Forordning om kunstig intelligens

12-01-2024

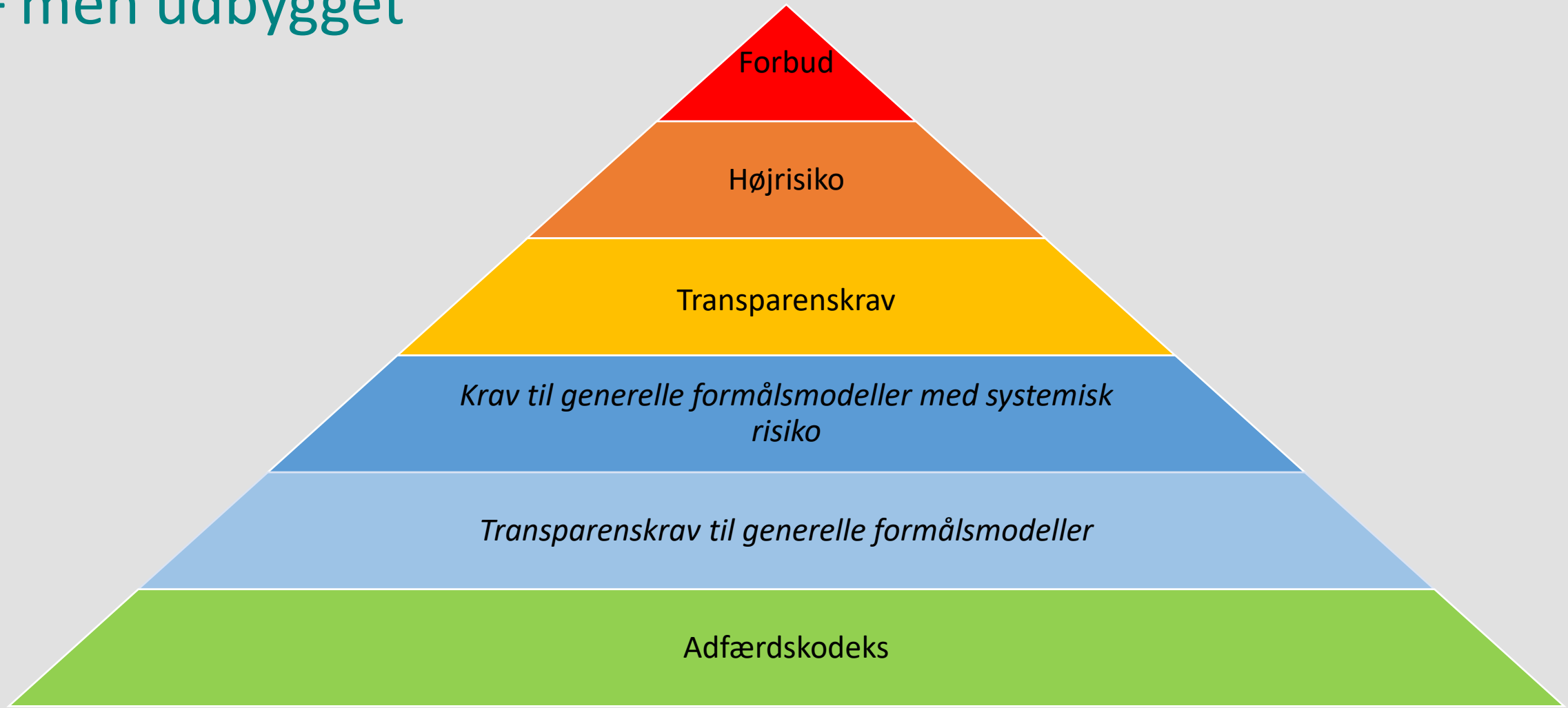
digitaliserings og ligestillingsministeriet

Dagsorden

1. Forordningens indhold
2. Næste skridt
3. DK implementering

digitaliserings og ligestillingsministeriet

Grundlæggende risikobaserede tilgang bevaret – men udbygget



digitaliserings og ligestillingsministeriet

Hvad er kunstig intelligens?

”An AI system is a machine-based system designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.”

Baseret på OECD’s definition fra November 2023

digitaliserings og ligestillingsministeriet

Hvad bliver forbudt?

Artikel 5:

- AI systemer, der anvender **subliminale teknikker** eller **teknikker der med vilje manipulerer** en persons opførsel på en sådan måde, at det forvolder skade
- AI systemer, der **udnytter sårbarheder hos udsatte grupper eller personer**, på en sådan måde, at det forvolder skade
- **Biometrisk kategoriseringssystemer** til at kategorisere fysiske personer på baggrund af biometrisk data med henblik på at udlede deres race, politiske holdninger, fagforeningsmedlemsskab, religiøse eller filosofiske overbevisninger, sex liv eller sexuel orientering.
- AI systemer til **social scoring** som fører til ugunst for borgerne i en ikke-relateret kontekst og/eller på uretfærdig eller disproportional vis ift. opførslen eller alvorligheden heraf.
- **Biometrisk fjernidentifikation** – fx ansigtsgenkendelse – i realtid i det offentlige rum med henblik på retshåndhævelse, medmindre det er strengt nødvendigt for at opnå et af følgende mål:
    - Målrettet eftersøgning af ofre for bortførelse, trafficking, og sexuel udnyttelse, samt til at søge efter forsvundne personer
    - Forebyggelse af en specifik, substantiel og overhængende trussel for liv eller fysisk sikkerhed af fysiske personer, eller en reel og tilstedeværende eller reel og forventelig trussel om et terrorangreb
    - Lokalisering eller identifikation af en person mistænkt for at have begået en forbrydelse, med henblik på at udføre en kriminalundersøgelse, retsforfølgelse eller gennemføre en strafferetslig straf for udvalgte oplistede forbrydelser med en strafferamme på mindst 4 år.
- *AI systemer til prædiktivt politiarbejde*
- *AI systemer til at opbygge eller udvide ansigtsgenkendelsesdatabaser igennem umålrettet scraping af internettet eller CCTV*
- *AI følelsesgenkendelsessystemer på arbejdspladser eller på uddannelsesinstitutioner*

digitaliserings og ligestillingsministeriet

Hvad er høj-risiko?

Bilag III – Højrisiko anvendelsesområder, uanset om producenten/brugeren en offentlig myndighed eller en virksomhed:

- Biometrisk identifikation af fysiske personer
- Forvaltning og drift af kritisk infrastruktur
- Uddannelse og erhvervsuddannelse
- Beskæftigelse, forvaltning af arbejdstagere og adgang til selvstændig virksomhed
- Adgang til og benyttelse af essentielle private og offentlige tjenester og fordele – *herunder forsikring*
- Retshåndhævelse
- Migrationsstyring, asylforvaltning og grænsekontrol
- Retspleje og demokratiske processer
- *Systemer der kan påvirke valg*

Medmindre systemet bruges til en af følgende ting:

- *Udfører en smal proceduremæssig opgave*
- *Forbedrer resultatet af en aktivitet allerede udført af et menneske*
- *Opdager mønske, som ikke påvirker beslutningen*
- *Udfører en forberedende opgave*

Dog er profilering altid høj-risiko

digitaliserings og ligestillingsministeriet

Hvad er høj-risiko?

Bilag II – AI indlejret i produkter der er <u>underlagt tredjepartskontrol</u> i sektorspecifik produkt lovgivning:

- Maskinforordningen
- Direktivet om legetøj
- Direktivet om radioudstyr
- Forordningerne om medicinsk udstyr
- Forordningen om værnemidler
- Direktivet om trykbærende udstyr
- Forordningen om tovbaneanlæg
- Etc.

Krav til høj-risiko systemer

Risikostyringssystem	Data og datahåndtering	Teknisk dokumentation	Logning
Transparens og information til brugere	Menneskeligt tilsyn	Akkurathed, robusthed og cybersikkerhed	Post-markeds monitorering
	Rapportering af hændelser	Forpligtigelser for udbydere og brugere og andre aktører (NLF classic)	

digitaliserings og ligestillingsministeriet

Krav til brugere af høj-risiko systemer – art.29 + 29a

Bruge systemet i overensstemmelse med brugsvejledningen

Sikre at personen der fører menneskeligt tilsyn har de nødvendige kompetencer

Sikre at input data er relevant og repræsentativt

Gøre opmærksom på uoverensstemmelse eller hændelser

Opbevare logs *i mindst 6 måneder*

Informere medarbejder om at systemet er i anvendelse

Offentlige myndigheder: registrere at de bruger systemet

Offentlige myndigheder: gøre borger opmærksom på brugen af systemet

Offentlige myndigheder: udføre en konsekvensanalyse for grundlæggende rettigheder

digitaliserings og ligestillingsministeriet

Transparenskrav – art.52

Fysiske personer skal vide at de interagere med AI

Udbydere af AI systemer der genererer indhold skal sikre at de mærker deres output

Brugere, der laver deep-fakes, skal oplyse om at indholdet er AI genereret

digitaliserings og ligestillingsministeriet

Krav til AI modeller

Teknisk dokumentation	Brug af ophavsretsbeskyttet materiale	Information om træningsdata	Code of Practice
Risikomitigering	Rapportering til KOM	Cybersikkerhed	Information om energiforbrug

Generelle formålsmodeller med systemisk risiko i det indre marked = FLOPS > 10^25

digitaliserings og ligestillingsministeriet

Tilsyn og håndhævelse på nationalt niveau (NLF) med høj-risiko systemer

Udbydere/brugere af

- Høj-risiko AI-systemer der er indlejret i produkter (bilag II)
- Selvstændige høj-risiko AI systemer (bilag III)

Krav

- Overensstemmelses-vurdering iht. pågældende lovgivning
- Selvevaluering

Hvis **harmoniseret standard** følges formodes overensstemmelse

digitaliserings og ligestillingsministeriet

Nationale myndigheders rolle ifølge forordningen

Én national koordinerende tilsynsmyndighed

- Kontaktpunkt for EU KOM
- Repræsentant i udvalg for AI
- Markedsovervågning
- Bemyndigende myndighed

- Vejledning til SMV'er og små offentlige myndigheder (+ kommunikationskanal)
- Sandkasser

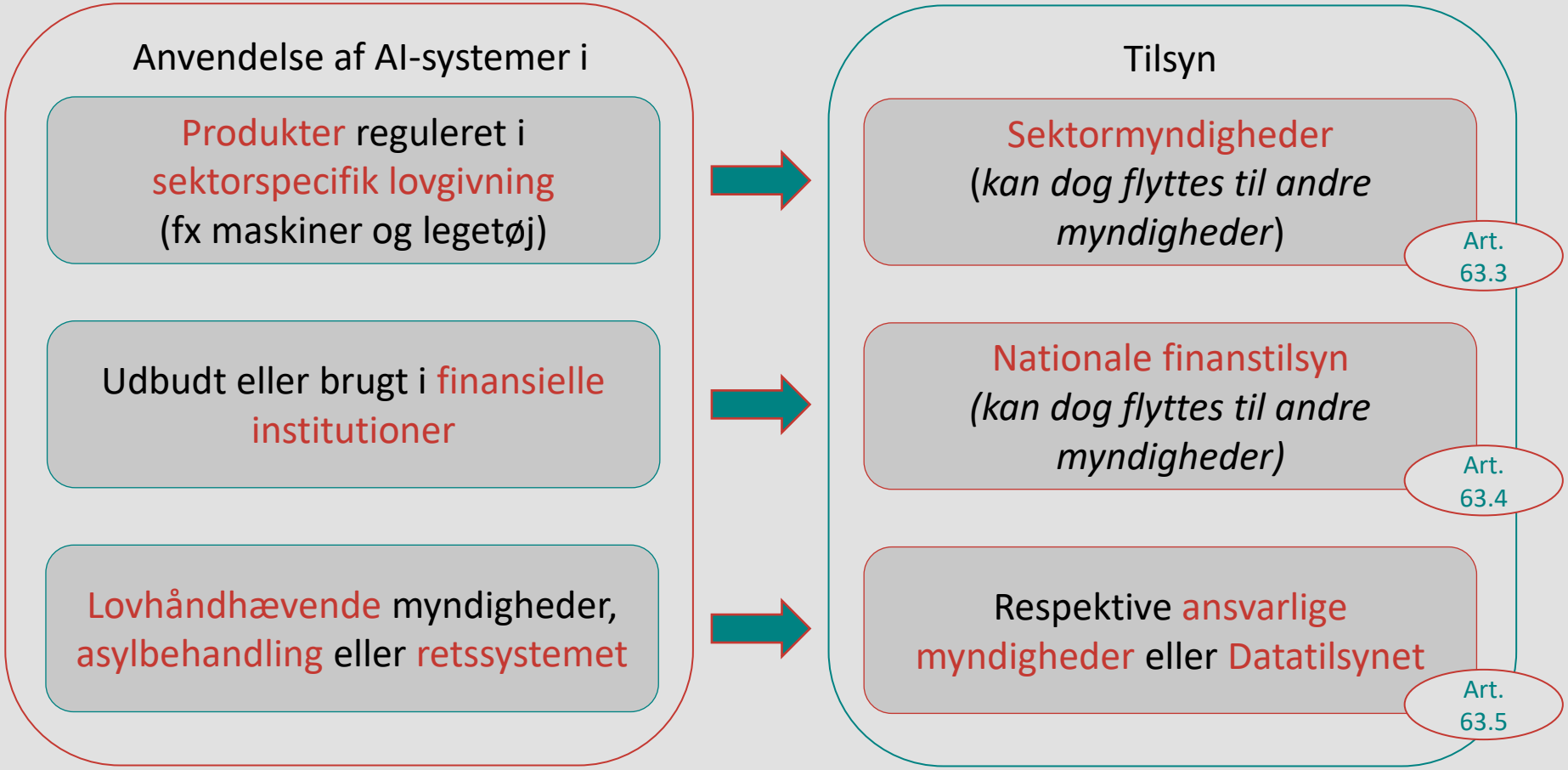
Én eller flere kompetent(e) myndighed(er)

Sektoransvarsprincip som udgangspunkt

- Markedsovervågning
- Bemyndigende myndighed
- *Klageadgang*

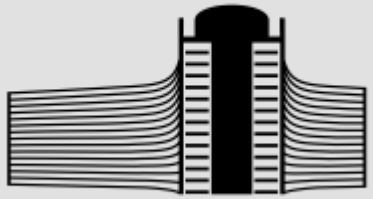
digitaliserings og ligestillingsministeriet

Fleksibilitet i national tilsyn med visse begrænsninger



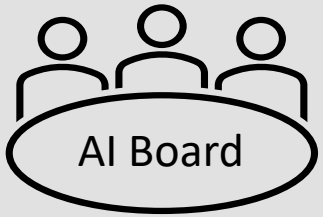
digitaliserings og ligestillingsministeriet

Tilsyn på EU niveau med AI modeller og systemer til generelle formål

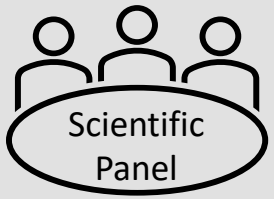


AI Office

Klageadgang for downstream udbydere



!

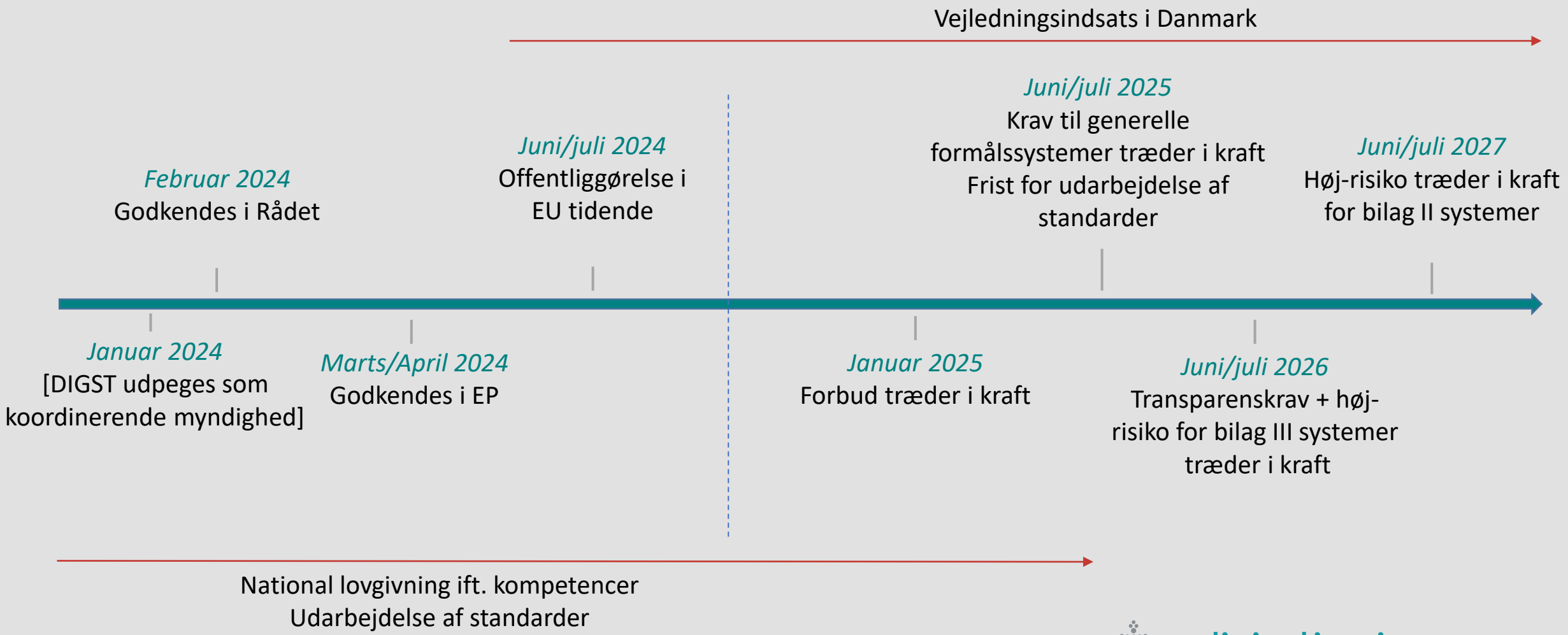


Database

Unions Testfacilitet

digitaliserings og ligestillingsministeriet

Næste skridt og implementeringsfrister



digitaliserings og ligestillingsministeriet

Spørgsmål?

Sektorbaseret tilgang i DK implementering

Koordinerende myndighed – DIGST/DT

- One-stop-shop
- Evt. ny klageadgang
- Vejledning til andre myndigheder
- Kompetencecenter
- Horisontal sandkasse
- Tilsyn med selvstændigt AI
  - Offentligt og privat

Sektoransvar - tilsyn med AI indlejret i produkter

LMST - Medicinsk udstyr
SIK - Maskiner, legetøj, etc.
SDFI - Radioudstyr
SFS - Maritimt udstyr
FT - Finansiel sektor

JM / UIM / DT

AI systemer brugt af lovhåndhævende myndigheder, til asylbehandling eller i retssystemet

digitaliserings og ligestillingsministeriet

Hvorfor sektorbaseret tilgang med DLM som koordinerende myndighed?

Sektoransvar

- Høj-risiko klassificeringen er *anvendelses* og dermed kontekst bestemt
- Virksomhederne og myndighederne kender allerede deres sektorlovgivning og procedurerne
- Forordningen lægger op til sektoransvar som udgangspunkt
- Bygger på eksisterende strukturer og kompetencer

DLM

- Samler erhvervslivet og den offentlige sektor
- Kompetencer indenfor kunstig intelligens (men behov for videreudvikling)
- Har forhandlet forordningen og har indgående kendskab hertil
- Vil naturligt få en koordinerende funktion på alle digitale sager fremadrettet

digitaliserings og ligestillingsministeriet