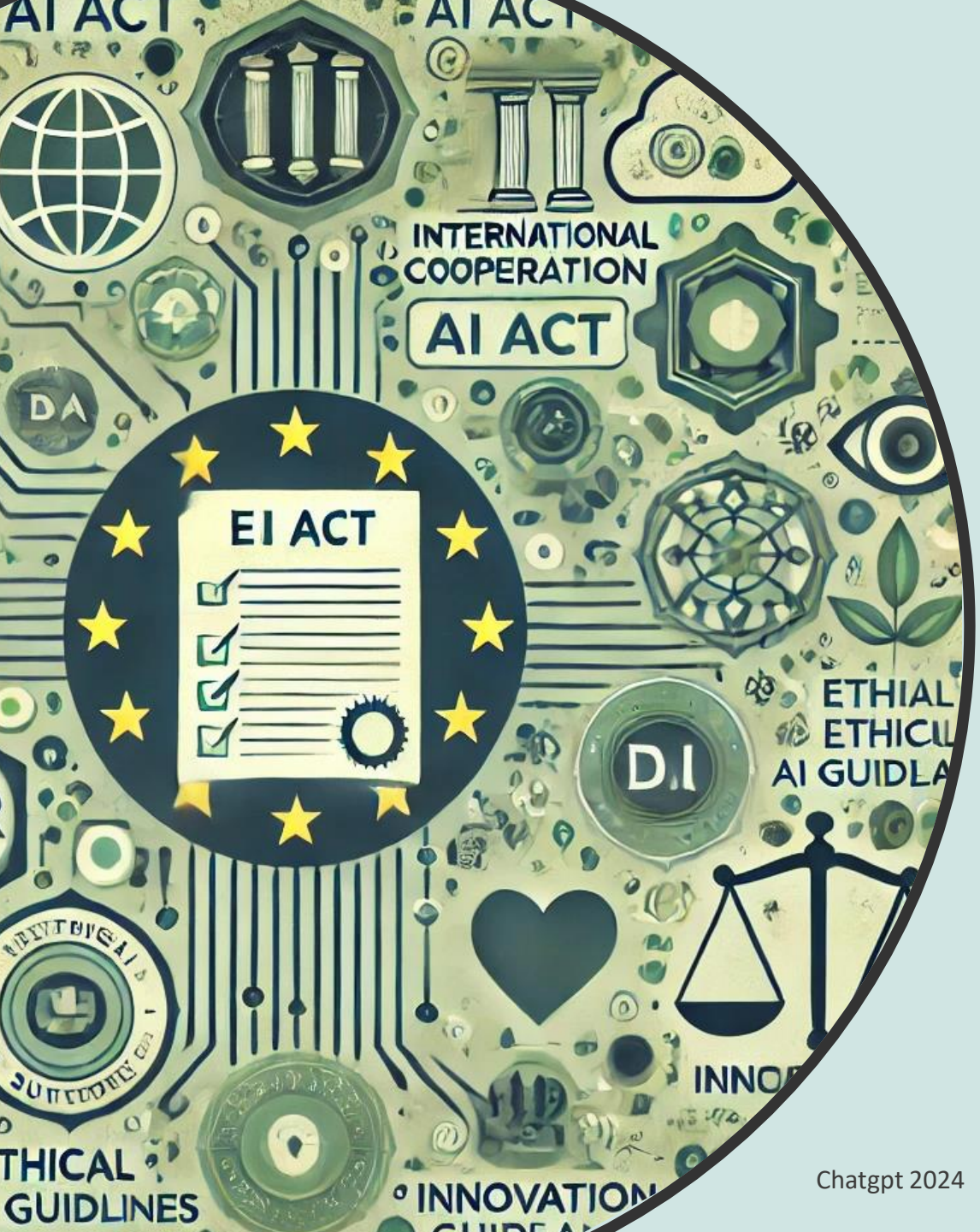


Chatgpt 2024

Hva er EU AI Act?

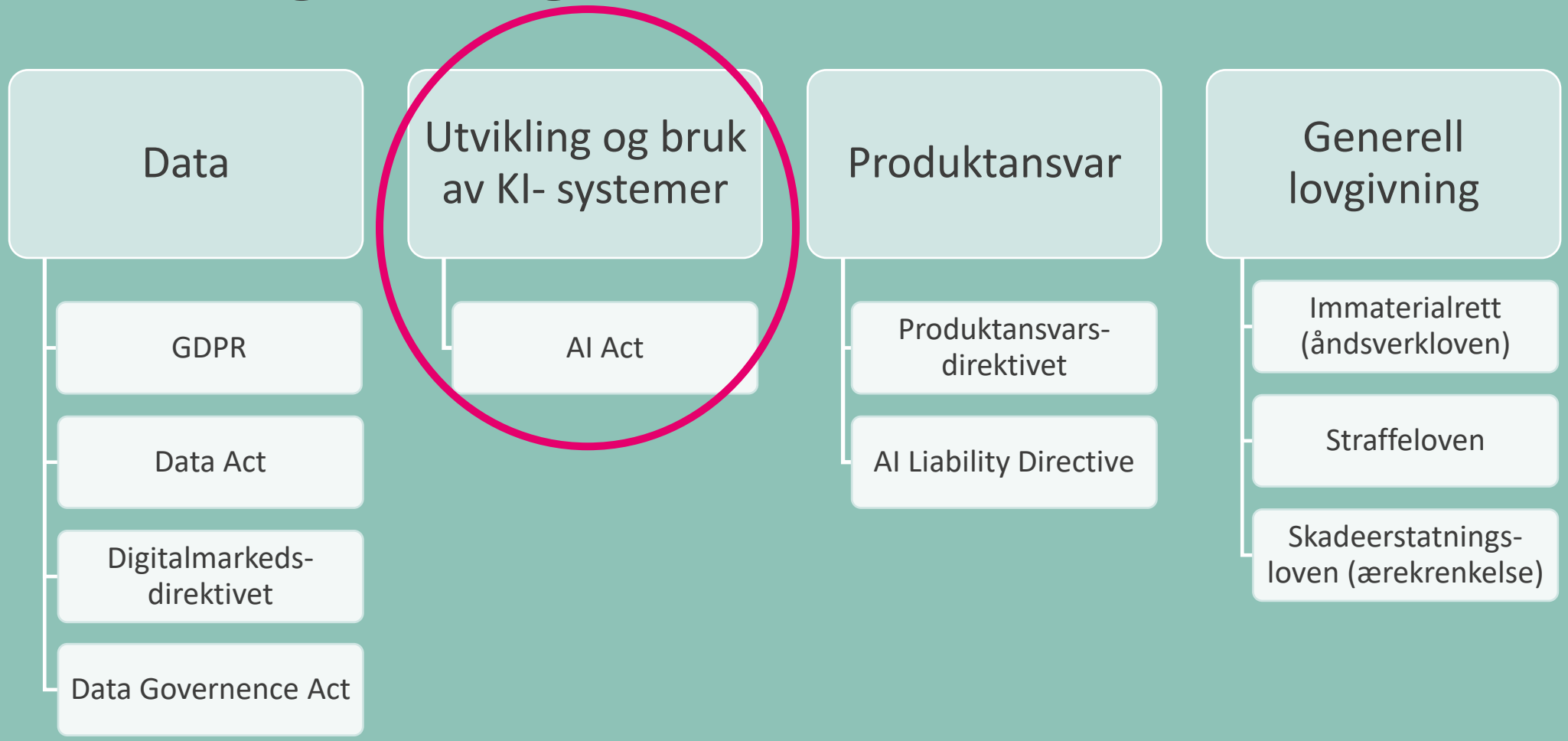
Fylkesbiblioteket i Akershus, Buskerud og Østfold,
29. oktober 2024

Lisa Digernes og Thale C. G. Gjerdsbakk

BULL

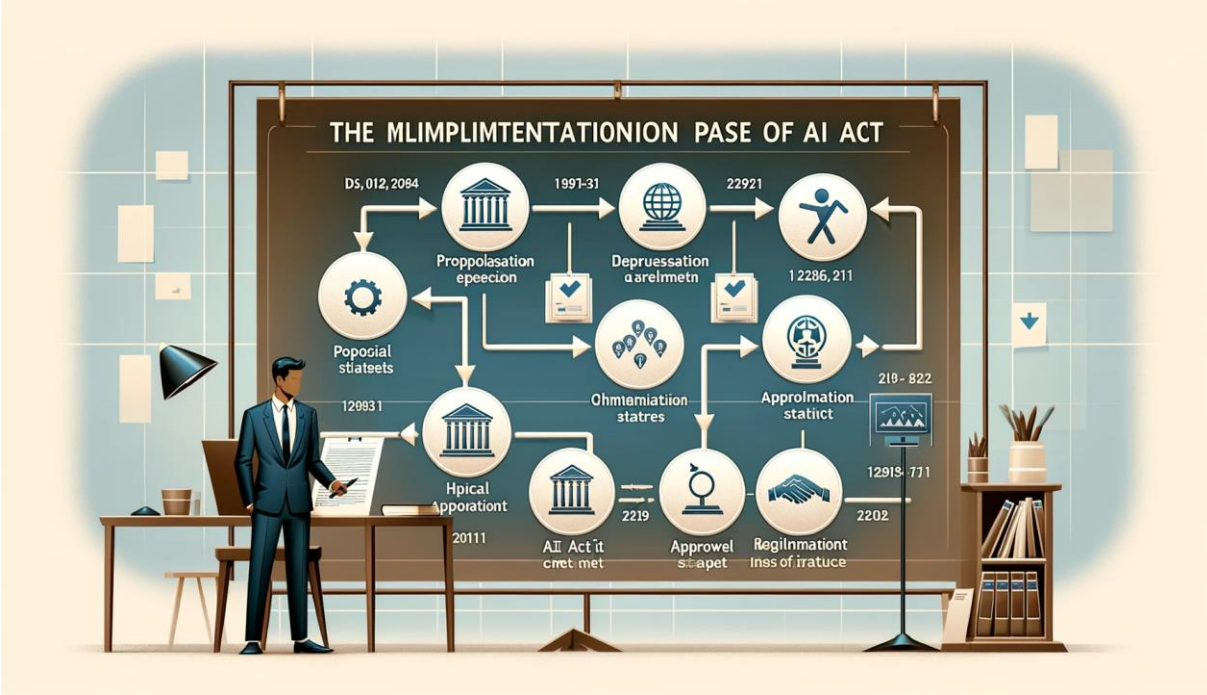
Regelutviklingen

AI regulering i EU – mer enn bare AI Act



Implementering – når trer reglene i kraft?

- Trådte i kraft 1. august
  - 13. mars 2024: Europaparlamentet vedtok AI Act eller KI Forordningen. Trer i kraft **20 dager etter publikasjon** i Offical Journal 12. juli 2024.
- Utgangspunkt (kapittel XIII!):
  - AI Act får virkning 24 mnd etter at forordningen trer i kraft, altså 1. august 2026
- Noen unntak:
  - Forbud mot KI-systemer med **uakseptabel risiko - 6 måneder (1. februar 2025)**
  - Kravene knyttet til **GPAI - generelle KI-systemer** - **12 måneder (1. august 2025)**
  - Kravene knyttet til **høyrisikosystemer** - **36 måneder (1. august 2027)**
- EØS-relevant
  - Får virkning i Norge i løpet av første halvdel 2026 (dep)



DALL*E, 2024

Roller

Leverandør

Påse at systemet oppfyller kravene til høyrisikosystemer i kap. 2.2 og at systemet har gjennomgått konformitetskontroller og oppnådd CE-merking før det markedsføres
Påse at det finnes kvalitetskontrollsystem og rutiner for oppbevaring av dokumentasjon
Påse at systemet er registrert

Importører

Verifisere at systemet overholder AI Act gjennom å

- kontrollere at det har gjennomgått konformitetskontroll
- At det foreligger teknisk dokumentasjon i henhold til kravene i Annex IV
- At systemet har CE-merking
- At leverandøren har en representant i EU etter Art. 22.

Distributører

Verifisere systemets CE-merking og at importør og leverandør har oppfylt sine plikter.
Ansvar for at systemet ikke lagres/brukes på en måte som skader dets egenskaper under kap. 2.2

Tredjeparter

Vil anses som «leverandør» dersom de

- Plasserer eget varemerke på systemet
- Modifiserer systemet eller godkjent bruk/formål

OBS, dette er husoversettelser

Men hva med de som *bruker* slike systemer?

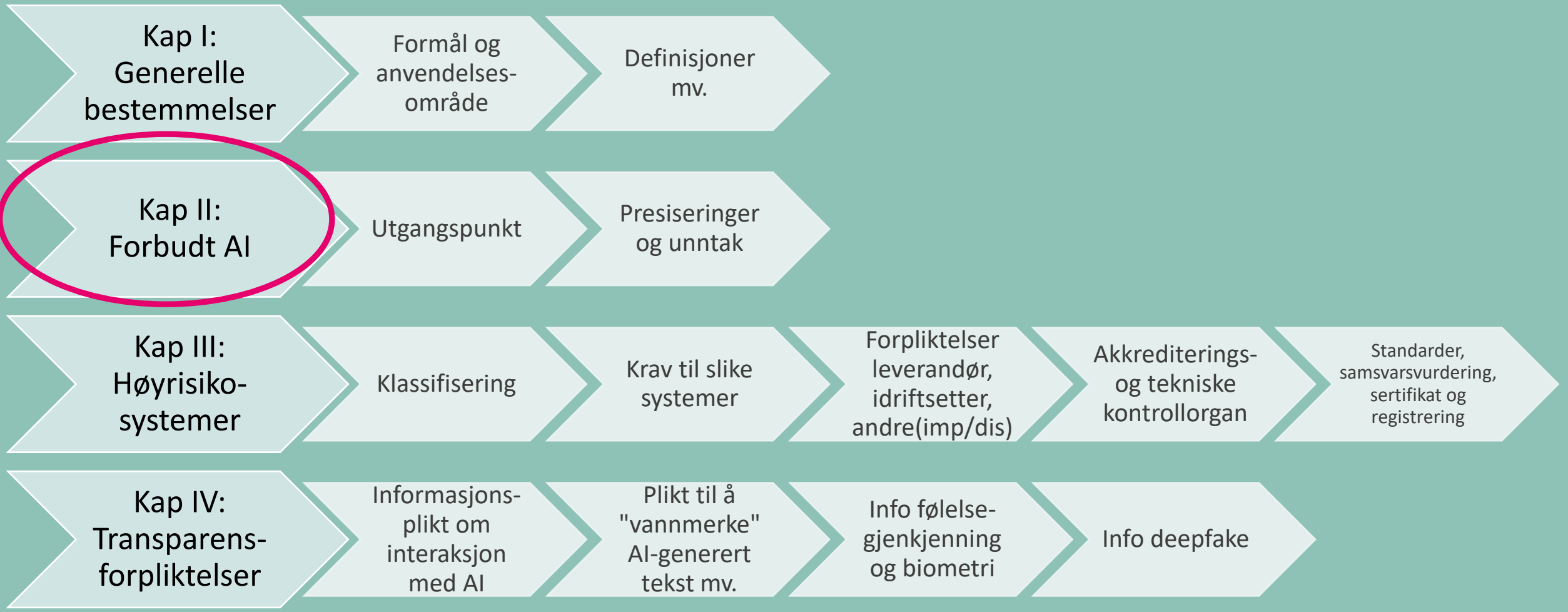
Grunnleggende krav til alle idriftsettere:

- følge bruksanvisningen
- sikre at personer med nødvendig opplæring har kontroll over systemet i bruk
- sikre at input-data er relevante og representative for systemets formål - hvis underlagt brukers kontroll
- Overvåke bruken i henhold til bruksanvisningen og rapportere avvik
- Oppbevare autogenererte logger fra systemet i minimum 6 måneder
- Gjennomføre DPIA hvor nødvendig
- Opplyse personer som blir utsatt for AI-assisterte beslutninger om dette

Særlige krav til visse idriftsettere: Evaluering av effekten av systemet på grunnleggende rettigheter

- Gjelder for visse Annex III - systemer
  - Offentlige myndigheter som bruker alle Annex III-systemene bortsett fra nr. 2
  - Private som yter offentlige tjenester
  - Private som bruker AI-systemer i pkt. 5 b) og c)
- Evalueringen skal som minimum inneholde
  - Beskrivelse av arbeidsprosesser og hvordan systemet vil bli brukt innen rammene av dets opprinnelige formål/bruksområde
  - Beskrivelse av tidsperiode og frekvens hvert AI-system er ment å brukes
  - Hvilke kategorier av personer vil bli berørt av bruken når denne skjer som planlagt.

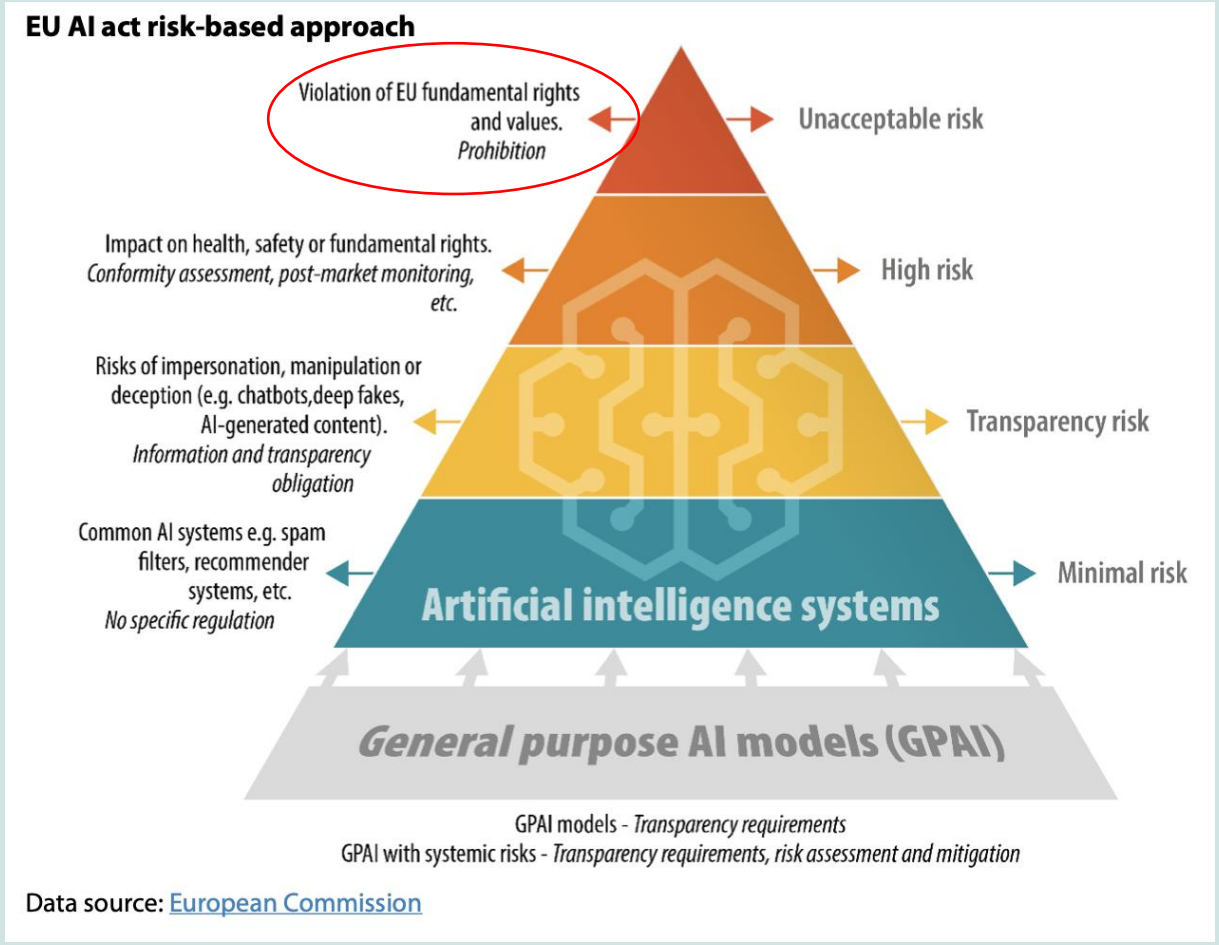
AI Act – oppbygning og struktur



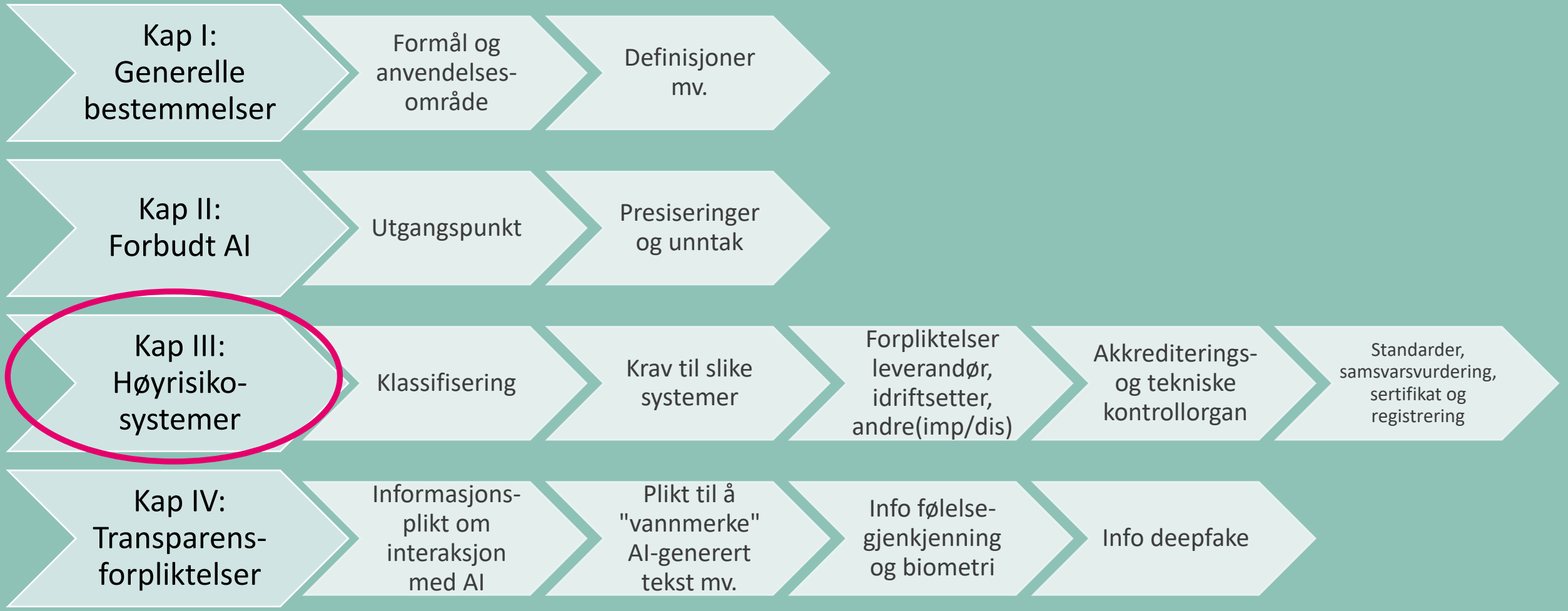
Så hva er da forbudt?

- **Biometri som**
  - identifiserer mennesker på offentlig sted i sanntid, med mindre dette gjøres etter reglene for etterforskning i kriminelle saker
  - kategoriserer mennesker etter grunnleggende karakteristika (kjønn, rase, politiske oppfatninger)

  eller
  - scraping av ansiktsdata for å bygge databaser
- **Social scoring – systemer**
  - Scoring av individer eller grupper basert på overvåkning
  - Systemer for risikovurdering av hvorvidt mennesker vil begå kriminell adferd
- **Systemer som kan manipulere mennesker**
  - Systemer som manipulerer individer eller grupper av individer til å gjøre ting de ellers ikke ville gjort
  - Systemer som er designet for å utnytte sårbarheten til utsatte grupper
- **Systemer som evaluerer følelser på arbeid eller skole**



AI Act – oppbygning og struktur



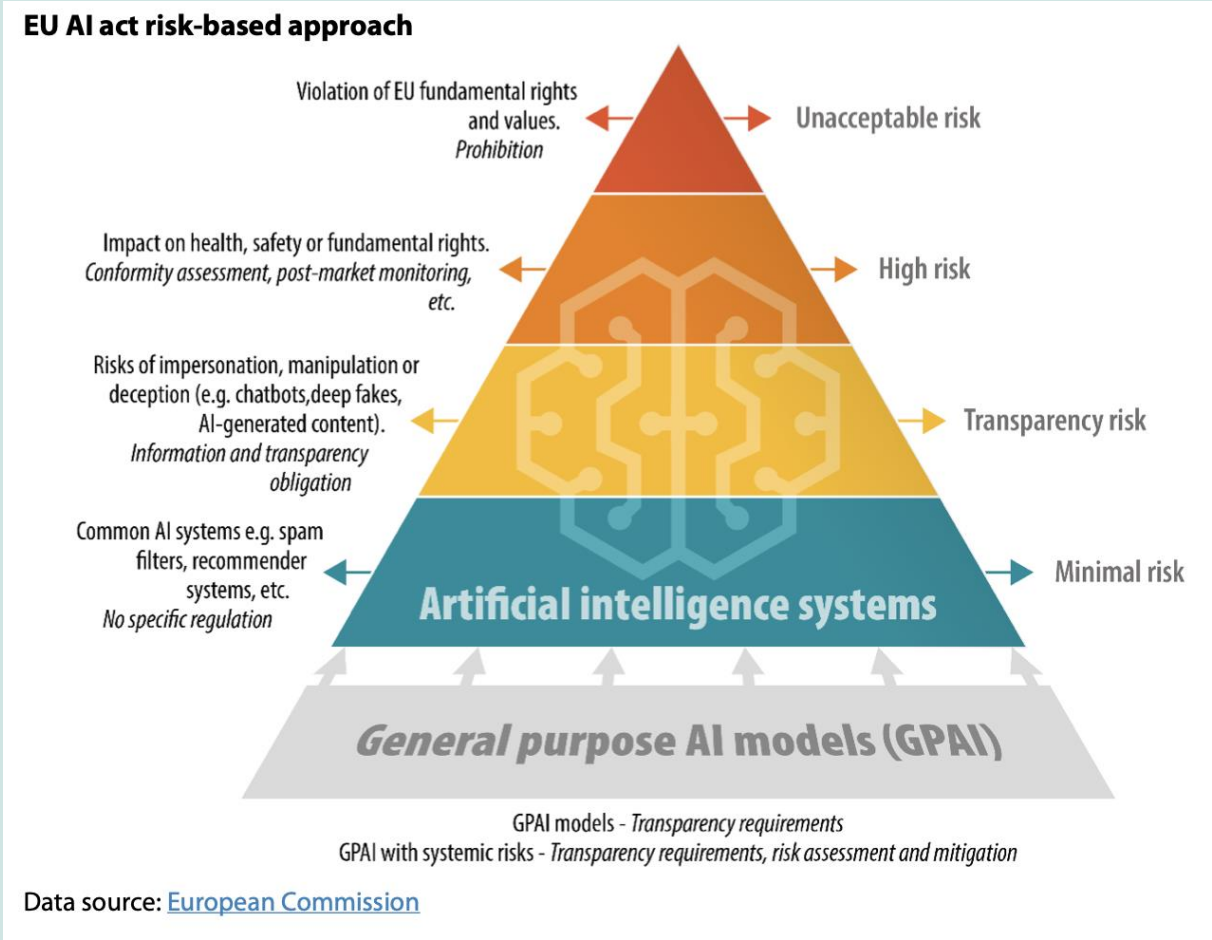
Hva er et høyrisikosystem?

- **Utgangspunktet**: Produktsikkerhetsregel – Art.6
  - AI'en er et sikkerhetssystem for produkter omfattet av produktsikkerhetsdirektiver definert i Annex I
  - Produktet må gjennomgå konformitetssjekk fra tredjepart i henhold til disse direktivene før det kan markedsføres

- **Tillegg**: Annex III som definerer visse former for AI hvor bruksområdet anses å utgjøre en risiko for grunnleggende rettigheter.

- **Unntak**: systemer på Annex III som ikke utgjør fare for helse, sikkerhet eller grunnleggende rettigheter fordi ett av vilkårene i Art. 6(3) er oppfylt.

- **Dynamisk system**: Kommisjonen kan endre vilkårene i Art. 6(3) eller legge til/fjerne bruksområder for AI fra Annex III etter Art. 6(6) og Art. 7.



Hva *er* da egentlig et høyrisikosystem?

- Sikkerhetssystemer og AI-systemer som selv er produkter dekket av produktsikkerhetslovgivning i Annex I.
- AI-systemer som brukes som sikkerhetssystemer i kritisk digital infrastruktur som nærmere definert i direktivet om kritiske enheters motstandsdyktighet, jf. Annex III pkt. 2
- Lovlige biometriske identifikasjonssystemer
- AI-systemer innen utdanning og yrkesutdanning
- AI-systemer innen HR og ansettelser
- AI-systemer som styrer tilgang til sentrale offentlig og private tjenester
- Etterforsknings- og politisystemer
- Systemer for grensekontroll
- Systemer for rettshåndhevelse

- Systemer som bestemmer opptak eller tilgang til utdanning/etterutdanning
- Systemer som skal evaluere læring, herunder slike som styrer læringsprosessene til personer
- Systemer som skal bedømme riktig nivå av læring for personer
- Systemer som avdekker juks.

- Systemer for rekruttering/annonsering, analyse av søknader og filtrering av kandidater
- Systemer som skal beslutte forfremmelser eller oppsigelser
- Systemer som allokerer oppgaver basert på prestasjon eller evaluerer ytelse

- Systemer for kredittvurdering
- Systemer for risikovurdering og –prising ved livs- og helseforsikring

(Svært) kort om kravene til høyrisikosystemer

Art. 9 – risikostyringssystem

- Identifisere rimelig forutsigbare risikoer mot liv helse og rettigheter som systemet kan skape når det brukes i henhold til forutsatt formål, risiko som kan oppstå under rimelig forutsigbart misbruk og andre risiki som kan skapes basert på data etter at systemet er satt i bruk.
- Iverksette risikostyringssystemer som så langt mulig fjerner risiko gjennom systemdesign og ellers via informasjon og trening.
- Teste systemet før det settes i drift

Art. 10 – krav til datakvalitet

- Kvalitetskrav til trening/validering/testsett av data
- Hjemmel for å behandle personopplysninger i den grad det er nødvendig for å motvirke bias i systemet

Art. 11-12 – krav til dokumentasjon og arkivering

Art. 13 – krav til gjennomsiktighet og informasjon til idriftsettere (brukere)

- Spesifikke opplysningskrav knyttet til systemets ytelse, presisjon og sikkerhet, behov for input-data og vedlikeholdsbehov

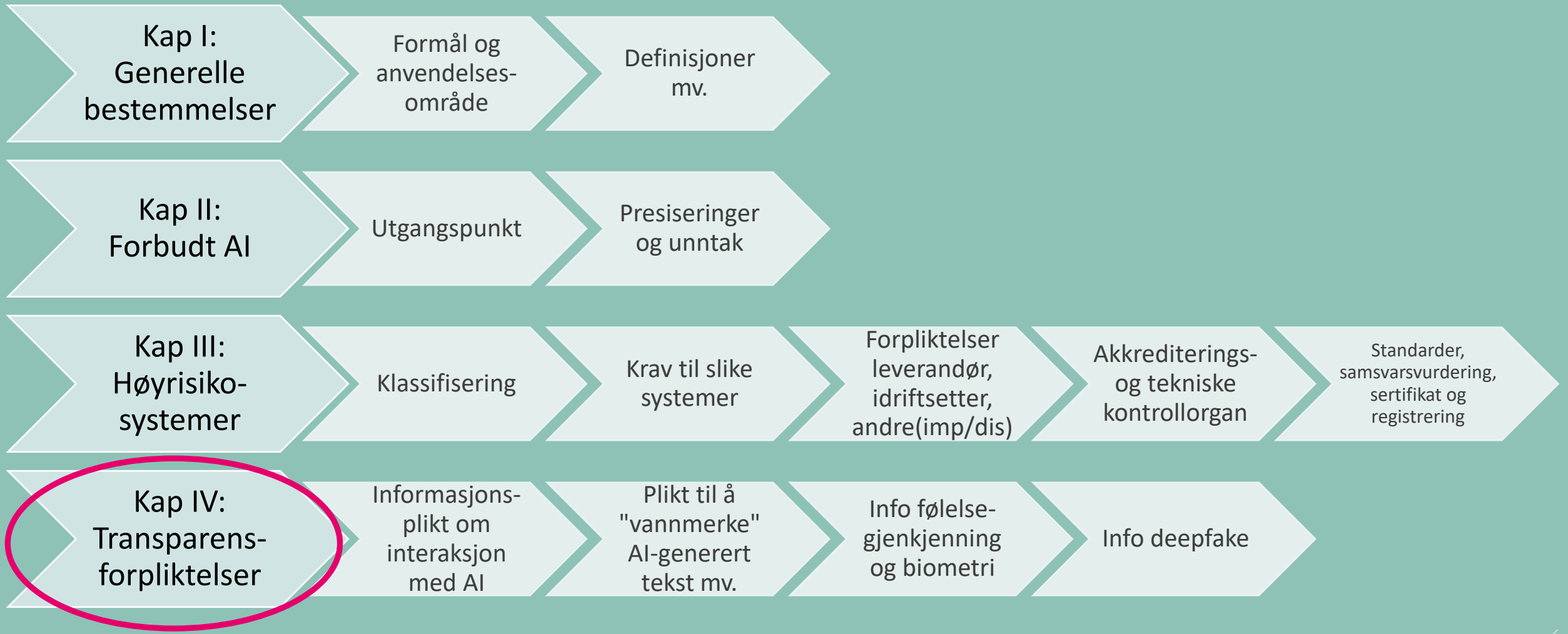
Art. 14 – krav til menneskelig kontroll

- Skal sikre en siste «failsafe» under normal bruk – eller under rimelig forutsigbart misbruk
- Mennesket skal kunne forstå systemets normale operasjoner, tolke «output» og være klar over eventuelle «vante» feil og/eller egen «automation bias» - og ha en stoppknapp

Art. 15 – krav til treffsikkerhet, robusthet og sikkerhet

- Data på treffsikkerhet skal oppgis i bruksanvisningen og Kommisjonen vil gi retningslinjer på hvordan dette måles
- Krav til design for å sikre robusthet (redundancy) og sikkerhet (blant annet datapoisoning)

AI Act – oppbygning og struktur



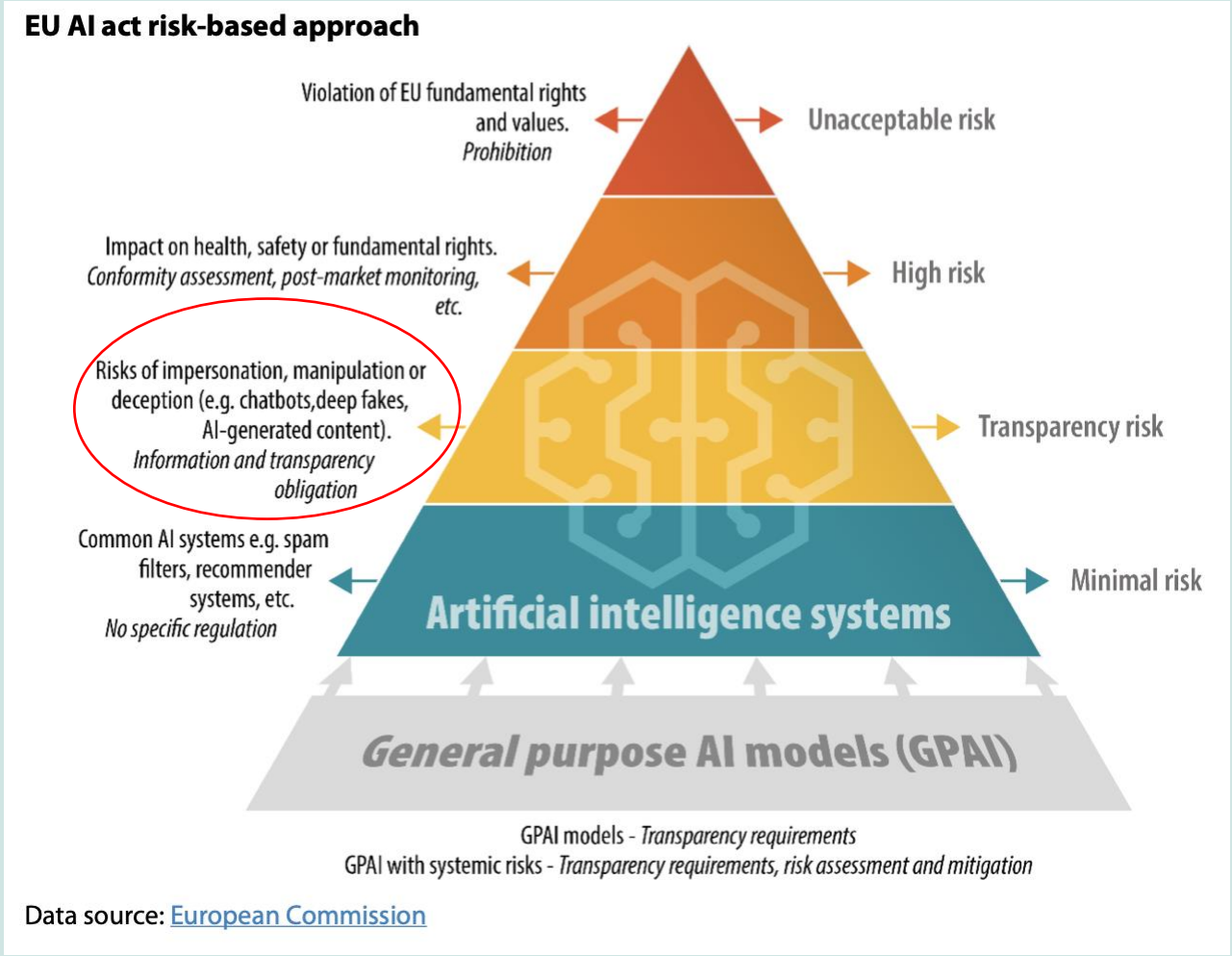
Forpliktelser om åpenhet

- AI-systemer som skal samhandle direkte med mennesker skal utvikles slik at det opplyse om at de er en AI
  - Unntatt hvor dette er åpenbart for en alminnelig aktsom person utfra kontekst og sammenheng

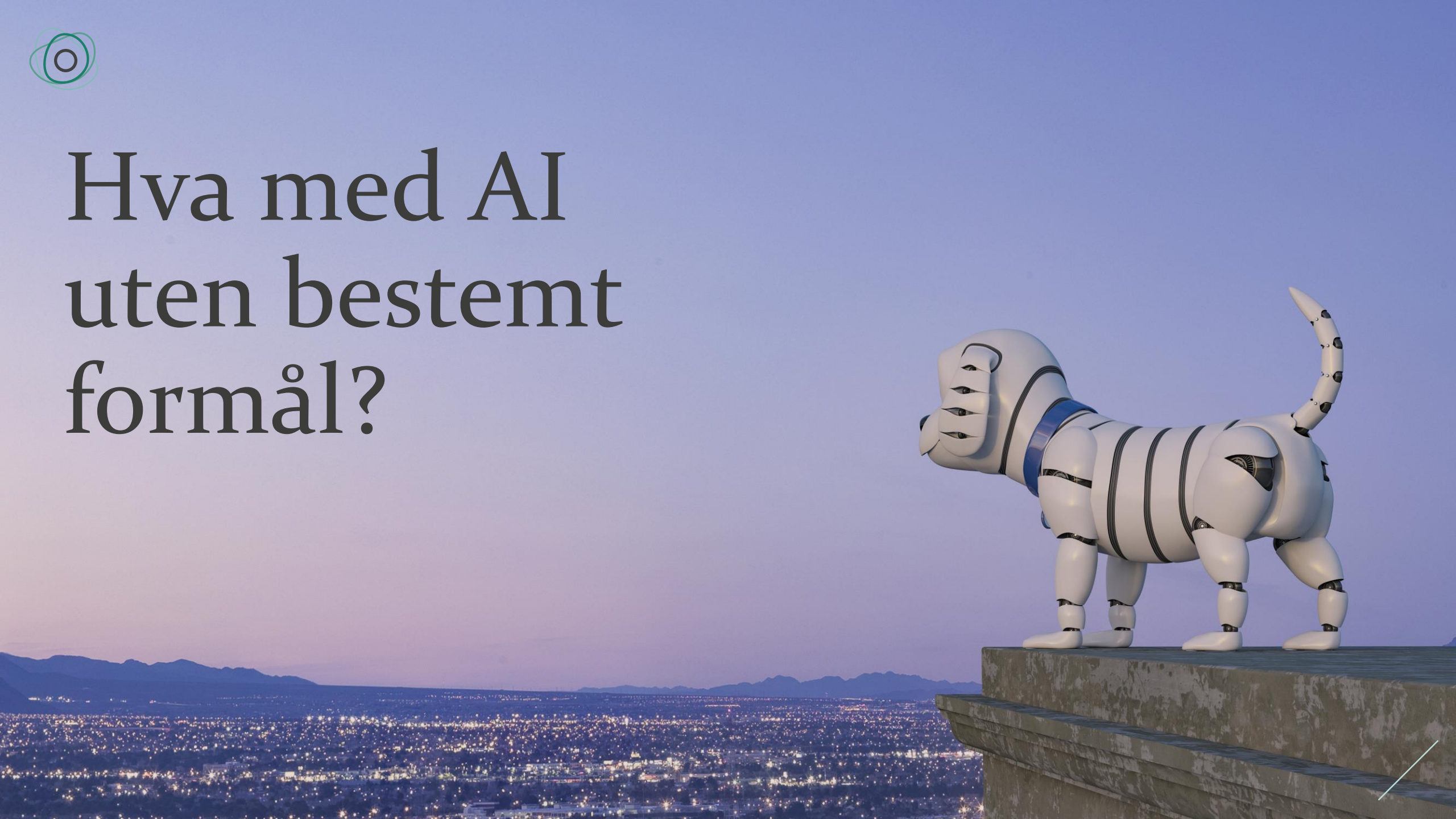
- Leverandører av AI-systemer som kan skape syntetisk audio, video, bilde eller tekst, skal sørge for at dette innholdet er merket på en maskinlesbar måte, i henhold til best practice og etterhvert, relevante standarder.

- Idriftsettere av system som gjenkjenner følelser eller biometriske kategoriseringssystemer, skal opplyse berørte personer om dette og behandle dataene i henhold til GDPR.

- Idriftsetter skal opplyse om deepfake



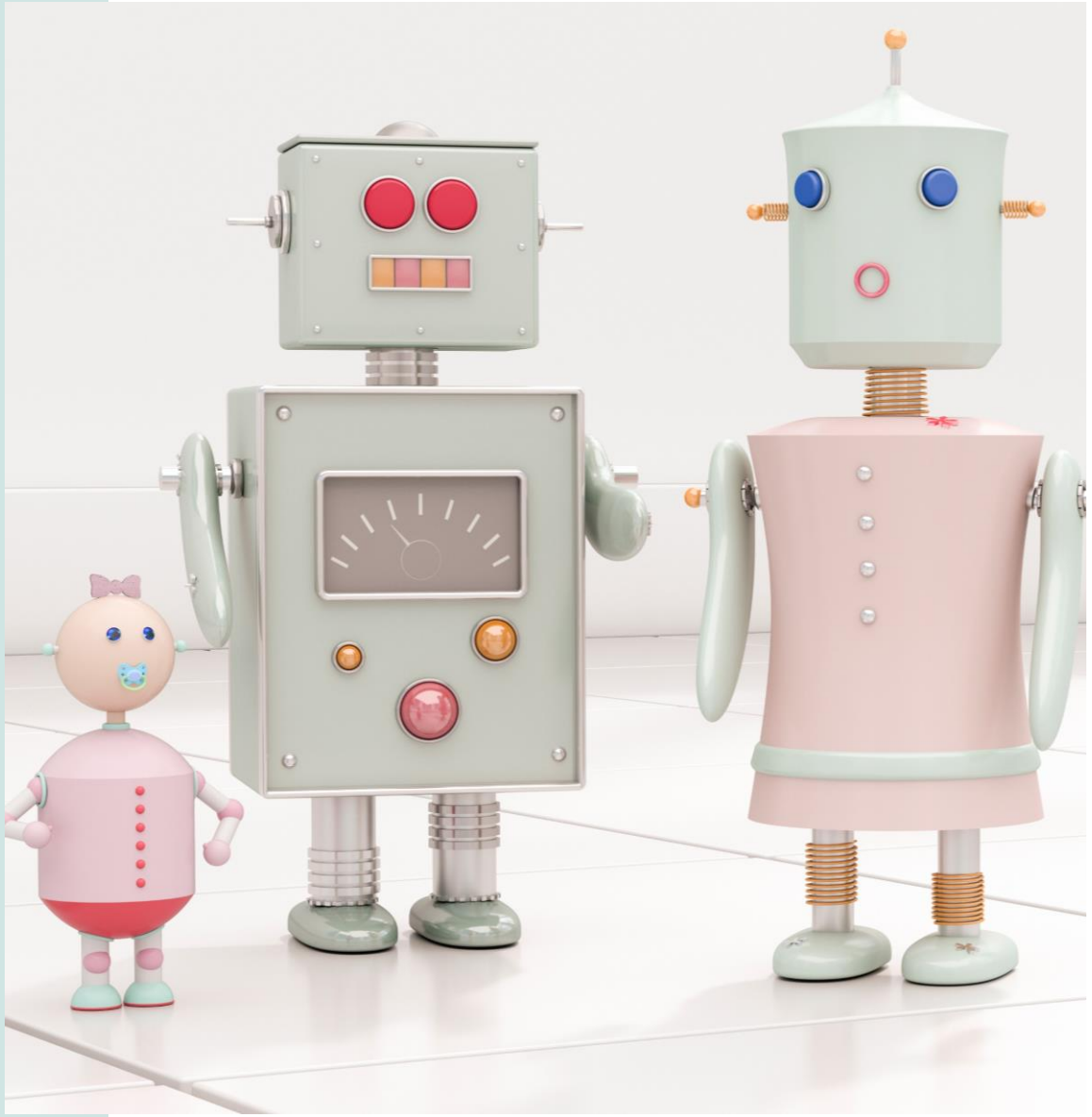
Hva med AI uten bestemt formål?



AI Act – oppbygning og struktur

Kategorier GPAI

1. AI-modeller (typisk APIer):
   - Krever ytterligere komponenter, f.eks. et brukergrensesnitt.
   - En sentral del av AI-systemer
   - Art. 3 nr. 63
2. AI-systemer (f.eks. ChatGPT)
   - Systemer som inneholder GPAI-modeller når dette medfører at systemet kan oppfylle mange formål
   - Art. 3 nr. 66
3. GPAI med systemisk risiko
   - Art. 3 nr. 65, art. 51



Roller og regler

- Leverandør/tilbyder («provider»)
  - Må forholde seg til regler om GPAI
- «Downstream provider» (de som implementerer)
  - Har krav på informasjon fra leverandøren
- Brukere («deployer»)
  - Har krav på informasjon fra leverandøren
  - Må forholde seg til de alminnelige reglene ihht. risiko

AI Act – oppbygning og strukturs

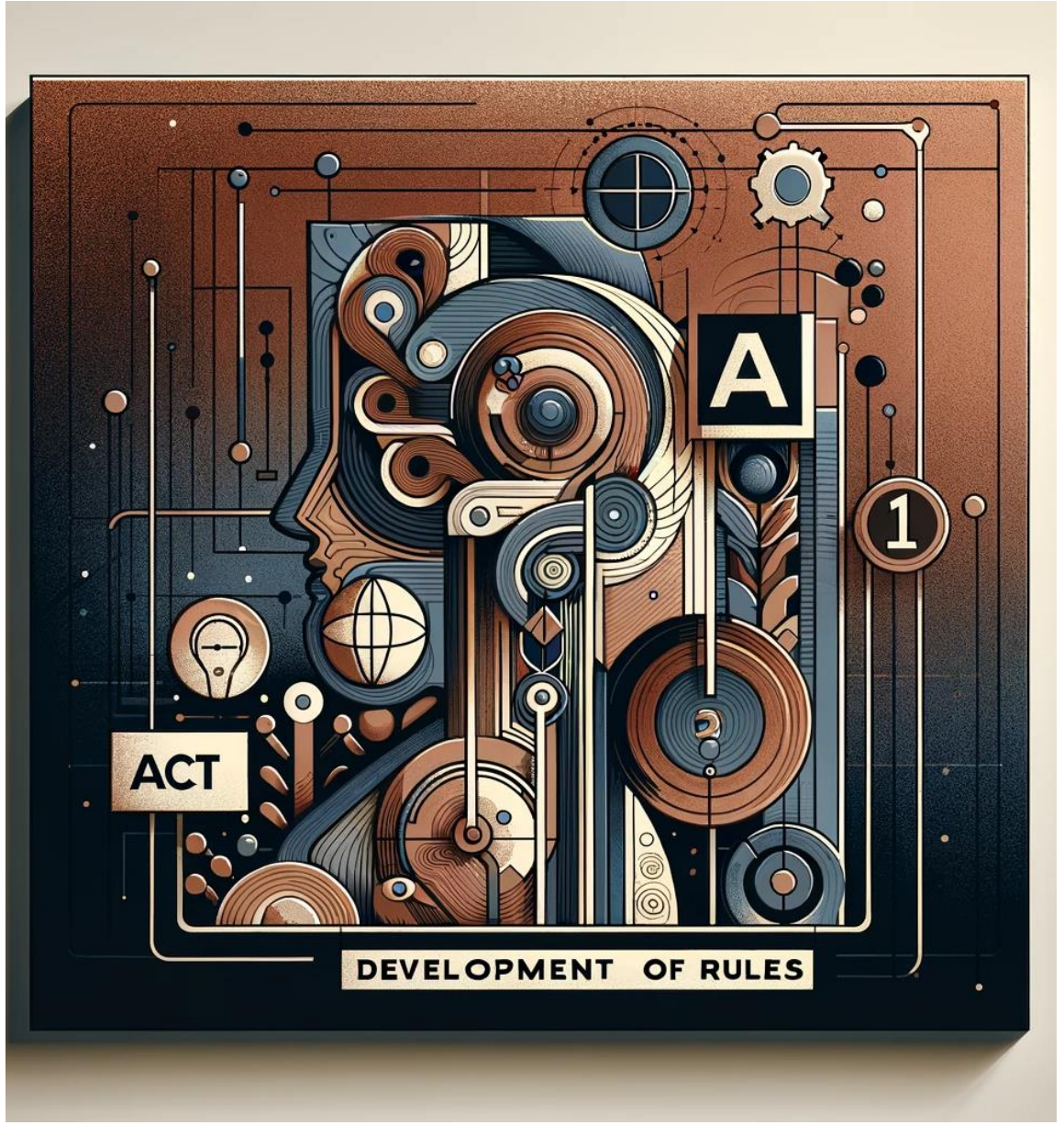
Kap IX: Markeds-overvåkning, informasjons-deling	Overvåkning etter høyrisikosystem på marked	Informasjons-deling alvorlige hendelser	Håndhevelse markedsover-våking og kontroll	Rettsmidler
Kap X Codes of conduct og retningslinjer	Adferdskoder for frivillig bruk	Retningslinjer fra kommisjonen om implementering		
Kap XI Delegasjons-prosedyre				
Kap XII Sanksjoner	7 % av turnover eller opp til 35 MEUR for ulovlig AI	3 % av turnover eller opp til 15 MEUR krav høyrisikosystem	3 % av turnover eller 15 MEUR kravene General Purpose AI	1 % av turnover eller opp til 7,5 MEUR for feilinformasjon

AI Act – oppbygning og struktur

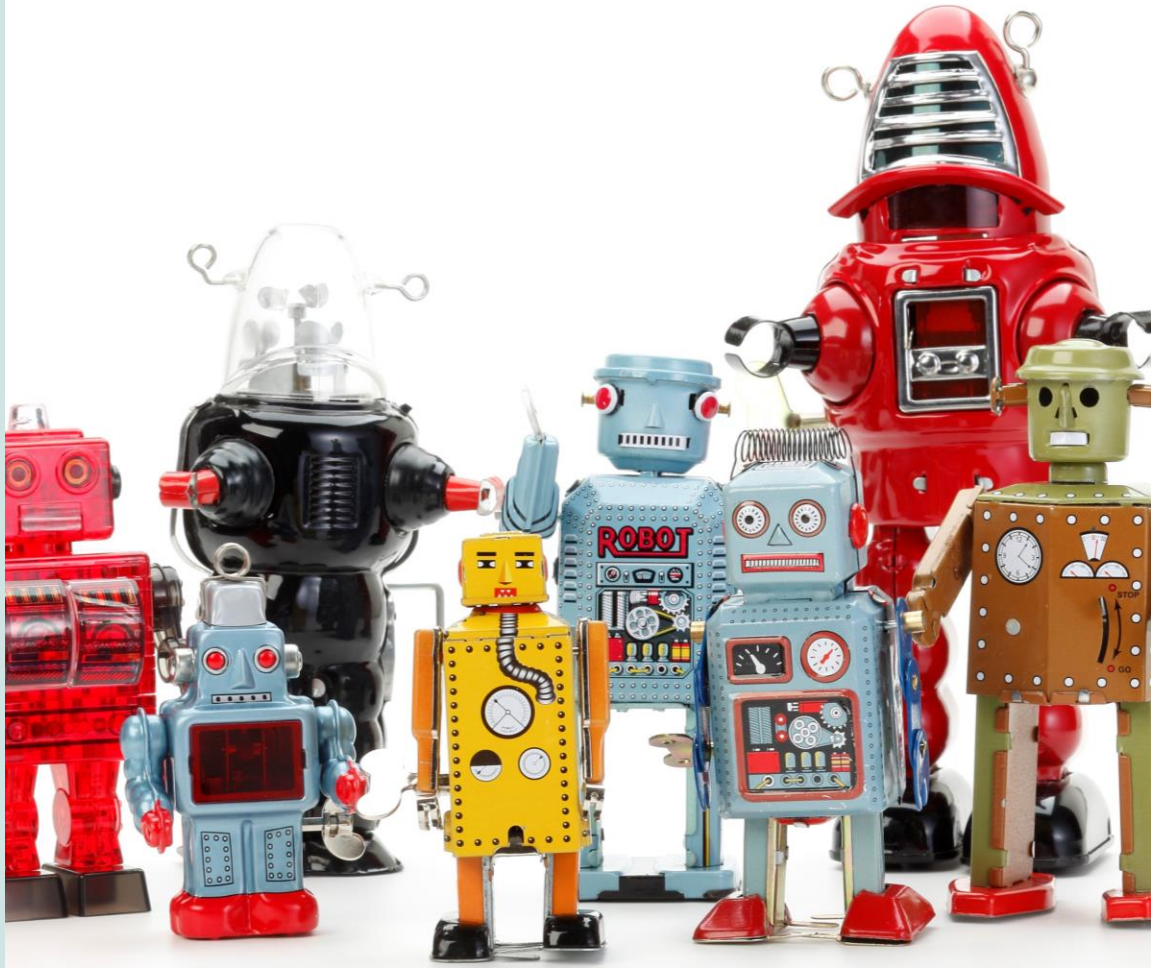
Annex I: List of Union Harmonisation Legislation
Annex II: List of Criminal Offences Referred to in Article 5(1), First Subparagraph, Point (h)(iii)
Annex III: High-Risk AI Systems Referred to in Article 6(2)
Annex IV: Technical Documentation Referred to in Article 11(1)
Annex V: EU Declaration of Conformity
Annex VI: Conformity Assessment Procedure Based on Internal Control
Annex VII: Conformity Based on Assessment of the Quality Management System and an Assessment of the Technical Documentation
Annex VIII: Information to be Submitted upon the Registration of High-Risk AI Systems in Accordance with Article 49
Annex IX: Information to be Submitted upon the Registration of High-Risk AI Systems Listed in Annex III in Relation to Testing in Real World Conditions in Accordance with Article 60
Annex X: Union Legislative Acts on Large-Scale IT Systems in the Area of Freedom, Security and Justice
Annex XI: Technical Documentation Referred to in Article 53(1), Point (a) - Technical Documentation for Providers of General-Purpose AI Models
Annex XII: Transparency Information Referred to in Article 53(1), Point (b) - Technical Documentation for Providers of General-Purpose AI Models to Downstream Providers that Integrate the Model into Their AI System
Annex XIII: Criteria for the Designation of General-Purpose AI models with Systemic Risk Referred to in Article 51

Regelutviklingen under forordningen

- «Guidelines»
  - Kap X art 96: Praktisk implementering av forordningen
  - Utarbeides av Kommisjonen
- «Codes of Conduct» «Codes of Practice»
  - Kap X art 95, Kap V art 56: Frivillig anvendelse
  - CoC utarbeides av leverandører eller brukere, eller av organisasjoner som representerer disse
  - CoP utarbeides av relevante stakeholders.
- Standarder
  - Art 40 - harmoniserte standarder – antas å være i overensstemmelse med krav til high risk
- Høyrisikosystemer nå og senere
  - Art 6 (6) og 7 – Kommisjonen kan endre og legge til betingelser, use case, eksempler



DALL*E, 2024



Steg for steg

1. Er det AI?
2. Er du innenfor virkeområdet til AI Act?
3. Hvilket risikonivå ligger du på?
4. Bruker du GPAI? Hvilken rolle har du i så fall?
5. Kartlegge plikter ihht. risikonivå og evnt. GPAI

Takk for oss!

Lisa Digernes
Partner

477 72 116
ld@bull.no

- TEKNOLOGI, IT OG AI
- IMMATERIALRETT OG MARKEDSFØRINGSRETT
- MEDIA UNDERHOLDNING OG KULTUR

Thale C. Gautier Gjerdsbakk
Advokatfullmektig

954 58 267
tcgg@bull.no

- PERSONVERN
- TEKNOLOGI, IT OG AI
- SPACE