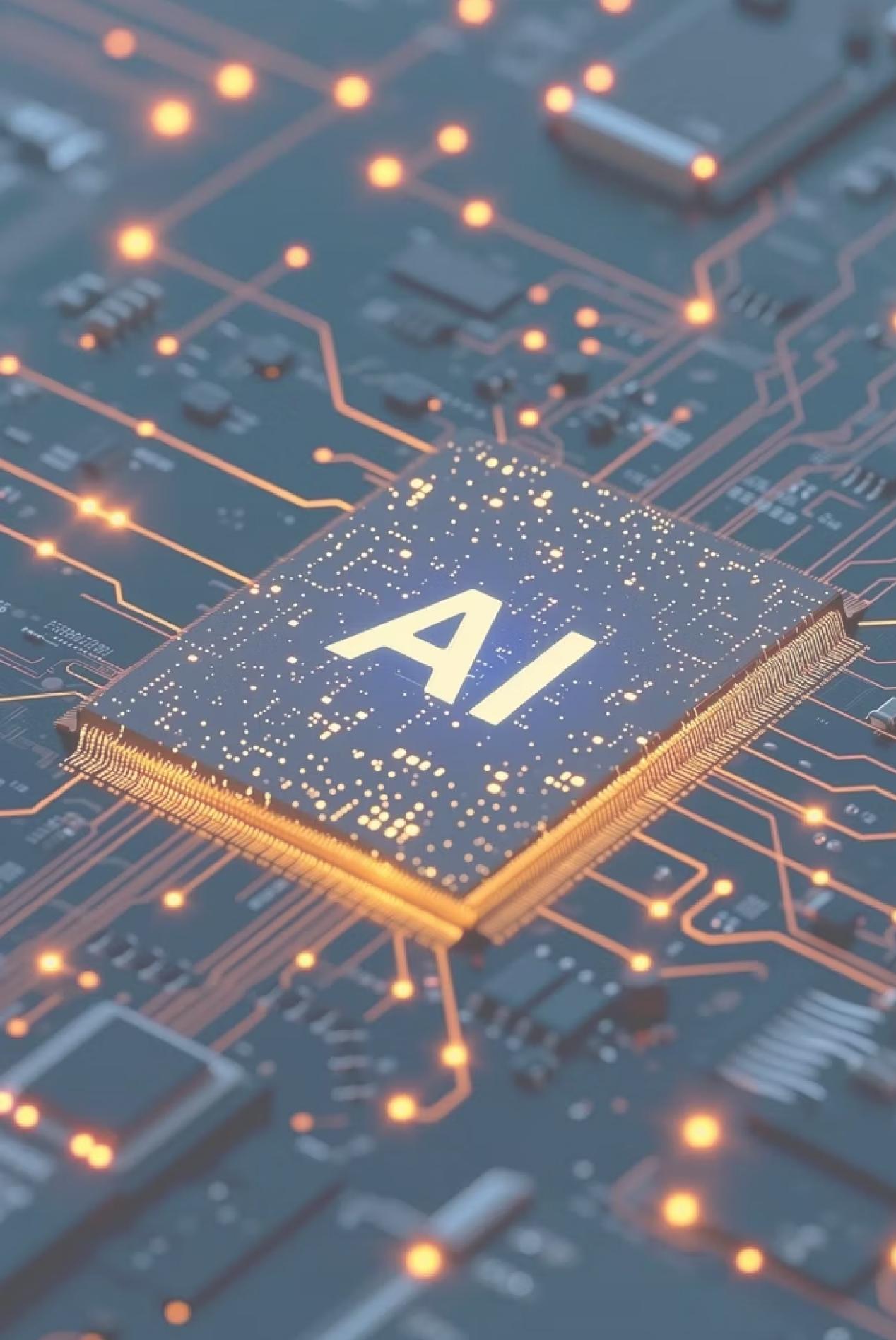
SDU - Teknologi forståelse (Legal  
Tech) 2023-2025



# Dagsorden

---

1. Indflyvning til AI fra et juridisk perspektiv
2. AI Act
  - Introduktion
  - Højrisiko-kravene
3. Det praktiske perspektiv og samarbejde mellem faggrupper



# AI fra et juridisk perspektiv

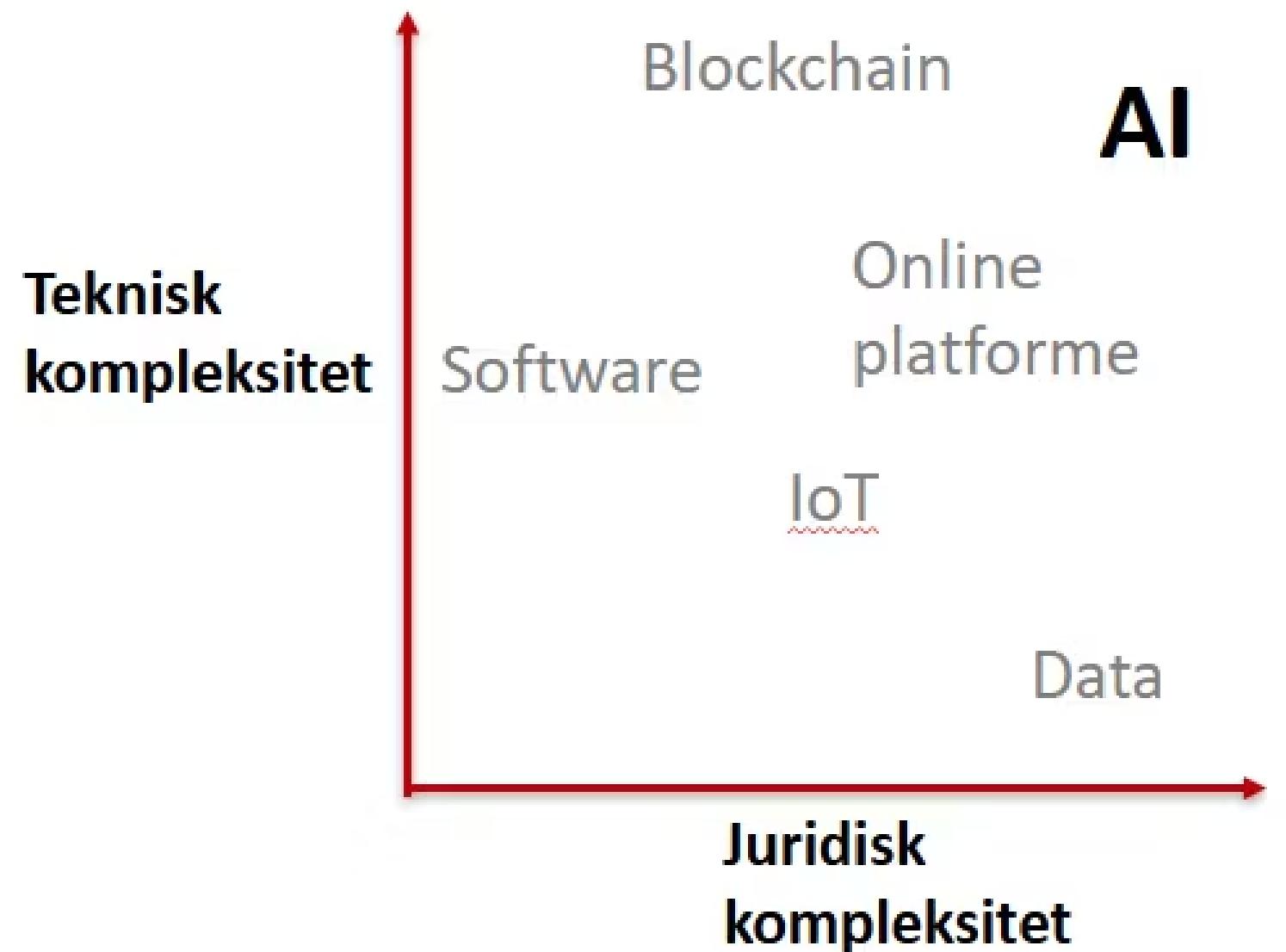
## Teknisk kompleksitet

- De fleste moderne AI løsninger består af **flere lag af digitale teknologier, som alle i sig selv giver juridiske udfordringer (software, data, cloud mv)**

## Juridisk kompleksitet

- AI bliver omfattet af en række **gældende regler**, men giver **nye udfordringer** (fx GDPR og ophavsret mv.)
- AI bliver herudover reguleret i en række **nye regler**

+ Løbende udvikling af teknologi og retskildebillede...



# AI er komplet...

## EU's "Digital Decade" – nye regler siden 2019

### Cybersikkerhed

- S: Cybersecurity Strategy
- F: Cybersecurity Act
- D: NIS2
- F: DORA (finanssektor)
- D: Critical Entities Resilience/CER
- F: Cybersecurity Regulation
- F: Cyber Resilience Act
- F: Cyber Solidarity Act
- F: Information Security Regulation

### Data (adgang og deling)

- S: Data Strategy
- F: Free Flow of Data
- D: Open Data
- F: Data Governance Act
- F: Data Act
- F: Interoperable Europe Act
- F: Data Collection and Sharing Relating to Short-Term Accommodation Rental Services Act
- F: European Health Data Space
- F: Financial Data Access

### Teknologier og ansvar

- S: AI Strategy + Blockchain Strategy
- F: Platform-to-Business forordning/P2B
- F: Digital Services Act
- F: Digital Markets Act
- F: MICA (kryptoaktiver)
- F: AI Act
- F: European Identity Wallet
- F: Machinery Regulation
- D: Product Liability Directive (revision)
- F: General Product Safety Regulation
- D: AI Liability Directive

#### Type af dokument

S = Strategi  
F = Forordning  
D = Direktiv

#### Status

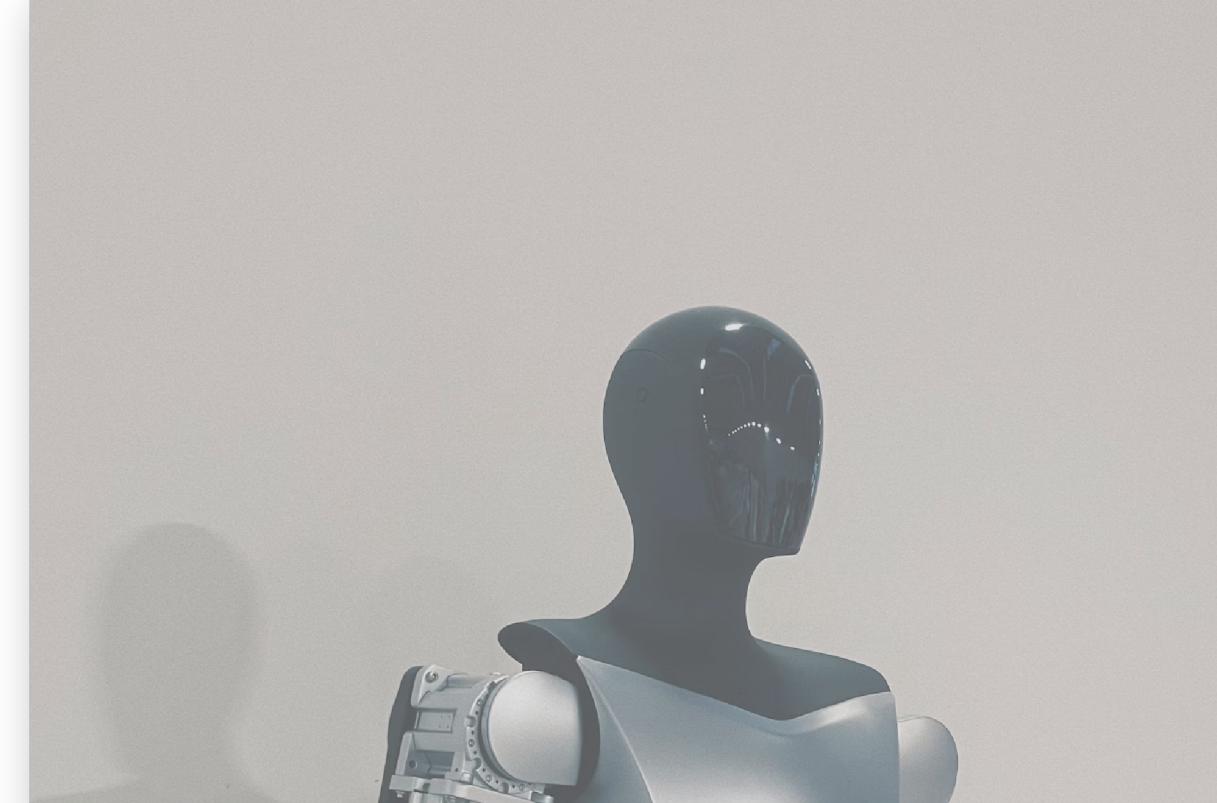
Almindelig tekst = Endeligt vedtaget  
(!) = Politisk enighed, endelig ordlyd mangler  
Blå = Forhandles pt. i EU  
Grå = Varslede regler/Impact Assessment

10

# AI er komplekst...

## Juridiske barrierer hæmmer idriftsættelse

Juridisk fortolkning og manglende klarhed om hjemler har været den næsthængste udfordring blandt AI-signaturprojekterne. Signaturprojekterne oplever ikke, at der er klarhed over, hvad der kan lade sig gøre inden for gældende rammer. Det er ofte op til den enkelte kommune eller region at for tolke et komplekst sæt af gældende og kommende regler og identificere potentielle muligheder. Denne usikkerhed skaber dels et stort ressourcetræk hos den enkelte myndighed, dels medfører det, at regler kan fortolkes forskelligt og give forskelle i retstilstand på tværs. Selvom der altid vil være behov for en konkret tolkning og risikovurdering hos den dataansvarlige myndighed, peger deltagerne i evalueringen på et behov for, at der fra central side sker en tydeligere vejledning om gældende regler og retspraksis.



## EVALUERING AF AI-SIGNATURPROJEKTER

På vegne af Digitaliseringsstyrelsen, Kommunernes Landsforening og Danske Regioner

NOVEMBER 2024



AI ACT

# AI Act / AI forordningen

---

- AI-forordningen, som regulerer ansvarlig brug af kunstig intelligens i Europa, er den første lovgivning i verden på dette område.
- Relevant for mange – men stor forskel på, hvem der skal vide hvad.

## Overskrifter

Vedtaget **sommer 2024**, og herefter **trinvis ikrafttræden** fra februar 2025 og frem.

- **113** artikler og **13** bilag
- Krav afhænger af **risiko** – særligt tunge krav til højrisiko AI samt udbydere af AI modeller til generel brug (ChatGPT mv)
- Forpligtelser for både **leverandører** ("*udbyder*") og **kunder** ("*idriftsætter*")
- **Håndhævelse** nationalt (Digitaliseringsstyrelsen, Datatilsynet mfl.) og på EU-plan ("European AI Board" og "AI Office")

Titel	Artikler
CHAPTER I: GENERAL PROVISIONS	Art. 1 - 4
CHAPTER II: PROHIBITED ARTIFICIAL INTELLIGENCE PRACTICES	Art. 5
CHAPTER III: HIGH-RISK AI SYSTEMS	Art. 6 - 49
CHAPTER IV: TRANSPARENCY OBLIGATIONS FOR PROVIDERS AND DEPLOYERS OF CERTAIN AI SYSTEMS	Art. 50
CHAPTER V: GENERAL PURPOSE AI MODELS	Art. 51 - 56
CHAPTER VI: MEASURES IN SUPPORT OF INNOVATION	Art. 57 - 63
CHAPTER VII: GOVERNANCE	Art. 64 - 70
CHAPTER VIII: EU DATABASE FOR HIGH-RISK AI SYSTEMS LISTED IN ANNEX III	Art. 71
CHAPTER IX: POST-MARKET MONITORING, INFORMATION SHARING, MARKET SURVEILLANCE	Art. 72 - 94
CHAPTER X: CODES OF CONDUCT AND GUIDELINES	Art. 95 - 96
CHAPTER X: DELEGATION OF POWER AND COMMITTEE PROCEDURE	Art. 97 - 98
CHAPTER XI: PENALTIES	Art. 99 - 101
CHAPTER XII: ENTRY INTO FORCE AND APPLICATION	Art. 102 - 113
ANNEX I-XIII	N/A

## EU AI Act: A Risk-Based Approach



Art. 53 - AI-modeller  
til almen brug

# Overblik over forordningens forpligtelser

Forpligtelse	Artikler	Uddybning	Pliktsubjekter	Ikrafttræden
AI-færdigheder (literacy)	4	Overblik over AI-systemer, målrettet uddannelse i risici og AI Act, risikovurderinger mv	Udbydere og idriftsættere	2. februar 2025
Forbudte AI-praksisser	5	Hvis brugen af AI falder indenfor de oplistede cases, er det forbudt	Udbydere og idriftsættere	2. februar 2025
Højrisiko	6-49	Efterlevelse af materielle krav til AI-systemet (art. 9-15), kvalitetsstyring (art. 17) samt udarbejdelse af relevant dokumentation mv (art. 16-50)	Udbydere og idriftsættere - flest forpligtelser på udbydere	2. august 2026 (dog 2027 fsva. Annex I)
Gennemsigtighed	50	Der skal fremgå klart, når en bruger interagere med AI	Udbydere og idriftsættere	2. august 2026
AI-modeller til generel brug	51-56	Skærpede krav til udbydere af AI-modeller til generel brug (GPT 4.0 mv)	Udbydere af de helt store modeller (OpenAI, Google, Meta mv)	2. August 2025

# Overblik over forordningens forpligtelser

Forpligtelse	Artikler	Uddybning	Pligtsubjekter	Ikrafttræden
AI-færdigheder (literacy)	4	Overblik over AI-systemer, målrettet uddannelse i risici og AI Act, risikovurderinger mv	Udbydere og idriftsættere	2. februar 2025
Forbudte AI-praksisser	5	Hvis brugen af AI falder indenfor de oplistede cases er det forbudt	Udbydere og idriftsættere	2. februar 2025
Højrisiko	6-49	Efterlevelse af materielle krav til A-systemet (art. 9-15), kvalitetssikring (art. 17) samt udarbejdelse af relevant dokumentation mv (art. 16-50)	Udbydere og idriftsættere - flest forpligtelser på udbydere	2. august 2026 (dog 2027 fsva. Annex I)
Gennemsigtighed	50	Der skal fremgå klart, når en bruger interagere med AI	Udbydere og idriftsættere	2. august 2026
AI-modeller til generel brug	51-56	Skærpede krav til udbydere af AI-modeller til generel brug (GPT 4.0 mv)	Udbydere af de helt store modeller (OpenAI, Google, Meta mv)	2. August 2025

# AI Act art. 4 - "AI færdigheder"

---

*"Uddydere og idriftsættere af AI-systemer træffer **foranstaltninger** til i videst muligt omfang at sikre et **tilstrækkeligt niveau af AI-færdigheder** hos deres personale og andre personer, der er involveret i drift og anvendelse af AI-systemer på deres vegne, og tager herved hensyn til disse personers **tekniske viden, erfaring og uddannelse** og den **kontekst, hvori AI-systemerne skal anvendes**, og de personer eller grupper af personer, som AI-systemerne skal anvendes på."*

## Konkretisering af kravet:

- Kommissionens FAQ fra maj 2025 ([link](#))
- Et "inspirationskatalog" publiceret af EU-Kommissionen ([link](#))
- Specifikation fra Dansk Standard ([link](#))

# Kommissionens Q&A fra maj 2025 – Uddrag:

---

## ***“What should be the minimum content to consider for an AI literacy programme complying with article 4 of the AI Act?”***

The AI Office will not impose strict requirements regarding Article 4 of the AI Act and its “sufficient level of AI literacy”. On the contrary, it considers necessary a certain degree of flexibility, considering the broad topic of AI literacy and the fast-evolving technology that AI is.

### ***Yet, as a minimum, to comply with Article 4 of the AI Act, providers and deployers of AI systems should:***

- a) Ensure a general understanding of AI within their organisation:*** What is AI? How does it work? What AI is used in our organisation? What are its opportunities and dangers?
- b) Consider the role of their organisation (provider or deployer of AI systems):*** Is my organisation developing AI systems or just using AI systems developed by another organisation?
- c) Consider the risk of the AI systems provided or deployed...***
- d) Concretely build their AI literacy actions on the preceding analysis, considering differences in technical knowledge, experience, education and training of the staff and other persons...***

***Considerations a, b, c, and d include legal and ethical aspects. Therefore, connections to the EU AI regulation (i.e., understanding of the AI Act) and to principles of ethics and governance are encouraged.”***

# Kommissionens Q&A fra maj 2025 – Uddrag:

---

**“Does the Commission already have a plan to put in place Article 4 of the AI Act in terms of its own employees?**

The AI@EC Communication already identified as operational action to Develop a policy to build and maintain an AI-skilled workforce. The European Commissions has already implemented several measures for its staff regarding AI literacy:

- The creation of **internal AI specific web portal** as one-stop shop accessible to all staff to the AI related content - AI guidelines, AI training resources, events, and news.
- **Definition on the Commission training platform of AI learning packages**, oriented to different targets - generalist, managers, and developers (specialist). These packages contain a curated list of relevant trainings, categorising them on essential, highly recommended and recommended. Additional trainings and recording of webinars are available also in the platform.
- AI tools trainings - **Specific section in the AI portal list the AI tools**, available to all staff has been created that includes the relevant learning resources for each tool. There are periodic Q&A sessions on using AI in your daily work.
- An **AI community of practice** exists where any person can do questions related to AI and interact with AI experts.”

# Eksempel - dansk standard (Idriftssætter)

## Step 1: Identifier relevante grupper af medarbejdere

- Ledelse
- System ejer
- Driftsmedarbejder
- Slutbruger

## Step 2: Konkret risikovurdering af AI-systemet

- kombinationen af sandsynligheden for, at der opstår en skade, og den pågældende skades alvor.

## Step 3: Tekniske praktiske og etiske færdigheder

**Tekniske færdigheder** handler om den grundlæggende viden om AI, fx forståelse for hvordan systemerne er udviklet, at systemet gør en forskel, hvilke datakilder man bruger og hvordan data vægtes, tolkes og præsenteres.

**Praktiske færdigheder** handler om at kunne anvende et specifikt system. Dvs. hvordan man anvender systemet, hvilke opgaver man må og ikke må løse med systemet. Dertil hvilke forholdsregler man bør tage i den aktuelle kontekst, som systemet skal fungere i.

**Etiske færdigheder** handler om at have forståelse for, om brugeren af et specifikt AI-system giver implikationer for mennesker og samfund. Ligeledes er det vigtigt, at slutbrugeren i sine tilbagemeldinger om brug af systemet kan reflektere over etiske problemstillinger.

# Andre interessante elementer fra Kommissionens Q&A

**When will the enforcement start? Is a company already late/at risk if it has not yet an established AI literacy initiative?**

Article 4 of the AI Act entered into application on **2 February 2025**, therefore the obligation to take measures to ensure AI literacy of their staff already applies. The supervision and enforcement rules apply from **3 August 2026** onwards.

**Does a company, whose employees are using ChatGPT for, e.g., writing advertisement text or translating text, need to comply with the AI literacy requirement of Article 4 of the AI Act?**

**Yes, they should be informed about the specific risks, for example hallucination**

**How do organisations have to document their actions to comply with article 4 of the AI Act and the best effort provisions in it? Do they need specific certificates?**

**There is no need for a certificate. Organisations can keep an internal record of trainings and/or other guiding initiatives.**

# Hvilke risici?

---

**Krav om AI-færdigheder har bl.a. til formål at minimere risici/skader relateret til:**

- Sundhed
- Sikkerhed, inkl. cybersikkerhed
- Grundlæggende rettigheder som defineret i EU's charter
- Manglende overholdelse af krav i AI Act eller anden regulering

# Hvilke risici?

---

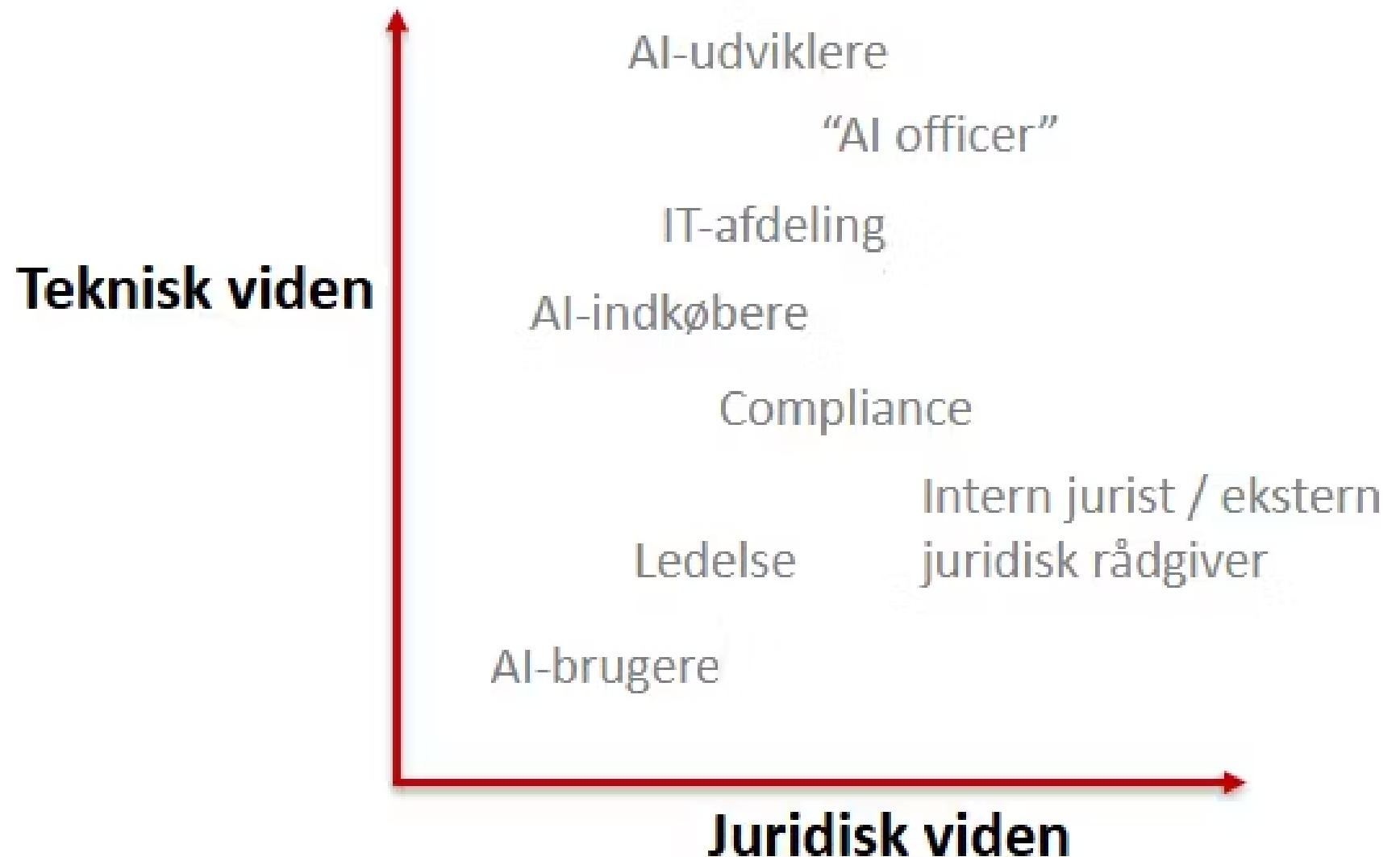
## Konkrete eksempler på risici

- Hallucinationer
- Målrettede hackerangreb, fx "Model Inversion Attacks" og "AI-agent-assisted Cyberattacks"
  - F.eks. <https://www.anthropic.com/news/disrupting-AI-espionage>
- Utilsigtet deling af fortrolige oplysninger fx forretningshemmeligheder
  - <https://www.forbes.com/sites/siladityaray/2023/05/02/samsung-bans-chatgpt-and-other-chatbots-for-employees-after-sensitive-code-leak/>
- Krænkelse af andres rettigheder, fx ophavsret til billeder eller lyd
- Overtrædelse af anden lovgivning, fx GDPR eller forvaltningsregler

# Teknisk og juridisk viden

---

- **Teknisk viden**
- Fx om konkrete løsninger, usecases, integration til øvrige IT-systemer, bagvedliggende modeller, datagrundlag, cybersikkerhed, potentielle bias mv.
- **Juridisk viden**
- Fx om AI Act, GDPR, sektorregulering, relevante standarder, officielle vejledninger, kontraktmæssige krav mv
- **Brobygning**
- Vi skal, også i relation til AI, væk fra silo-tilgangen!



Stilling	Ansvar (eksempler)	Behov for viden
Ledelsen	Overordnet ansvar for risikostyring inkl. overholde lovgivning	Overordnet viden om <b>muligheder, trusler og regulering</b> + <b>organisatorisk forankring</b>
AI-udviklere (internt)	"Compliance by Design" = Sikre at løsningen fra start lever op til relevante lovkrav	Primært <b>teknisk</b> , men også forståelse for <b>konkrete lovkrav</b> (GDPR, AI Act mv) + tilhørende standarder, vejledninger mv
Indkøber af AI systemer	Forstå forretningsmæssigt behov. Sikre relevante kontraktmæssige krav.	Konkret <b>viden om den konkrete AI-løsning + relevante lovkrav</b>
Bruger af AI systemer	Ansvarlig brug af AI-løsninger, herunder overholde retningslinjer mv	Konkret <b>retningslinjer for brug</b>
IT / cybersikkerhed	Afdække samspil med organisationens generelle IT-miljø og drift, herunder politikker for cybersikkerhed	<b>Overblik over AI-løsninger i brug + viden om AI-specifikke risici</b>
Intern jurist / ekstern juridisk rådgiver	Afklaring af juridiske spørgsmål, fx overblik over relevante lovkrav, samspil mellem regelsæt, vurdering af konkret usecase mv	Primært <b>juridisk</b> , men også behov for <b>en vis teknisk forståelse</b>
Compliance	Tænke AI-governance ind i organisationens eksisterende governance-framework samt sikre løbende opfølgning og dokumentation, herunder for menneskeligt tilsyn	Behov for <b>en vis teknisk og juridisk forståelse</b>
"AI officer"	En stilling som bliver stadigt mere udbredt internationalt. Overordnet ansvar for strategi, drift og lovlighed af AI-løsninger.	Behov for <b>ekspertviden ift. det tekniske</b> , og også <b>dyb viden om jura</b>

# Overblik over forordningens forpligtelser

Forpligtelse	Artikler	Uddybning	Pligtsubjekter	Ikrafttræden
AI-færdigheder (literacy)	4	Overblik over AI-systemer, målrettet uddannelse i risici og AI Act, risikovurderinger mv.	Udbydere og idriftsættere	2. februar 2025
Forbudte AI-praksisser	5	Hvis brugen af AI falder indenfor de oplistede cases er det forbudt	Udbydere og idriftsættere	2. februar 2025
Højrisiko	6-49	Efterlevelse af materielle krav til A-systemet (art. 9-15), kvalitetssikring (art. 17) samt udarbejdelse af relevant dokumentation mv (art. 16-50)	Udbydere og idriftsættere - flest forpligtelser på udbydere	2. august 2026 (dog 2027 fsva. Annex I)
Gennemsigtighed	50	Der skal fremgå klart, når en bruger interagere med AI	Udbydere og idriftsættere	2. august 2026
AI-modeller til generel brug	51-56	Skærpede krav til udbydere af AI-modeller til generel brug (GPT 4.0 mv)	Udbydere af de helt store modeller (OpenAI, Google, Meta mv)	2. August 2025

# Forbudte AI-praksisser

a) Bevidst manipulation

b) Udnyttelse af sårbarheder

c) Social bedømmelse

d) Risikovurderinger af fysiske personer

e) Oprettelse eller udvidelse af ansigtsgenkendelsesdatabaser

f) Udledning af følelser på arbejdspladser og uddannelsesinstitutioner

g) Biometrisk kategorisering

h) Biometerisk fjernidentifikation i realtid på offentlige steder



# Overblik over forordningens forpligtelser

Forpligtelse	Artikler	Uddybning	Pligtsubjekter	Ikrafttræden
AI-færdigheder (literacy)	4	Overblik over AI-systemer, målrettet uddannelse i risici og AI Act, risikovurderinger mv.	Udbydere og idriftsættere	2. februar 2025
Forbudte AI-praksisser	5	Hvis brugen af AI falder indenfor de oplistede cases er det forbudt	Udbydere og idriftsættere	2. februar 2025
Højrisiko	6-49	Efterlevelse af materielle krav til AI-systemet (art. 9-15), kvalitetssikring (art. 17) samt udarbejdelse af relevant dokumentation mv (art. 16-50)	Udbydere og idriftsættere - flest forpligtelser på udbydere	2. august 2026 (dog 2027 fsva. Annex I)
Gennemsigtighed	50	Der skal fremgå klart, når en bruger interagere med AI	Udbydere og idriftsættere	2. august 2026
AI-modeller til generel brug	51-56	Skærpede krav til udbydere af AI-modeller til generel brug (GPT 4.0 mv)	Udbydere af de helt store modeller (OpenAI, Google, Meta mv)	2. August 2025

# Højrisiko-AI systemer

## Bilag I (produktsikkerhedslovgivning)

1. Maskiner

7. Trykbærende udstyr

2. Legetøj

8. Tovbaneanlæg

3. Fritidsfartøjer og personlige fartøjer

9. Personlige værnemidler

4. Elevatorer

10. Gasapparater

5. Sikringssystemer til eksplosiv atmosfære

11. Medicinsk udstyr

6. Radioudstyr

12. In vitro-diagnostik

## Bilag III (anvendelsesområder)

1. Biometri

7. Migration, asyl og grænseforvaltning

2. Sikkerhed i kritisk infrastruktur

5. Væsentlige offentlige tjenester og ydelser

3. Uddannelse

6. Retshåndhævelse

4. Beskæftigelse

8. Retspleje og demokrati



Digitaliseringsstyrelsen

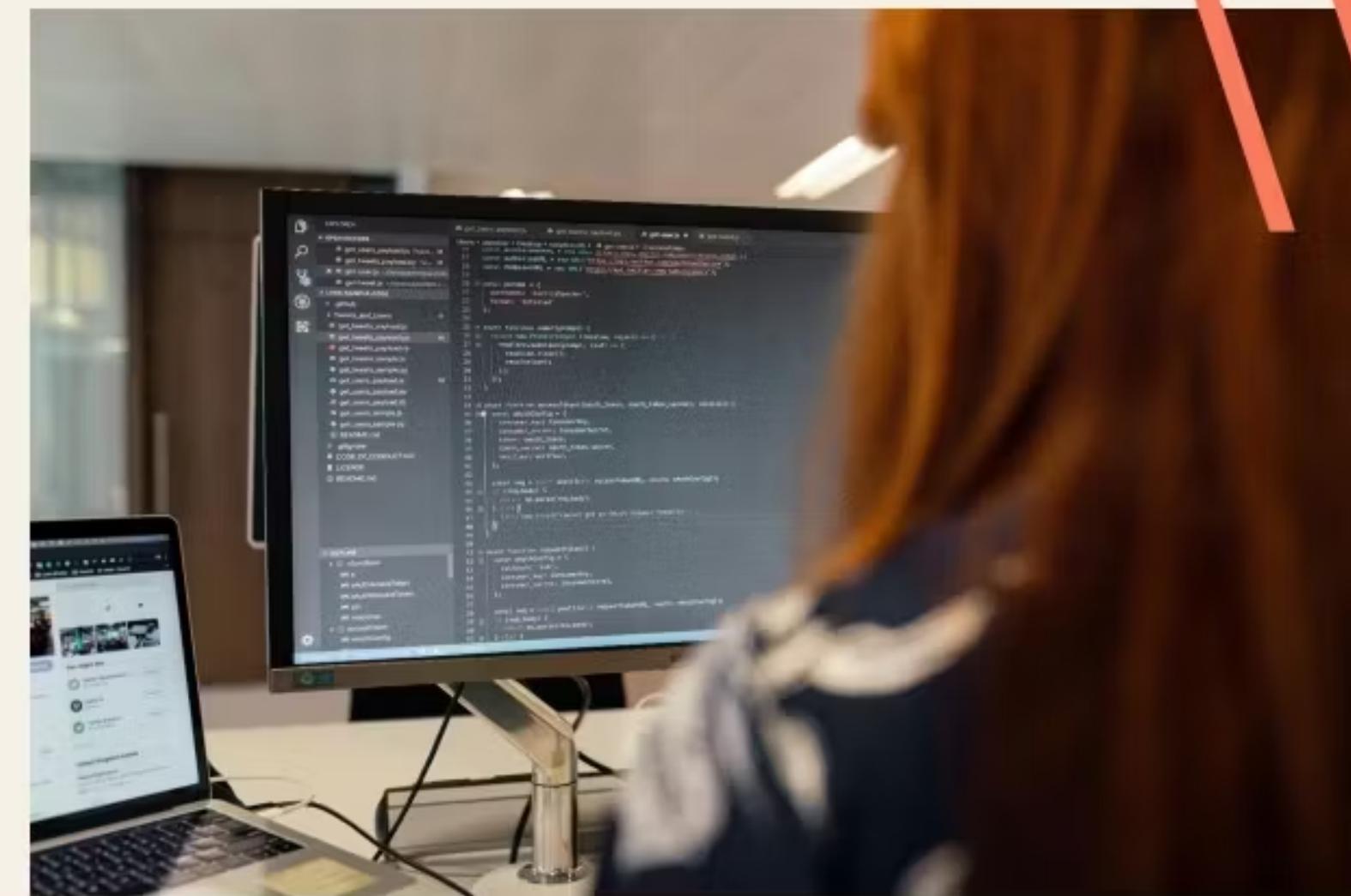
# Højrisiko-AI systemer - pligter for “providers”

## Forpligtelser (art. 9-22)

Risikostyring (art. 9)	Data og datastyring (art. 10)	Teknisk dokumentation (art. 11 / bilag IV)
Registrering af hændelser (art. 12)	Transparens og information til idriftsættere (art. 13)	Menneskeligt tilsyn (art. 14)
Nøjagtighed, robusthed og cybersikkerhed (art. 15)	Kvalitetsstyrings-system (art. 17)	Rapportering af hændelser (art. 20)

\*Ikke udtømmende liste af krav mv. på siden

Kilde: Digitaliseringsstyrelsen



OBS!

*Fra idriftsætter til udbyder*

- a) anbringer eget navn eller varemærke,
- b) foretager væsentlig ændringer eller
- c) ændrer tilsigtede formål med AI-system



# I. AI Act: Main Operational Elements

New Legislative Framework (NLF)

Product Safety Legislation +



Sets

Mandatory Requirements  
for high-risk AI system  
before they can be used



Provides for

Presumption of conformity  
if AI high risk AI system is  
in compliance with  
harmonized standards



risks to health, safety and  
fundamental rights

1. **risk management system** for AI systems *[Art. 9 AI Act]*
2. **governance and quality of datasets** used to build AI systems *[Art. 10 Data and data governance]*
3. **record keeping** - built-in logging capabilities in AI systems *[Art. 11 Technical documentation and Art. 12 record-keeping]*
4. **transparency and information** to the users of AI systems *[Art. 13 Transparency and provisions of information to users]*
5. **human oversight** of AI systems *[Art. 14 Human oversight]*
6. **accuracy** specifications for AI systems *[Art. 15 Accuracy, robustness and cybersecurity]*
7. **robustness** specifications for AI systems *[Art. 15 Accuracy, robustness and cybersecurity]*
8. **cybersecurity** specifications for AI systems *[Art. 15 Accuracy, robustness and cybersecurity]*
9. **quality management system** for providers of AI system *[Art. 17]*
10. **conformity assessment** for AI systems *[Art. 19 + Art. 43 Conformity Assessment]*



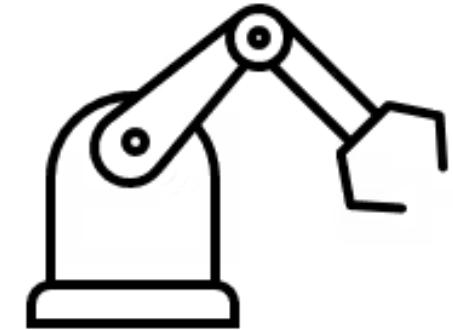
# Hvad er New Legislative Framework?

---

"New Legislative Framework" er i stor omfang en videreførelse af "New Approach" fra 1985, der fastsatte følgende principper:

- Harmoniseringslovgivning begrænses til udelukkende, at indeholde **de væsentlige krav**, som produkter på det indre marked skal opfylde.
- De konkrete **tekniske specifikationer** for produkterne som omtalt i lovgivningen, stilles i **harmoniserede standarder**, der kan anvendes parallelt med lovgivningen.
- Der gælder en **formodning om overensstemmelse** - Produkter, der er fremstillet i overensstemmelse med **harmoniserede standarder**, formodes at være i overensstemmelse med den gældende lovgivning

# Eksempel på samspil: Kirurgisk robotarm



- Høj-risiko AI system der er et sikkerhedskomponent for en robotarm, der anvendes til kirurgi på et hospital. Robotarmen anvender et 5G radiosignal.
- Robotarmen vil omfattes af flere regelsæt:

Medical Device  
Regulation  
(2017/745)

Article 10  
**General obligations of manufacturers**

Article 52  
**Conformity assessment procedures**

Radio Equipment  
Directive

Article 10  
**Obligations of manufacturers**

Article 17  
**Conformity assessment procedures**

Machinery Regulation

Article 10  
**Obligations of manufacturers of machinery and related products**

Article 21  
**EU declaration of conformity of machinery and related products**

Article 22  
**EU declaration of incorporation of partly completed machinery**

AI ACT

Article 16  
**Obligations of providers of high-risk AI systems**

(Providers of high-risk AI systems shall:  
...)

(e) ensure that the high-risk AI system undergoes the relevant conformity assessment

procedure as referred to in Article 43, prior to its placing on the market or putting into service

Article 43  
**Conformity assessment**

# Højrisiko-AI systemer - pligter for “deployers”

## Forpligtelser (art. 26)

Følg brugsanvisning	Menneskeligt tilsyn med nødvendige kompetencer	Hvis kontrol med inputdata = sikre relevant data ift. formål
Overvåg drift af systemet og underret hvis risiko og hændelser	Opbevar logfiler (hvis under idriftsætters kontrol)	Informér medarbejdere hvis systemet anvendes på arbejdsplads
Underret personer hvis AI-systemet bruges til beslutninger	Konsekvensanalyse vedr. persondata (DPIA)	

\*Ikke udtømmende liste af krav mv. på siden

Særligt for offentlige myndigheder, banker og forsikring

Konsekvensanalyse for grundlæggende rettigheder  
(art. 27)

Sikre registrering af AI-systemet i EU-database  
(off. myndigheder, art. 49)



# Spørgsmål

---

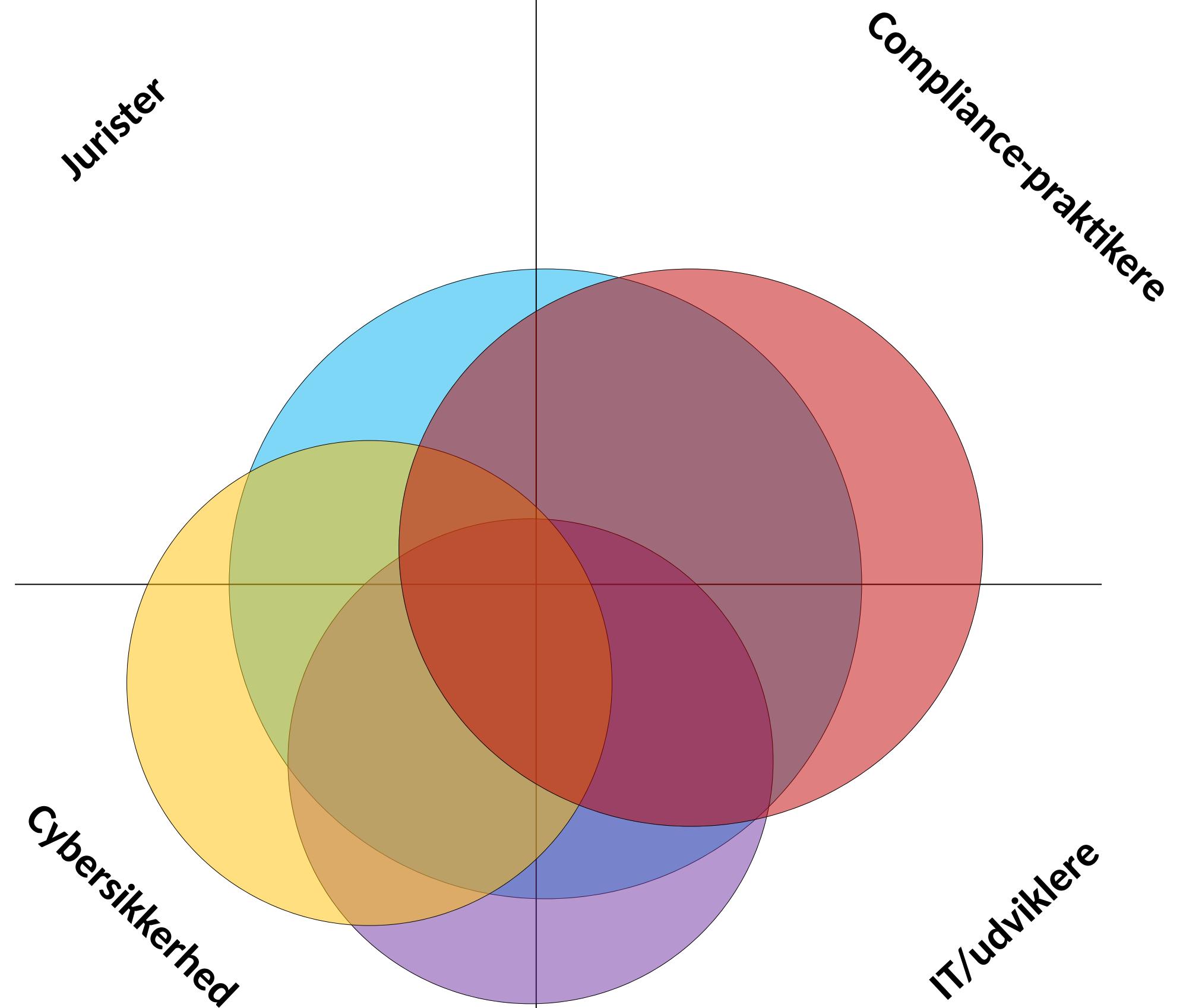
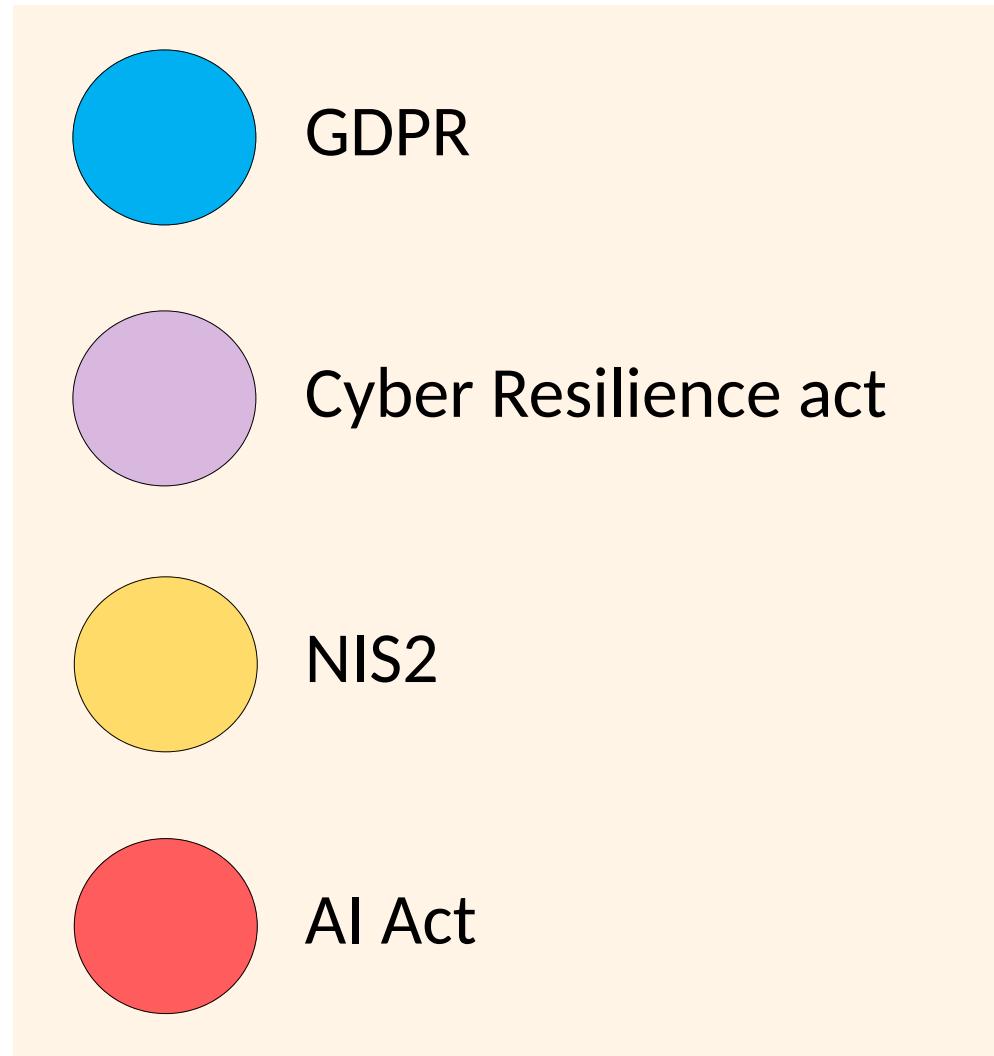
- Hvilke fordele og ulemper kan der være ved at regulere kunstig intelligens som vi gør det i Europa?

Til sammenligning:

- I USA reguleres/kontrolleres udviklingen af AI i mindre omfang end i EU.
- I Kina reguleres/kontrolleres udviklingen af AI i større omfang end i EU.

# DET PRAKTISKE PERSPEKTIV OG SAMARBEJDE MELLEM FAGGRUPPER

# Digital regulering og behovet for forskellige kompetencer



# Opgaver til forskellige faggrupper – AI Act

Regelsæt	"Compliance-praktikere"*	Udviklere / Data Scientists	Cybersikkerhed	Jurister
AI Act	<ul style="list-style-type: none"><li>• "High Risk": Dokumentation for efterlevelse af krav inkl. risikostyring, kvalitetsledelse, 'conformity assessments', teknisk dokumentation, logning, "Human Oversight" mv, herunder kommende EU-standarder</li><li>• Øvrige: Efterleve kommende Codes of Conduct (overlap med High Risk)</li><li>• Kontroller, herunder for bias</li></ul>	<ul style="list-style-type: none"><li>• Data Governance</li><li>• Security by Design</li><li>• Implementering af standarder i de udviklede løsninger</li><li>• Test af løsninger</li><li>• (Kommende EU-standarder i regi af AIA, fx om Data Governance)</li></ul>	<ul style="list-style-type: none"><li>• AI-specifikke trusselsvurderinger</li><li>• (Informationssikkerhedsledelse (fx ISO 27001))</li><li>• (Kommende EU-standard i regi af AIA art. 15 om "cybersecurity")</li></ul>	<ul style="list-style-type: none"><li>• Juridisk fortolkning, herunder vurdering af scope, lovlighed og/eller ansvar</li><li>• Fundamental Rights Impact Assessments</li><li>• Kontrakter med leverandører (AlaaS, implementeringspartner, konsulenter, drift mv)</li><li>• Samarbejdsaftaler (fx fælles AI-projekter, data-puljing mv) og AI-politikker.</li><li>• Samspil med anden regulering, herunder GDPR samt EU's øvrige regler om produktsikkerhed (NLF)</li><li>• Dialog med tilsynsmyndigheder</li></ul>

# Spørgsmål

---

- Gå sammen i grupper i diskutér med jeres sidemand, hvilken rolle I tror at lovregulering kommer til at betyde for jeres arbejde i fremtiden, samt hvilke udfordringer I evt. ser relateret hertil?