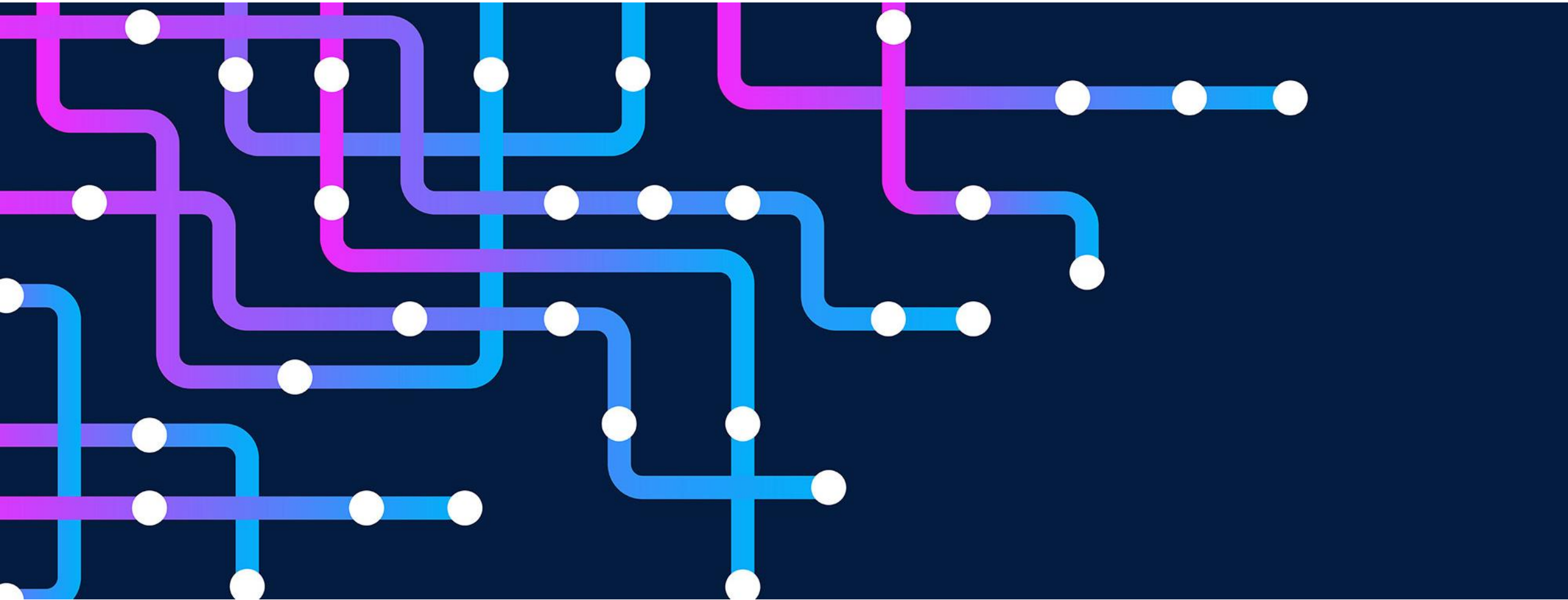







DEN KOMMENDE AI-FORORDNING



DAGSORDEN

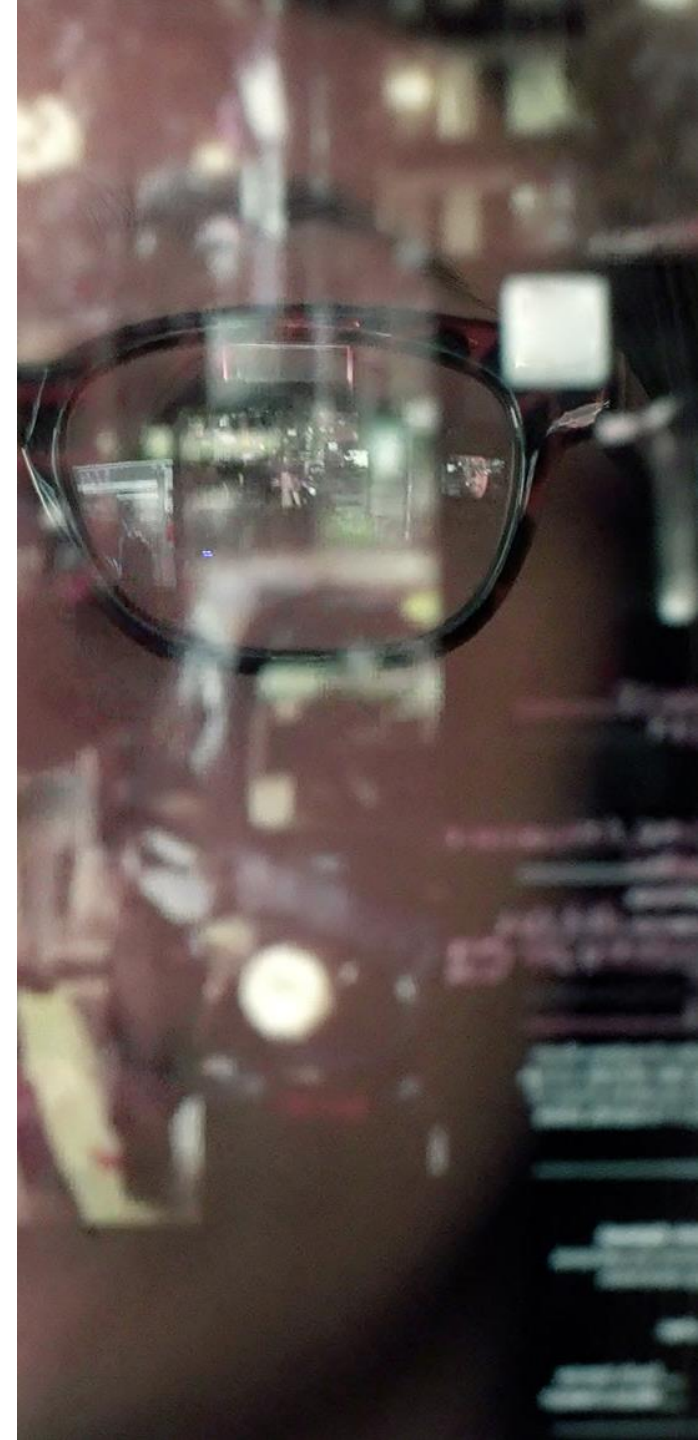
-  Introduktion og baggrund
-  Screening af systemer og aktører
-  Forpligtelser ved højrisiko-systemer
-  Gennemsigtighed i AI-systemer –
Internt og eksternt
-  Afrunding



INTRODUKTION OG BAGGRUND

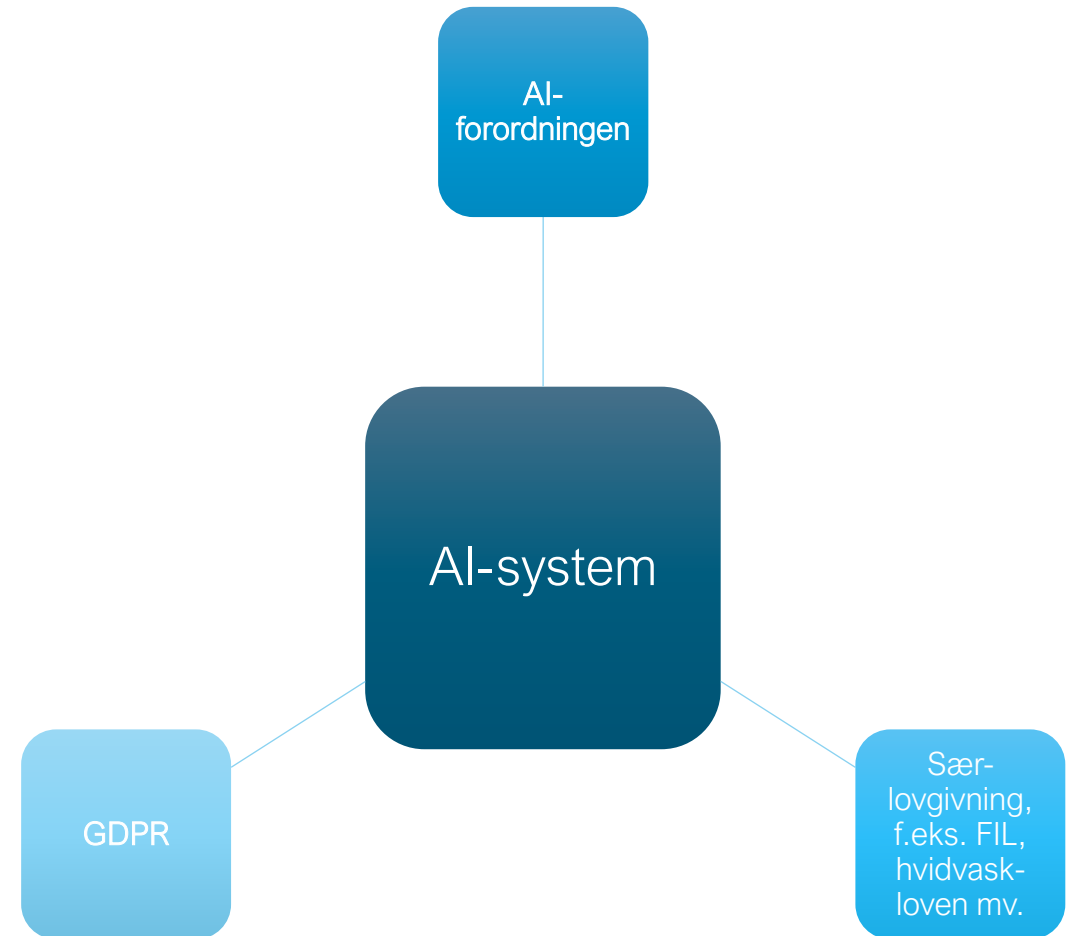
STATUS PÅ FORORDNINGEN

- Behov for hård jura eller blød dataetik – eller en kombi?
 - EU-strategi for AI og koordineret plan med medlemsstaterne i 2018.
 - Den Uafhængige Ekspertgruppe på Højt Niveau om Kunstig Intelligens – etiske retningslinjer for pålidelig kunstig intelligens i april 2019.
 - Hvidbog ("white paper") og datastrategi fra EU-Kommissionen den 19. februar 2020.
- Den 21. april 2021 offentliggjorde Kommissionen et udkast til en ny forordning med generel regulering af AI.
 - Rådet har løbende offentliggjort kompromistekster, der ændrer Kommissionens forslag.
 - 309 ændringsforslag fra Europa-Parlamentets JURI-udvalg.
 - Politisk aftale ultimo 2023
- Suppleres af ny Maskin-forordning – sikkerhedskrav, når AI indbygges i produkter, f.eks. græsslåmaskiner, 3D-printere, produktionsmaskiner etc.



HVAD GÆLDER I DAG?

- Der gælder allerede i dag en række regler, som regulerer AI-systemer, herunder
 - Databeskyttelsesforordningen
 - Databeskyttelsesloven
 - Ligebehandlingsloven
 - Særlovgivning
 - M.fl.
- Om lidt også NIS-II eller DORA
- Når AI-forordningen vedtages, vil den gælde side om side med og/eller supplere eksisterende regler.



OVERORDNET OM FORHOLDET MELLEM GDPR OG AIF

- Materielt anvendelsesområde:
 - Behandling af personoplysninger (herunder i AI-systemer) vs. AI-systemer (uanset datatype).
- Pligtssubjektet:
 - Den dataansvarlige/databehandleren i GDPR vs. udbyder/bruger i AIF.
- Overlap i flere af de centrale temaer, hvor AIF indeholder mere AI-specifikke regler.
- Forholdet mellem AIF og GDPR
 - Er ikke reguleret direkte i AIF.
 - Men ifølge pr. 41 skaber AIF ikke hjemmel til behandling af personoplysninger, og GDPR gælder ved siden af AIF.
 - De to regelsæt eksisterer side om side – AIF supplerer GDPR.
 - GDPR har bl.a. betydning ved siden af AIF, når AIF ikke finder anvendelse, f.eks. fordi et AI-system udvikles, men ikke bringes i omsætning eller anvendes i EU (men uden for EU).



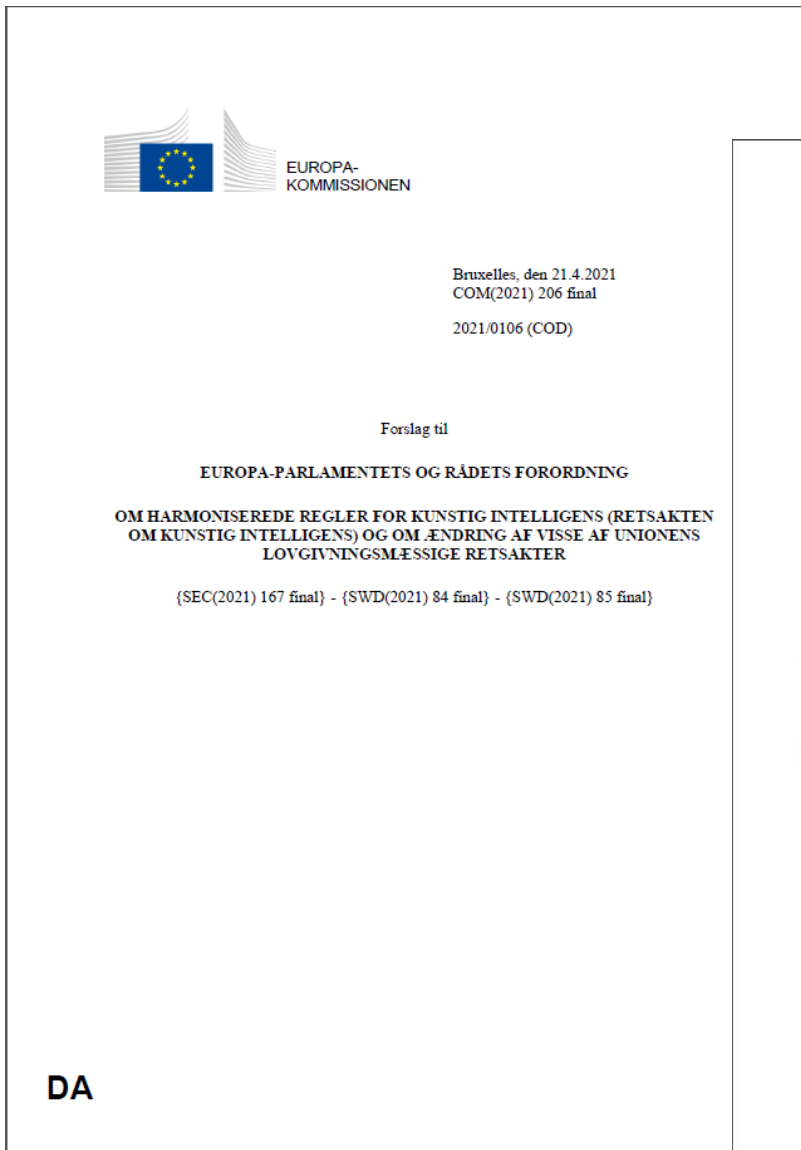
OVERBLIK OVER AI-FORORDNINGEN

Oprindeligt...

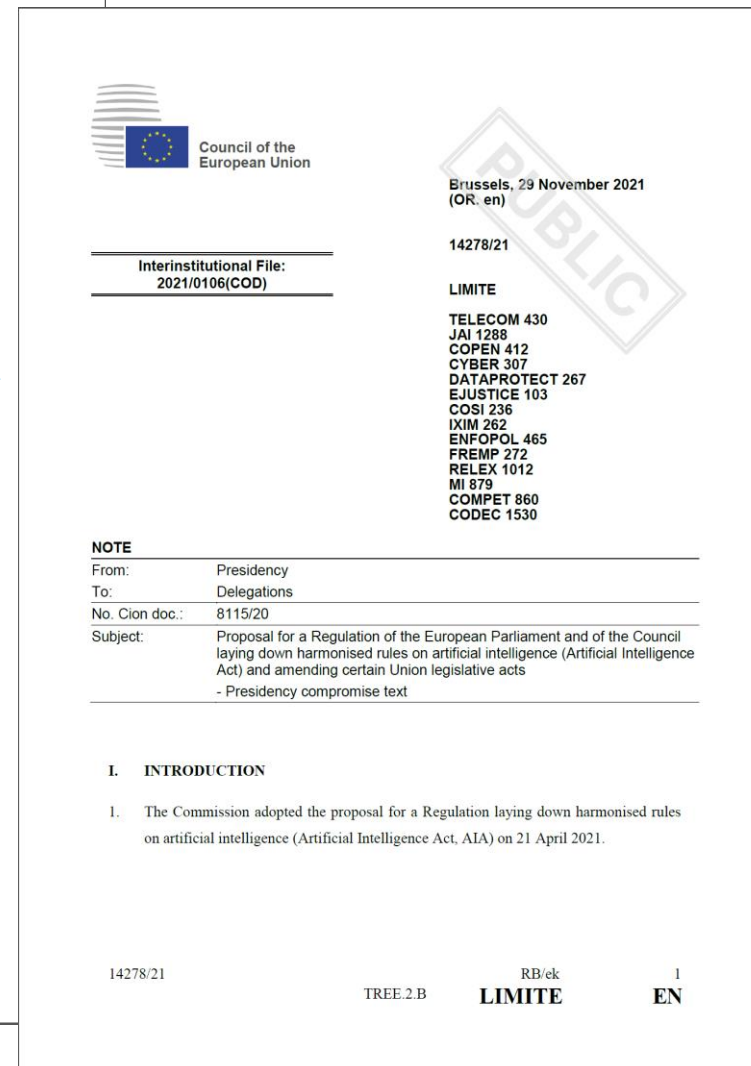
- 85 artikler
- 89 præambelbetragtninger
- 9 bilag

- Rådet har løbende offentliggjort en række kompromistekster, der ændrer Kommissionens forslag, herunder navnlig den 29. november 2021, og senere.
- Og der er løbende kommet ændringsforslag fra Europa-Parlamentets Retsudvalg (JURI) m.fl., senest den 16. maj 2023.
- Politisk aftale i december 2023, men endnu ikke renskrevet endelig tekst.

Poul Schmith



The cover page features the European Commission logo at the top left. The text is centered and includes the date and reference number: 'Bruxelles, den 21.4.2021 COM(2021) 206 final' and '2021/0106 (COD)'. Below this is the title 'Forslag til' followed by 'EUROPA-PARLAMENTETS OG RÅDETS FORORDNING' and the subject 'OM HARMONISEREDE REGLER FOR KUNSTIG INTELLIGENS (RETSAKTEN OM KUNSTIG INTELLIGENS) OG OM ÆNDRING AF VISSE AF UNIONENS LOVGIVNINGSMÆSSIGE RETSAKTER'. At the bottom, it lists related documents: '{SEC(2021) 167 final} - {SWD(2021) 84 final} - {SWD(2021) 85 final}'. The language code 'DA' is in the bottom left corner.



This page is a document from the Council of the European Union. It features the Council logo at the top left. The date and reference number are 'Bruxelles, 29 November 2021 (OR. en)' and '14278/21'. A large 'PUBLIC' watermark is visible. The text includes 'Interinstitutional File: 2021/0106(COD)', 'LIMITE', and a list of related documents: 'TELECOM 430', 'JAI 1288', 'COPEN 412', 'CYBER 307', 'DATAPROTECT 267', 'EJUSTICE 103', 'COSI 236', 'IXIM 262', 'ENFOPOL 465', 'FREMP 272', 'RELEX 1012', 'MI 879', 'COMPET 860', 'CODEC 1530'. A 'NOTE' section follows, detailing the document's origin (Presidency), recipients (Delegations), and subject (Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts - Presidency compromise text). The 'I. INTRODUCTION' section begins with '1. The Commission adopted the proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act, AIA) on 21 April 2021.'. At the bottom, it shows '14278/21', 'TREE.2.B', 'RB/ek', 'LIMITE', and '1 EN'.

OVERBLIK OVER AI-FORORDNINGEN (ARTIKEL 1)

- Horizontal regulering af AI-systemer i hele livscyklus – fra udvikling til markedet og overvågning i drift.
- Forbud mod visse AI-praksisser.
- En risikobaseret tilgang med specifikke krav til høj-risiko AI-systemer og forpligtelser for bl.a. leverandører og brugere af sådanne systemer.
- Harmoniserede regler om gennemsigtighed (transparency) for visse AI-systemer.
- Særlige regler for udbydere af general purpose AI models.
- Regler om markedsovervågning og tilsyn og skrappe sanktioner modelleret efter GDPR.
- Foranstaltninger til fremme af innovation, herunder fastsættes der en ramme for implementering af reguleringsmæssige sandkasser.
- Regler om etablering af og funktion for EU organer



ANVENDELSESOMRÅDE

- AIF finder anvendelse på (art. 2)
 - a) Udbydere af AI-systemer, der omsætter eller ibrugtager AI-systemer i EU, uanset om de er etableret i EU eller et tredjeland
 - b) Deployere af AI-systemer, som er etableret eller befinder sig i EU
 - c) Udbydere og deployere af AI-systemer, der er etableret eller befinder sig i et tredjeland, hvis output generet af systemet anvendes i EU
 - d) Producenter af produkter, der omsætter eller ibrugtager AI-systemer, sammen med produkter og under eget navn/varemærke.
 - e) Importører og distributører af AI-systemer samt repræsentanter for udbydere af AI-systemer, hvor sådanne importører m.fl. er etableret eller befinder sig i EU (ny – parlamentets forslag)
 - f) "affected persons" som defineret i artikel 3, nr. 8a, som befinder sig i EU

SCREENING AF SYSTEMER OG AKTØRER

CENTRALE DEFINITIONER

- AIF indeholder 68 definitioner, som bl.a. har betydning for screening af systemer og fastlæggelse af forpligtelser.
- De mest centrale definitioner er følgende:



'Artificial intelligence system' (AI-system)



'General purpose AI model'



'General purpose AI system'



'Udbyder' (provider)



'Bruger' (deployer)



'Risk' og 'significant risk'



DEFINITIONER AF AI-SYSTEMER

"Artificial intelligence system" (AI system)

"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."

"General purpose AI model"

"AI model, including when trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable to competently perform a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications."

"General purpose AI system"

"AI system which is based on a general purpose AI model, that has the capability to serve a variety of purposes, both for direct use as well as for integration in other AI systems."

RISICI VED AI-SYSTEMER

- Med AI-forordningen indføres en risikobaseret tilgang til brugen af AI-systemer, hvor der indføres forskellige niveauer af forpligtelser, alt efter hvilken risiko AI-systemet indebærer.

- AI-forordningen opdeler AI-systemer i følgende risikokategorier:


1. **Uacceptabel risiko**, hvor der som udgangspunkt gælder et forbud mod visse anvendelser.
2. **Høj risiko**, hvor der er specifikke, skrappe krav forbundet med AI-systemerne, og hvor der er påkrævet forudgående overensstemmelsesvurdering og efterfølgende markedsovervågning.
3. **Begrænset risiko**, hvor der er gennemsigtighedsforpligtelser for visse AI-systemer.
4. **Lav eller minimal risiko**, hvor der ikke er specifikke krav, og som derfor kan omsættes og anvendes frit, men hvor der er mulighed for at underlægge sig krav frivilligt gennem adfærdskodekser.

- AI-forordningen fastsætter ikke krav om gennemførelse af en egentlig risikovurdering, men derimod krav om en vurdering af, om det pågældende AI-system er omfattet af art. 5, 6 eller 52.
- En egentlig risikovurdering kan dog være påkrævet efter anden lovgivning, såsom GDPR, DORA eller den finansielle regulering.

UDVALGTE FORBUDTE AI-PRAKSISSER (AFSNIT II, ARTIKEL 5)

Bl.a. forbud mod AI-systemer, der

- I. deploys subliminal techniques beyond a person's consciousness or purposefully manipulative or deceptive techniques, with the objective to or the effect of materially distorting a person's or a group of persons' behaviour by appreciably impairing the person's ability to make an informed decision, thereby causing the person to take a decision that that person would not have otherwise taken in a manner that causes or is likely to cause that person, another person or group of persons significant harm,
- II. that exploits any of the vulnerabilities of a person or a specific group of persons due to their age, disability or a specific social or economic situation, with the objective to or the effect of materially distorting the behaviour of that person or a person pertaining to that group in a manner that causes or is reasonably likely to cause that person or another person significant harm,
- III. for the evaluation or classification of natural persons or groups thereof over a certain period of time based on their social behaviour or known, inferred or predicted personal or personality characteristics, with the social score leading to either or both of the following: (i) detrimental or unfavourable treatment of certain natural persons or whole groups thereof in social contexts that are unrelated to the contexts in which the data was originally generated or collected; (ii) detrimental or unfavourable treatment of certain natural persons or groups thereof that is unjustified or disproportionate to their social behaviour or its gravity.



HØJRISIKO-AI-SYSTEMER (1/2)

- Kriterierne for hvornår der er tale om et **højrisiko**-AI-system er fastsat i art. 6, stk. 1-3:
 - (1-2) AI-systemer, der selv er et produkt eller er beregnet til at blive anvendt som sikkerhedskomponenter i produkter, der er omfattet af harmoniseret EU-lovgivning nævnt i bilag 2, og der er forpligtet til at gennemgå en overensstemmelsesvurdering vedr. sundheds- eller sikkerhedsmæssige risici fra tredjepart (f.eks. maskiner, legetøj, medicinsk udstyr).
 - (3) Andre selvstændige AI-systemer – uafhængige af et produkt – hvor systemet er omfattet af en eller flere af de kritiske områder eller use cases som angivet i bilag 3 og dermed udgør en høj risiko for menneskers sundhed, sikkerhed eller grundlæggende rettigheder.

HØJRISIKO-AI-SYSTEMER (UDVALGTE) (2/2)

Annex III

HIGH-RISK AI SYSTEMS REFERRED TO IN ARTICLE 6(2)

High-risk AI systems pursuant to Article 6(2) are the AI systems listed in any of the following areas:

1. Biometrics, insofar as their use is permitted under relevant Union or national law
 - (a) Remote biometric identification systems.
This shall not include AI systems intended to be used for biometric verification whose sole purpose is to confirm that a specific natural person is the person he or she claims to be;
 - (aa) AI systems intended to be used for biometric categorisation, according to sensitive protected attributes or characteristics based on the inference of those attributes or characteristics.
(ab) AI systems intended to be used for emotion recognition;
2. Critical infrastructure:
 - (a) AI systems intended to be used as safety components in the operation of critical digital infrastructure, road traffic and heating and electricity.
3. Education and vocational training:
 - (a) AI systems intended to be used to determine access or admission of natural persons to educational and vocational training institutions;
 - (b) AI systems intended to be used to evaluate learning outcomes where the results of the evaluation are used to steer the learning process of natural persons in educational and vocational training institutions at all levels.
 - (ba) AI systems intended to be used for the purpose of assessing the appropriate level of education that individual will receive or will be able to access, in the context

- (bb) AI systems intended to be used for monitoring students during tests in the context of work-related institutions;
4. Employment, workers management and access to services:
 - (a) AI systems intended to be used for recruitment, notably to place targeted job advertisements and to evaluate candidates;
 - (b) AI systems intended to be used to make decisions affecting terms or conditions of work-related relationships, promotion and termination of work-related contractual relationships, to allocate tasks based on individual behavior or personal traits or characteristics and to monitor and evaluate performance and behavior of persons in such relationships.

4(a) AI systems intended to be used for recruitment or selection of natural persons, notably for placing targeted job advertisements screening or filtering applications, evaluating candidates in the course of interviews or tests.

5(b) AI systems intended to be used to evaluate the creditworthiness of natural persons or establish their credit score, with the exception of AI systems used for the purpose of detecting financial fraud.

5(ca) AI systems intended to be used for risk assessment and pricing in relation to natural persons in the case of life and health insurance.

authorities or on their behalf to assess the risk of a natural person to become a victim of criminal offences;

- (e) AI systems intended to be used by law enforcement authorities or on their behalf or by Union institutions, agencies, offices or bodies in support of law enforcement authorities for assessing the risk of a natural person of offending or re-offending not solely based on profiling of natural persons as referred to in Article 3(4) of Directive (EU) 2016/680 or to assess personal traits and characteristics or past criminal

border control management, for the purpose of detecting, recognising or identifying natural persons with the exception of verification of travel documents;

8. Administration of justice and democratic processes:

- (a) AI systems intended to be used by a judicial authority or on their behalf to assist a judicial authority in researching and interpreting facts and the law and in applying the law to a concrete set of facts or used in a similar way in alternative dispute resolution
- (aa) AI systems intended to be used for influencing the outcome of an election or referendum or the voting behaviour of natural persons in the exercise of their vote in elections or referenda. This does not include AI systems whose output natural persons are not directly exposed to, such as tools used to organise, optimise and structure political campaigns from an administrative and logistic point of view.
deleted

relevant Union or national law:

- (a) AI systems intended to be used by competent public authorities as polygraphs and similar tools;

(b) AI systems intended to be used by or on behalf of competent public authorities or by agencies or bodies to assess a risk, including a security risk, a risk of terrorism or a health risk, posed by a natural person who intends to enter or remain on the territory of a Member State;



BEGRÆNSET ELLER LAV/INGEN RISIKO

- For systemer med en **begrænset** risiko, som er opregnet i art. 52, gælder en række gennemsigthedsforpligtelser. Dette gælder følgende systemer:

- AI-systemer, der er beregnet til at interagere med fysiske personer
- AI-systemer til følelsesgenkendelse eller et system til biometrisk kategorisering
- AI-system, der genererer eller manipulerer tekst, lyd eller visuelt indhold, som fejlagtigt fremstår som autentisk eller sandfærdigt, og som indeholder skildringer af personer, der ser ud til at sige eller gøre ting, de ikke har sagt eller gjort, uden deres samtykke ("deepfake") (uformel oversættelse af Parlamentets kompromisforslag).

- For andre AI-systemer end nævnt i art. 5, 6 eller 52 gælder der ingen specifikke krav, og disse kan derfor omsættes og anvendes frit. De er dog stadig omfattet af forordningen.
- AI-forordningen fastsætter ikke krav om gennemførelse af en egentlig risikovurdering, men derimod krav om en vurdering af, om det pågældende AI-system er omfattet af art. 5, 6 eller 52.
- En egentlig risikovurdering kan dog være påkrævet efter anden lovgivning, såsom GDPR, DORA og/eller den finansielle regulering

FORPLIGTELSER VED HØJRISIKOSYSTEMER

FORSKELLIGE FORPLIGTELSE AFHÆNGIG AF ROLLE

Udbydere (art. 16)

- Compliance med kapitel 2 i AIF, f.eks.
 - Risikostyringsystemer
 - Krav til data og data governance
 - Teknisk dokumentation
 - Logning og
 - Menneskeligt tilsyn
- Kvalitetsstyringsystem (art. 17)
- Dokumentationsforpligtelser (art. 18)
- Forenelighedsvurderinger art. 16, stk. 1, litra ea og art. 43
- CE-mærkning
- "Corrective actions" og informationsforpligtelser
- M.fl.

Brugere (art. 29)

- Menneskeligt tilsyn
- "Necessary competence, training, authority and support" til personer, der gennemfører menneskeligt tilsyn
- Relevante og repræsentative input data
- Monitorere AI-systemets
- Informationsforpligtelse ved begrundet mistanke om risici ved brugen af AI systemet i overensstemmelse med brugsanvisningen samt ved "serious incidents".
- Opbevare logs
- Informere fysiske personer om automatiske beslutninger genereret af et højrisiko AI system
- I visse tilfælde fundamental rights impact assessment (art. 29a)

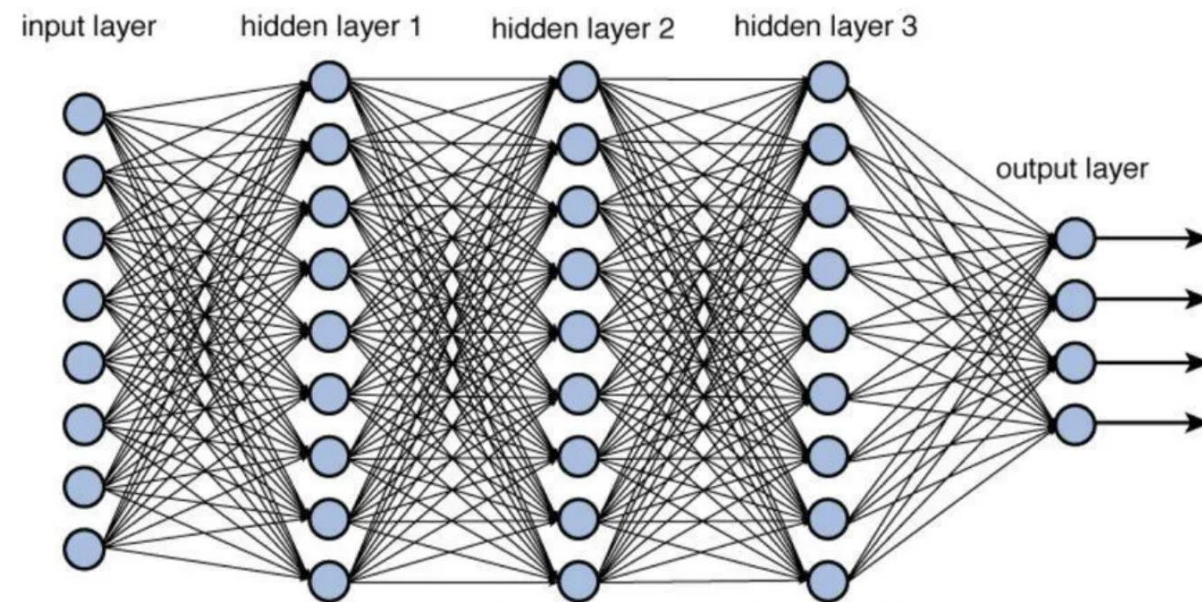
Brugere, der er finansielle institutioner underlagt krav om deres intern governance o.lign. efter den EU-retlige finansielle regulering, skal opfylde disse forpligtelser som en del af dokumentationen efter den finansielle regulering

GENNEMSIGTIGHED I AI- SYSTEMER – INTERNT OG EKSTERNT

TRANSPARENSPROBLEMET ("BLACK BOX"-PROBLEMET)

- Hvordan forklarer vi beslutninger i machine learning, deep learning og neurale netværk?
- Ikke tale om "hård kodning" i den forstand, at alle kriterier er fastlagt på forhånd efter en deduktiv metode.
- Vi kan ikke nødvendigvis frembringe et beslutningstræ.

Dybt neuralt netværk med flere skjulte lag



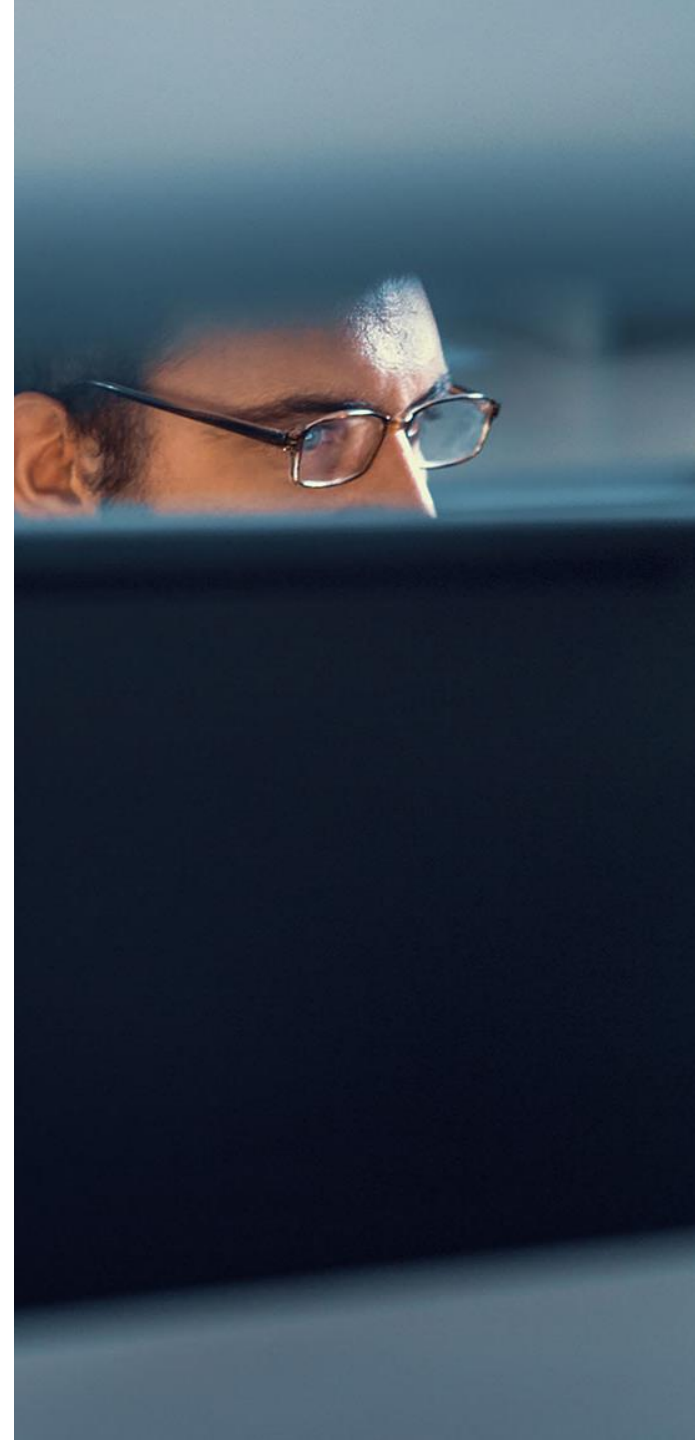
Kilde: <https://towardsdatascience.com/training-deep-neural-networks-9fdb1964b964>

REGLERNE OM TRANSPARENS OG INFORMATION M.V. I DAG

- GDPR artikel 5, stk. 1, litra a: Personoplysninger skal behandles lovligt, rimeligt og på en gennemsigtig måde i forhold til den registrerede («lovlighed, rimelighed og gennemsigtighed«).
- Artikel 12 – om meningsfulde, lettilgængelige oplysninger.
- GDPR artikel 13-14 – oplysningspligten.
- Indsigtsret, jf. artikel 15.
- Udvidet ret til underretning ved fuldautomatiske afgørelser efter artikel 22, hvor hensynet til information er størst – det kommer vi tilbage til.

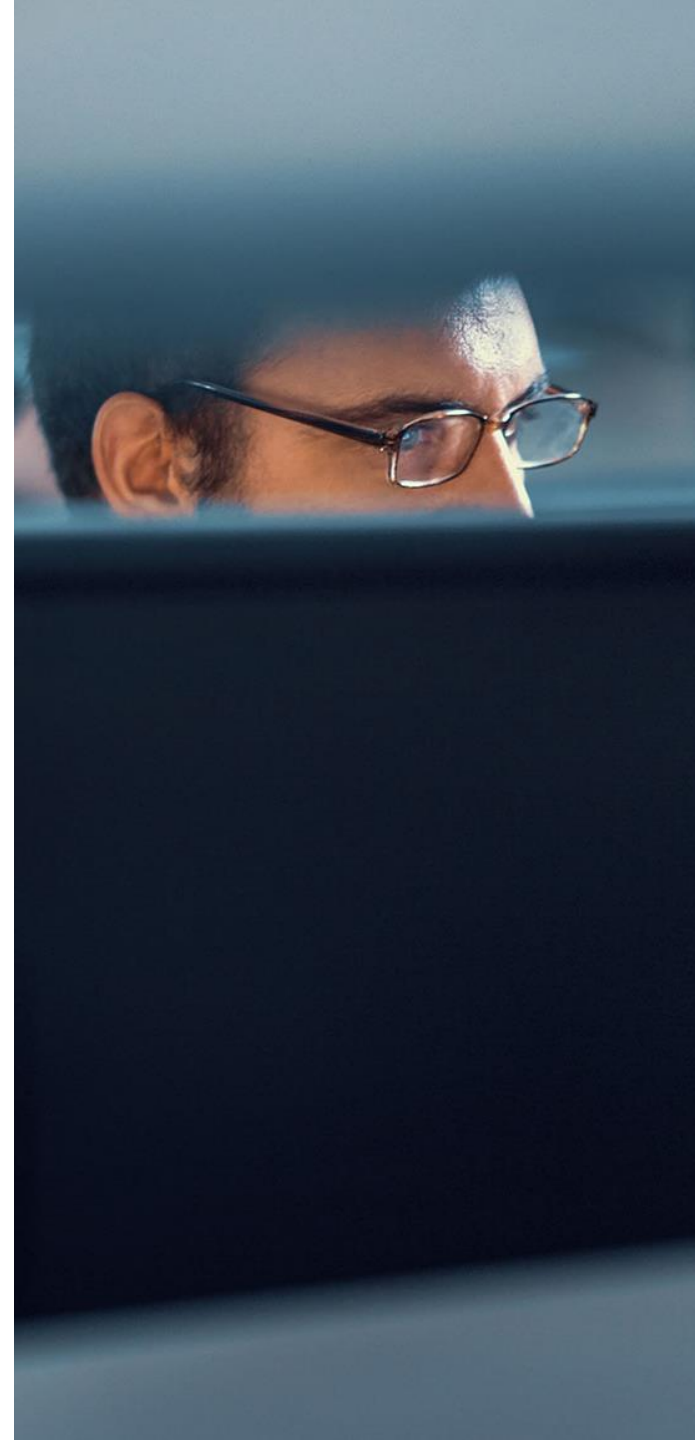
MENNESKELIGT TILSYN (1/2) – ARTIKEL 14

- **Højrisiko-AI-systemer** skal være designet og udviklet på en sådan måde, at de effektivt kan overvåges af fysiske personer.
- Stå i et rimeligt forhold til de risici, der er forbundet med systemet.
- Fysiske personer, som er ansvarlige for at sikre menneskelig tilsyn, skal have et **tilstrækkeligt niveau af AI-færdigheder**.
- Skal have nødvendig støtte og bemyndigelse til at udøve den funktion, i den periode, AI-systemet er i brug, og adgang til grundig undersøgelse efter en utilsigtet hændelse.
- **Formål med tilsyn:** Forebygge eller minimere de risici for menneskers sundhed, sikkerhed eller grundlæggende rettigheder eller miljøet, der kan opstå, når et højrisiko-AI-system anvendes.



MENNESKELIGT TILSYN (2/2) – ARTIKEL 14

- Ved tilrettelæggelse af tilsynet skal der tages højde for følgende:
 1. De specifikke risici,
 2. Niveauet af automatisering
 3. Kontekst for AI-systemet
- Sikres ved én eller flere af følgende foranstaltninger afhængig af rolle:
 - a) Menneskeligt tilsyn er fastlagt og, hvis det er teknisk muligt, indbygget i højrisiko-AI-systemet fra udbyderens side, inden systemet bringes i omsætning eller tages i brug
 - b) Menneskeligt tilsyn er fastlagt fra udbyderens side, inden højrisiko-AI-systemet bringes i omsætning eller tages i brug, og er egnet til at blive gennemført af brugeren.



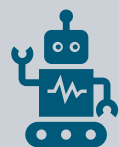
GENNEMSIGTIGHED I HØJRISIKO AI-SYSTEMER (ARTIKEL 13) (1/2)



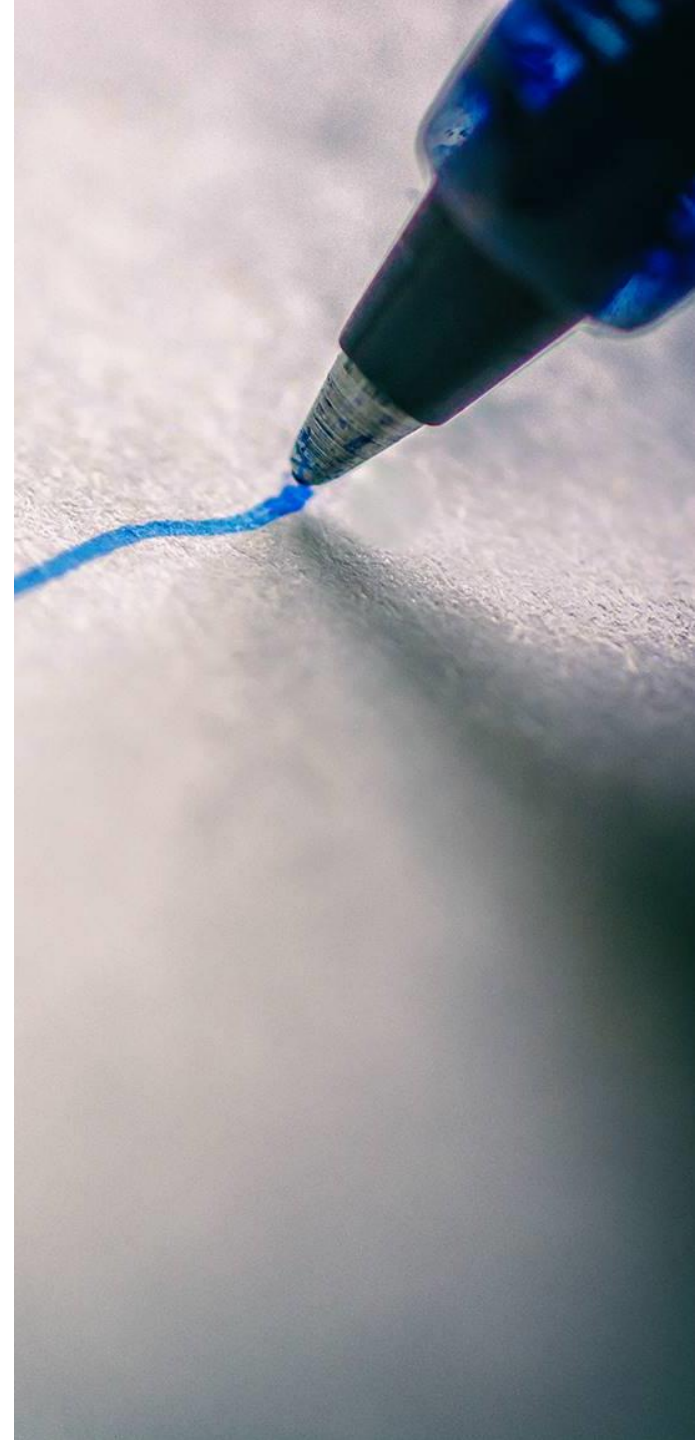
Gennemsigtighed i højrisiko-AI-systemer betyder, at alle tilgængelige, almindeligt anerkendte tekniske foranstaltninger skal bruges til at sikre, at AI-systemets output kan fortolkes af udbyderen og brugeren.



Brugeren skal være i stand til at forstå og bruge AI-systemet korrekt ved generelt at vide, hvordan AI-systemet fungerer, og hvilke data det behandler



Højrisiko-AI-systemer udformes og udvikles på en sådan måde, at deres drift er tilstrækkeligt gennemsigtig til, at udbyderne og brugerne kan forstå systemets funktioner.



GENNEMSIGTIGHED I HØJRISIKO-AI-SYSTEMER (ARTIKEL 13) (2/2)

- Højrisiko-AI-systemer ledsages af brugsanvisninger, som skal indeholde kortfattede, fuldstændige, korrekte og klare oplysninger, som er relevante, tilgængelige og forståelige for brugerne.
- Indholdsmæssige krav, herunder

- Identitet på og kontaktoplysninger for udbyderen og dennes eventuelle bemyndigede repræsentant
- AI-systemets egenskaber, kapacitet og begrænsninger for dets ydeevne
- Eventuelle ændringer af AI-systemet og dets ydeevne, som udbyderen på forhånd har fastsat på tidspunktet for den indledende overensstemmelsesvurdering
- Foranstaltninger til menneskeligt tilsyn, jf. artikel 14, herunder de tekniske foranstaltninger, der er indført for at lette brugernes fortolkning af AI-systemets output
- Eventuelle nødvendige vedligeholdelses- og plejeforanstaltninger for at sikre, at AI-systemet fungerer korrekt, herunder med hensyn til softwareopdateringer.

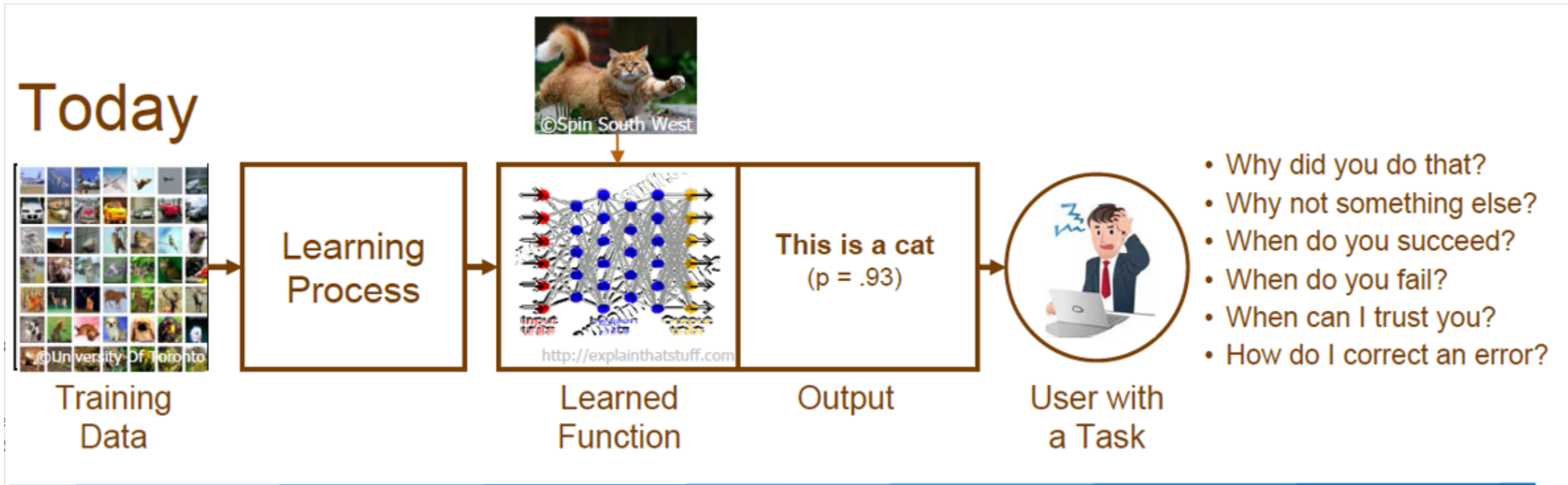
GENNEMSIGTIGHEDSFORPLIGTELSER FOR VISSE AI-SYSTEMER – ARTIKEL 52

- 1) Udbydere skal sikre, at AI-systemer, der er beregnet til at **interagere med fysiske personer**, udformes og udvikles på en sådan måde, at fysiske personer oplyses om, at de interagerer med et AI-system, medmindre dette er indlysende ud fra omstændighederne og anvendelsessammenhængen.
- 2) Brugere af et system til **følelsesgenkendelse eller et system til biometrisk kategorisering** skal oplyse de fysiske personer, der er eksponeret for systemet, om anvendelsen af systemet.
- 3) Brugere af et AI-system, der **genererer eller manipulerer billed-, lyd- eller videoindhold**, der i væsentlig grad ligner faktiske personer, genstande, steder eller andre enheder eller begivenheder, og som fejlagtigt vil fremstå ægte eller sandfærdigt ("deepfake"), skal oplyse, at indholdet er blevet genereret kunstigt eller manipuleret.

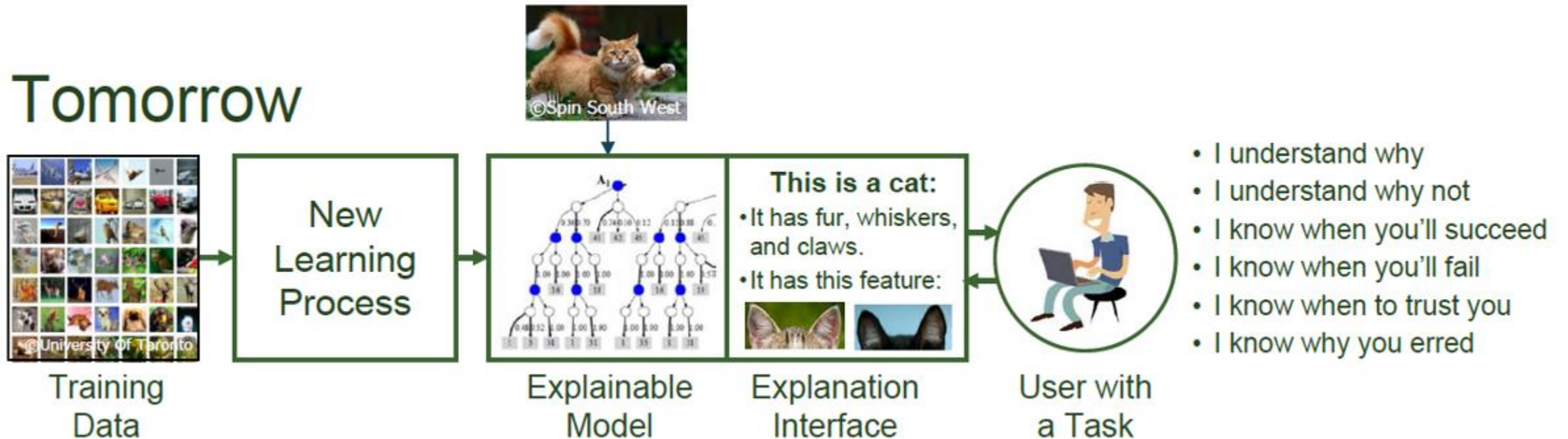
- Undtagelser for
 - (a) systemer, der er tilladt ved lov med henblik på retshåndhævelse, og for sidstnævnte tillige
 - (b) hvis anvendelsen er nødvendig for at udøve retten til ytringsfrihed eller retten til kunst og videnskab, der er sikret ved EU-charteret.



TRANSPARENS – EXPLAINABLE ARTIFICIAL INTELLIGENCE (XAI)

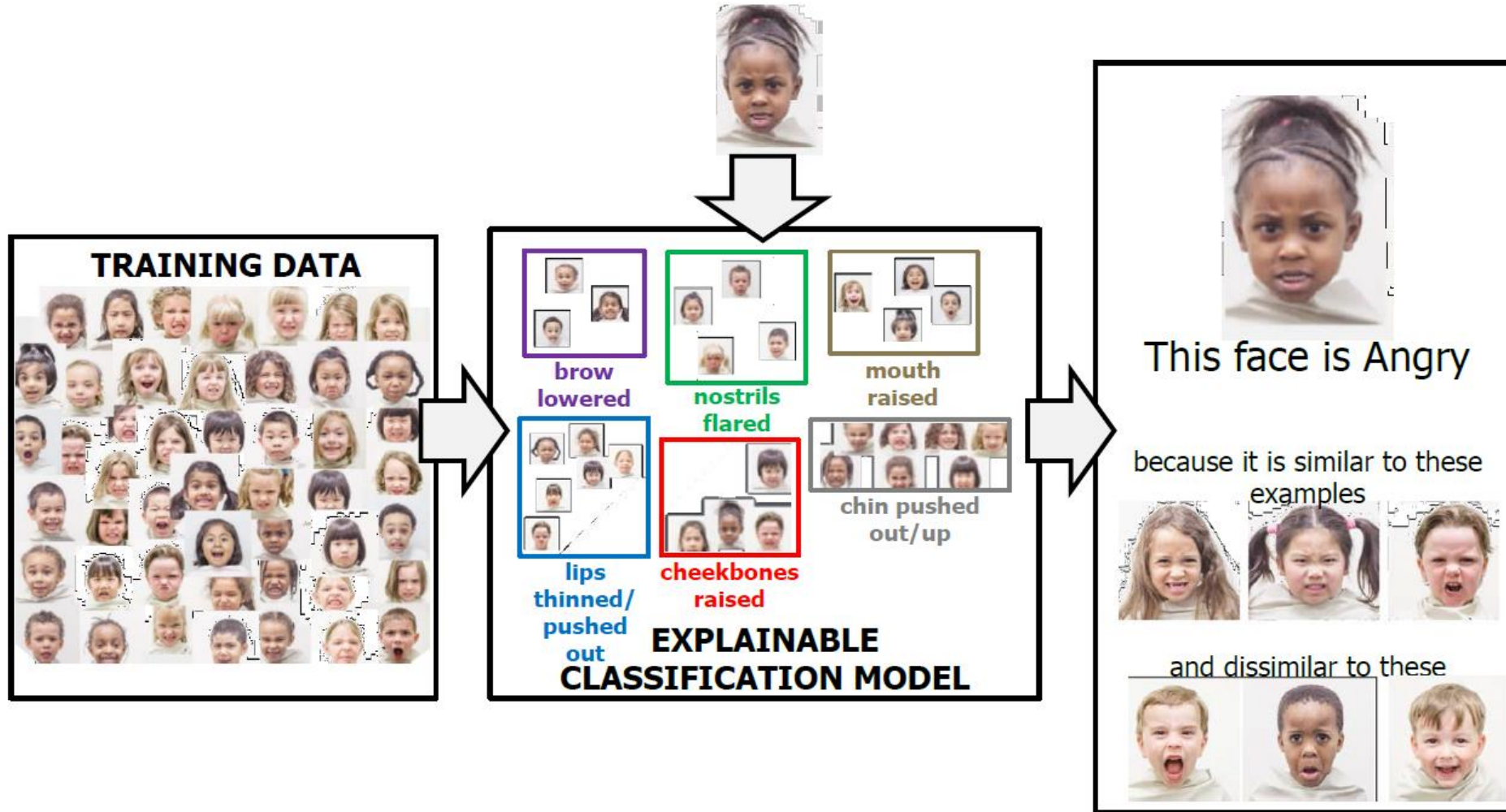


TRANSPARENS – EXPLAINABLE ARTIFICIAL INTELLIGENCE (XAI)



Kilde: DARPA

TRANSPARENS – EXPLAINABLE ARTIFICIAL INTELLIGENCE (XAI) (FORTSAT)



Kilde: DARPA

AFRUNDING

GODE RÅD



Først og fremmest: Hav styr på gældende regler i GDPR og evt. særregler.



Få et overblik over de AI-systemer, I eventuelt allerede anvender eller påtænker at anvende – hvilken risiko henhører systemet under?



Begynd allerede nu at indtænke kravene fra AI-forordningen, herunder ift. indkøb af applikationer/forhandling med leverandører, f.eks. kravsætning i udbud.



Uddannelse og awareness om reglerne.

RESPONSIBLE AI GOVERNANCE & COMPLIANCE

- Poul Schmith/Kammeradvokaten udbyder i samarbejde med DTU Compute og Datatilsynet en ny AI-uddannelse.
- Toleddet uddannelse – for generalisten og praktikereren
- Følg med på vores hjemmeside og på LinkedIn



RESPONSIBLE
AI GOVERNANCE
& COMPLIANCE

SPØRGSMÅL OG TAK FORDI I LYTTETUDE!



Kirsten Marie Donato
PARTNER, ADVOKAT

M 22 26 23 57
@ KIPE@POULSCHMITH.DK



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.