# AI Act
## - regulation / forordning

Eva Jarbekk

# Agenda

1. Situasjon i EU – trilogforhandling
2. Generelle forhold - forholdet til GDPR
3. Hva er AI?
   Omfattes GPAI, foundation models og generativ AI?
4. Risikobasert tilnærming
5. Grunnleggende forhold
6. Forbudt AI
7. Høyrisiko AI
   Hva er høyrisiko
   Kontrakter om høy-risiko
   Dokumentasjonskrav
8. Begrenset/Limited risiko
9. Noen kommentarer til slutt

Innledende betraktninger med forbehold for fragmentert rettskildebilde– ingen komplett gjennomgang av alle kriterier

# Situasjon i EU – trilogforhandling

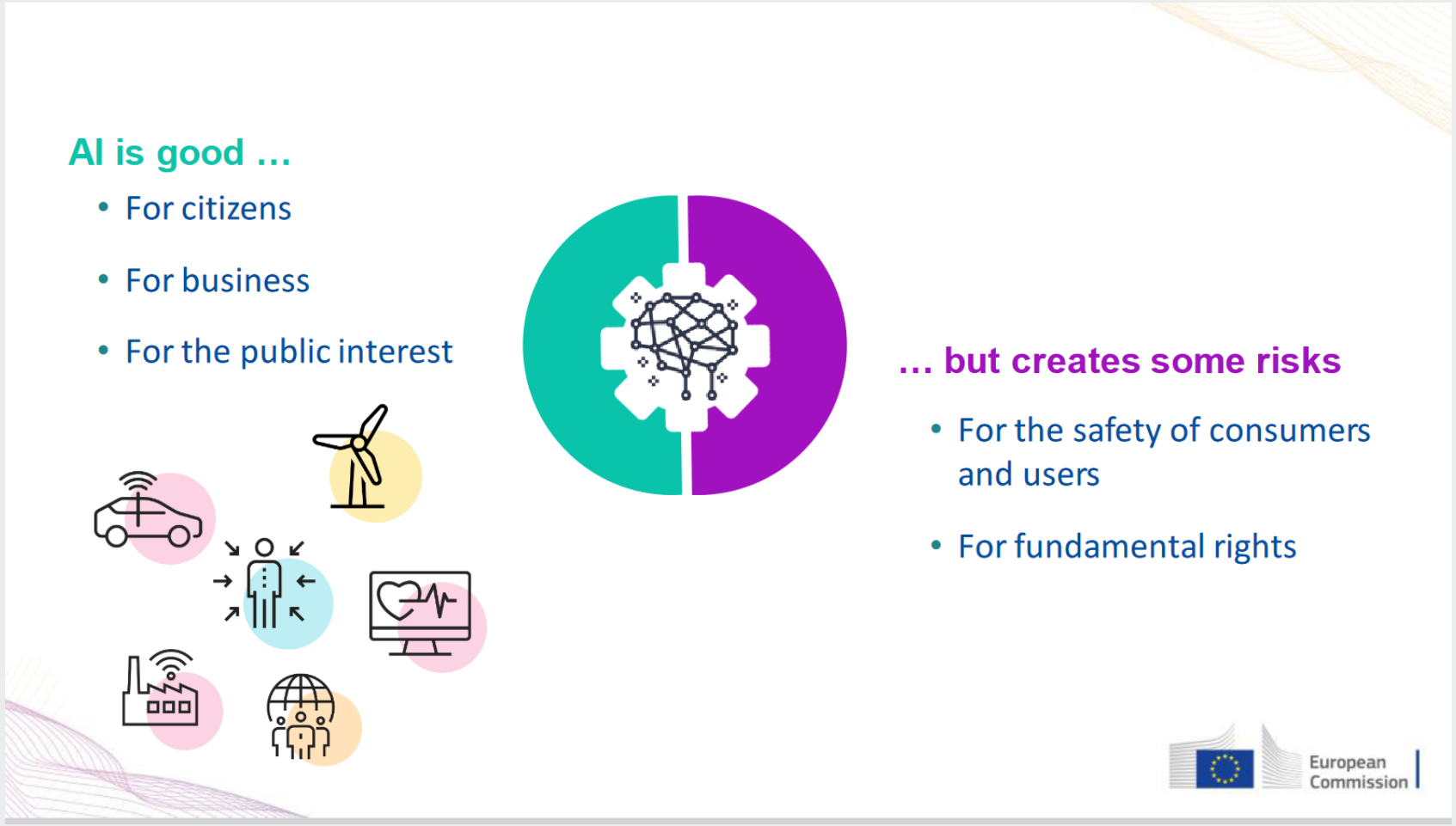
- Kommisjonens forslag 21. april 2021
- Joint opinion fra EDPS og EDPB 18. juni 2021
- Rådets kommentarer 6. desember 2022
- Parlamentets kommentarer 14. juni 2023
- Nå: trilogforhandlinger, møter er i gang
  - Spania leder arbeidet – ferdig 2023? (Valg i EU juni 2024)
- 1,5-3 års implementeringstid er foreslått – tidligst virkning i 2025

## Andre EU-initiativ:

AI Code of Conduct - non-legally binding AI
AI Pact - commitment of early compliance with the future AI Act by businesses
AI liability

# Generelt

# Litt generell bakgrunn



Recital 3 a (new)

Miljøfokus

Regulation = bindende as-is

***(3a) To contribute to reaching the carbon neutrality targets, European companies should seek to utilise all available technological advancements that can assist in realising this goal. Artificial Intelligence is a technology that has the potential of being used to process the ever-growing amount of data created during industrial, environmental, health and other processes. To facilitate investments in AI-based analysis and optimisation tools, this Regulation should provide a predictable and proportionate environment for low-risk industrial solutions.***

Forordning, men

.. noen unntak fra bindende regler

..som GDPR

***5c. This regulation shall not preclude Member States or the Union from maintaining or introducing laws, regulations or administrative provisions which are more favourable to workers in terms of protecting their rights in respect of the use of AI systems by employers, or to encourage or allow the application of collective agreements which are more favourable to workers.***

# Forholdet til GDPR

EDPB og EDPS foreslo tydeliggjøring av at GDPR compliance er en «precondition» for lansering

Ny Art 4a fra Parlamentet sier gjeldende personvernregler skal overholdes

Rapport: *https://fpf.org/blog/fpf-report-automated-decision-making-under-the-gdpr-a-comprehensive-case-law-analysis/*

- GDPR Art 22 gjelder for systemer der AI Act ikke gjelder
- Der GDPR Art 22 ikke gjelder, vil resten av GDPR gjelde
- AI Act pålegger «users» flere forpliktelser enn «controllers» - men begrepene ser ut til å bli endret underveis
- GDPR's forpliktelser vil i stor grad påhvile det AIA kaller «deployers»

## Recital 72 a (new)

## Annen hjemmel må finnes i GDPR

***(72a) This Regulation should provide the legal basis for the use of personal data collected for other purposes for developing certain AI systems in the public interest within the AI regulatory sandbox only under specified conditions in line with Article 6(4) of Regulation (EU) 2016/679, and Article 6 of Regulation (EU) 2018/1725, and without prejudice to Article 4(2) of Directive (EU) 2016/680. Prospective providers in the sandbox should ensure appropriate safeguards and cooperate with the competent authorities, including by following their guidance and acting expeditiously and in good faith to mitigate any high-risks to safety, health and the environment and fundamental rights that may arise during the development and experimentation in the sandbox. The conduct of the prospective providers in the sandbox should be taken into account when competent authorities decide over the temporary or permanent suspension of their participation in the sandbox whether to impose an administrative fine under Article 83(2) of Regulation 2016/679 and Article 57 of Directive 2016/680.***

# Recital 45 a (new)

***(45a) The right to privacy and to protection of personal data must be guaranteed throughout the entire lifecycle of the AI system. In this regard, the principles of data minimisation and data protection by design and by default, as set out in Union data protection law, are essential when the processing of data involves significant risks to the fundamental rights of individuals. Providers and users of AI systems should implement state-of-the-art technical and organisational measures in order to protect those rights. Such measures should include not only anonymisation and encryption, but also the use of increasingly available technology that permits algorithms to be brought to the data and allows valuable insights to be derived without the transmission between parties or unnecessary copying of the raw or structured data themselves.***

Hva er AI?

Omfattes GPAI, Foundation AI og generativ AI?

# Definition and technological scope of the regulation (Art. 3)

## Definition of Artificial Intelligence

- Definition of AI should be **as neutral as possible** in order to cover techniques which are not yet known/developed
- **Overall aim is to cover all AI**, including traditional symbolic AI, Machine learning, as well as hybrid systems
- **Annex I**: list of AI techniques and approaches should provide for legal certainty (adaptations over time may be necessary)

> *"a software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with"*

European Commission

Kommisjonen: AI begrenset til software "acting for human-defined objectives"

Parlamentet – bredere definisjon:

"a machine-based system that is designed to operate with varying levels of autonomy and that can, for explicit or implicit objectives, generate outputs such as predictions, recommendations, or decisions, that **influence physical or virtual environments**."

"Foundation models" – trent på "broad data at scale, is designed for generality of output, and can be adapted to a wide range of distinctive tasks."

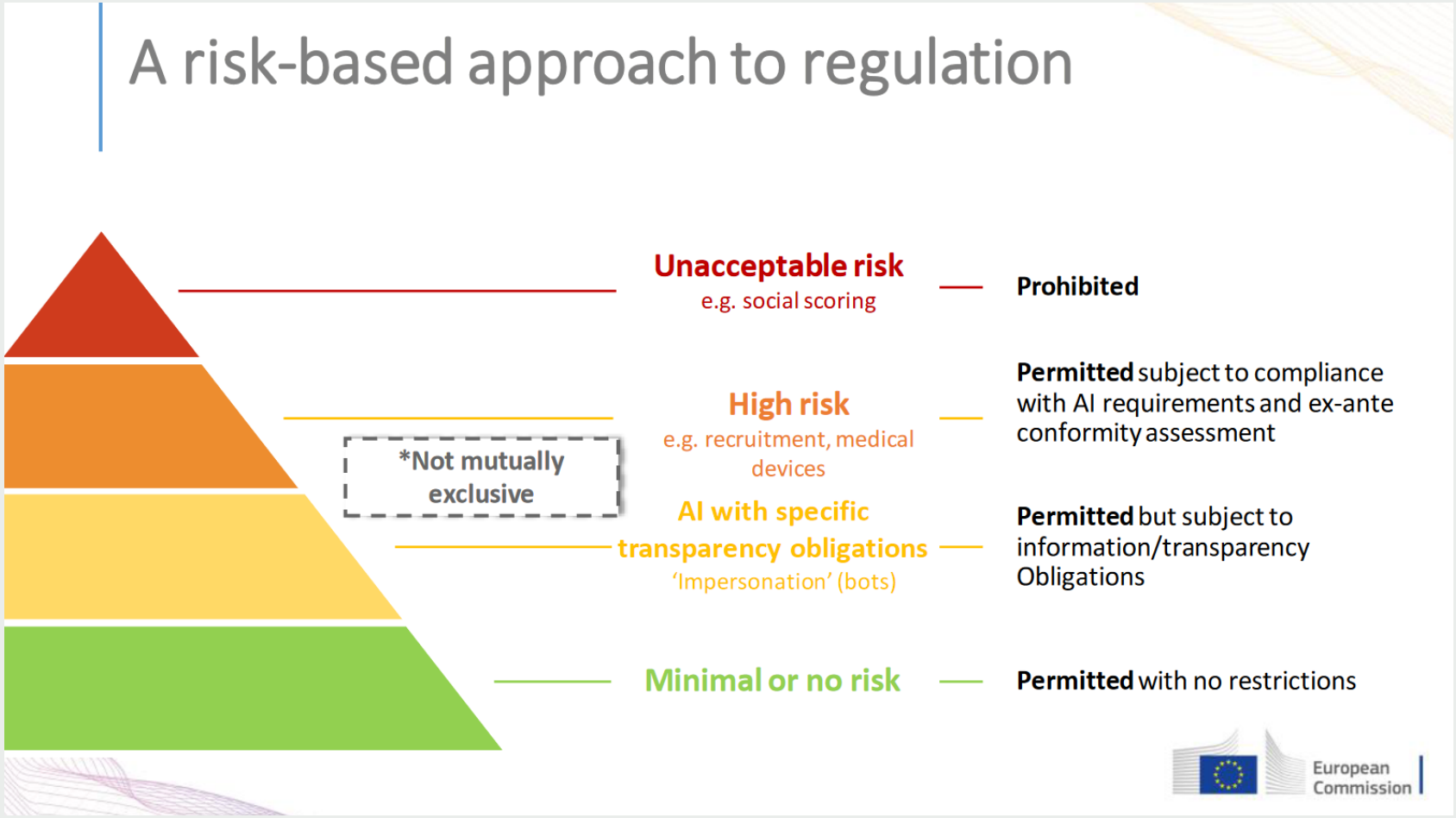
General purpose AI: generative AI Systems based on Foundation Models

- pålegges omfattende treningskrav,
- hindre ulovlig innhold,
- making publicly available documentation summarising the use of training data protected under copyright law,
- transparens-krav, bla mht "deep-fakes"

# Art 3(1) Sammensatte løsninger omfattes

AI systems “can be used as stand-alone software system, integrated into a physical product (embedded), used to serve the functionality of a physical product without being integrated therein (non-embedded) or used as an AI component of a larger system,” in which case the entire larger system should be considered as one single AI system if it would not function without the AI component in question

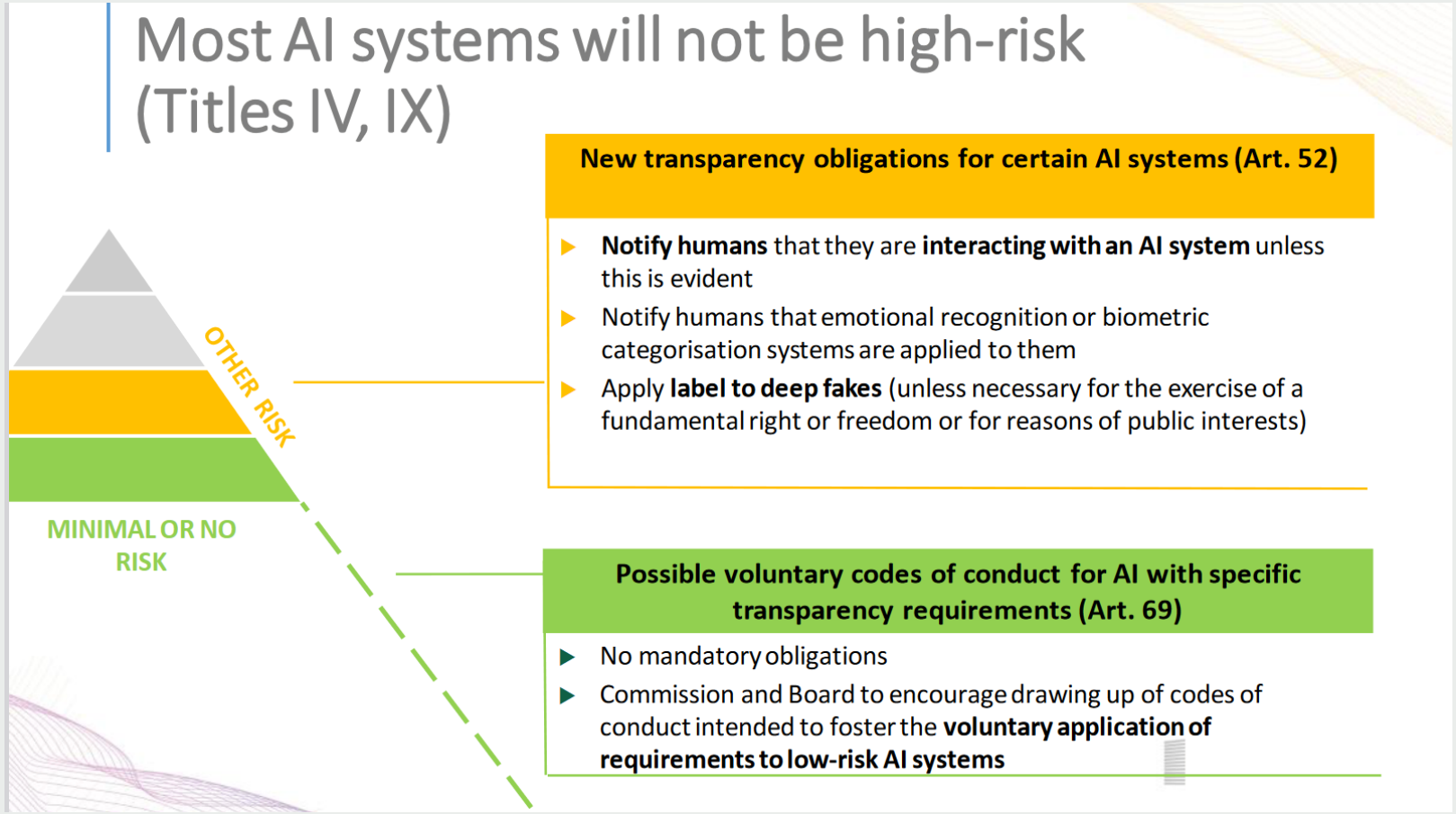
# Risikobasert tilnærming


A risk-based approach to regulation
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
European Commission

..sier kommisjonen ..

..litt uklart om riktig..

Parlamentet både strammer inn og utvanner kriteriene for høy risiko mer..



# Grunnleggende forhold

# Territoriell anvendelse

Art 2
“placing AI systems on the market or putting into service” in the EU irrespectively of whether those providers are established within the EU or a third country

Kan bli landmark benchmark regelverk for AI – som GDR ble det for personvern

Men også: Ønsker å forhindre forbudt praksis fra å bli "eksportert” ut av EØS av tilbydere eller distributører utenfor EØS

# Recital 10

(10) In order to ensure a level playing field and an effective protection of rights and freedoms of individuals across the Union ***and on international level***, the rules established by this Regulation should apply to providers of AI systems in a nondiscriminatory manner, irrespective of whether they are established within the Union or in a third country, and to ***deployers*** of AI systems established within the Union. ***In order for the Union to be true to its fundamental values, AI systems intended to be used for practices that are considered unacceptable by this Regulation, should equally be deemed to be unacceptable outside the Union because of their particularly harmful effect to fundamental rights as enshrined in the Charter. Therefore it is appropriate to prohibit the export of such AI systems to third countries by providers residing in the Union.***

# Grunnprinsipper

## Article 4 a (new) – paragraph 1

(‘operator’ means the provider, ***the deployer***, the authorised representative, the importer and the distributor)

(Sml GDPR art 5)

***Article 4 a***

***General principles applicable to all AI systems***

***1. All operators falling under this Regulation shall make their best efforts to develop and use AI systems or foundation models in accordance with the following general principles establishing a high- level framework that promotes a coherent human-centric European approach to ethical and trustworthy Artificial Intelligence, which is fully in line with the Charter as well as the values on which the Union is founded:***

***a) ‘human agency and oversight’ means that AI systems shall be developed and used as a tool that serves people, respects human dignity and personal autonomy, and that is functioning in a way that can be appropriately controlled and overseen by humans;***

***b) ‘technical robustness and safety’ means that AI systems shall be developed and used in a way to minimize unintended and unexpected harm as well as being robust in case of unintended problems and being resilient against attempts to alter the use or performance of the AI system so as to allow unlawful use by malicious third parties;***

***c) ‘privacy and data governance’ means that AI systems shall be developed and used in compliance with existing privacy and data protection rules, while processing data that meets high standards in terms of quality and integrity;***

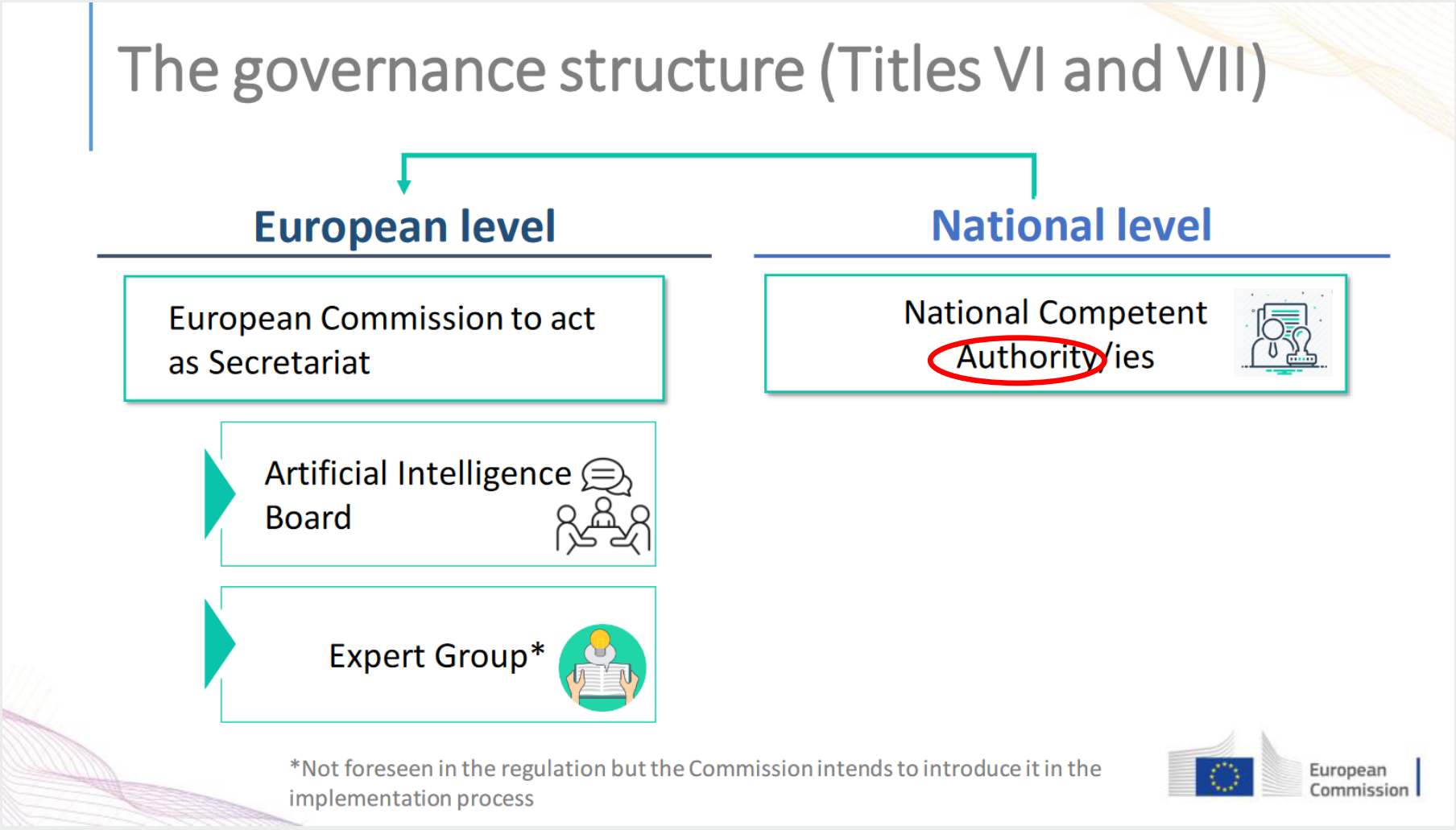
***d) ‘transparency’ means that AI systems shall be developed and used in a way that allows appropriate traceability and explainability, while making humans aware that they communicate or interact with an AI system as well as duly informing users of the capabilities and limitations of that AI system and affected persons about their rights;.***

***e) ‘diversity, non-discrimination and fairness’ means that AI systems shall be developed and used in a way that includes diverse actors and promotes equal access, gender equality and cultural diversity, while avoiding discriminatory impacts and unfair biases that are prohibited by Union or national law;***

***f) ‘social and environmental well-being’ means that AI systems shall be developed and used in a sustainable and environmentally friendly manner as well as in a way to benefit all human beings, while monitoring and assessing the long- term impacts on the individual, society and democracy.***

**Kun ett tilsyn pr land**
ikke sektorvise tilsyn som kommisjonen åpnet for

Fordeler og ulemper!
HR: må forholde seg til arbeidstilsyn, Datatilsyn og AI-tilsyn



Kommisjonens AI Board (sml EDPB)

blir «AI office»

Som blant annet skal:

1. Monitor implementation of the AI Act
2. Providing guidance
3. Foster cooperation between national authorities
4. Coordinate joint investigations

Recital 80 a (new)

(ganske likt GDPR)

***(80a) Given the objectives of this Regulation, namely to ensure an equivalent level of protection of health, safety and fundamental rights of natural persons, to ensure the protection of the rule of law and democracy, and taking into account that the mitigation of the risks of AI system against such rights may not be sufficiently achieved at national level or may be subject to diverging interpretation which could ultimately lead to an uneven level of protection of natural persons and create market fragmentation, the national supervisory authorities should be empowered to conduct joint investigations or rely on the union safeguard procedure provided for in this Regulation for effective enforcement. Joint investigations should be initiated where the national supervisory authority have sufficient reasons to believe that an infringement of this Regulation amount to a widespread infringement or a widespread infringement with a Union dimension, or where the AI system or foundation model presents a risk which affects or is likely to affect at least 45 million individuals in more than one Member State.***

## Klageadgang for individer

Kommisjonen: ikke for enkeltpersoner

Parlamentet:
Informasjonsplikt for høyrisiko AI, rett til en forklaring og **klagerett** til nasjonalt tilsyn

# Ansvar

- Vanlige ansvarsregler gjelder
- GDPR gjelder
- Liability ikke nevnt i AI Act
- Kommisjonsforslag: AI Liability Directive (28 September 2022)
    - sivilrettslig erstatningsansvar utenfor kontrakt
    - regler for fremleggelse av dokumentasjon for høyrisikosystemer med kunstig intelligens for å gjøre det mulig for saksøker å underbygge et eventuelt erstatningsansvar
    - regler for bevisbyrden ved skyldansvar for skader forårsaket av AI
    - om saksøkte ikke imøtekommer en domstols anmodning om fremleggelse av dokumentasjon, foreslås en presumsjon for at saksøke ikke har utvist tilstrekkelig aktsomhet, likevel slik at saksøkte fortsatt har mulighet til å motbevise dette

# Generelt behov for å utdanne mennesker om AI

Article 4 b (new)

***Article 4 b***

***AI literacy***

1. ***When implementing this Regulation, the Union and the Member States shall promote measures for the development of a sufficient level of AI literacy, across sectors and taking into account the different needs of groups of providers, deployers and affected persons concerned, including through education and training, skilling and reskilling programmes and while ensuring proper gender and age balance, in view of allowing a democratic control of AI systems***
2. ***Providers and deployers of AI systems shall take measures to ensure a sufficient level of AI literacy of their staff and other persons dealing with the operation and use of AI systems on their behalf, taking into account their technical knowledge, experience, education and training and the context the AI systems are to be used in, and considering the persons or groups of persons on which the AI systems are to be used.***
3. ***Such literacy measures shall consist, in particular, of the teaching of basic notions and skills about AI systems and their functioning, including the different types of products and uses, their risks and benefits.***
4. ***A sufficient level of AI literacy is one that contributes, as necessary, to the ability of providers and deployers to ensure compliance and enforcement of this Regulation.***

## Sandboxes blir obliatorisk

Recital 71

(overly restrictive law would stifle AI innovation)

(71) Artificial intelligence is a rapidly developing family of technologies that requires regulatory oversight and a safe ***and controlled*** space for experimentation, while ensuring responsible innovation and integration of appropriate safeguards and risk mitigation measures. To ensure a legal framework that ***promotes innovation,*** is future-proof***,*** and resilient to disruption, Member States should establish ***at least one*** artificial intelligence regulatory ***sandbox*** to facilitate the development and testing of innovative AI systems under strict regulatory oversight before these systems are placed on the market or otherwise put into service. ***It is indeed desirable for the establishment of regulatory sandboxes, whose establishment is currently left at the discretion of Member States, as a next step to be made mandatory with established criteria. That mandatory sandbox could also be established jointly with one or several other Member States, as long as that sandbox would cover the respective national level of the involved Member States. Additional sandboxes may also be established at different levels, including cross Member States, in order to facilitate cross-border cooperation and synergies. With the exception of the mandatory sandbox at national level, Member States should also be able to establish virtual or hybrid sandboxes. All regulatory sandboxes should be able to accommodate both physical and virtual products. Establishing authorities should also ensure that the regulatory sandboxes have the adequate financial and human resources for their functioning.***

# SMB prioriteres inn i sandbox

# En viss mulighet for viderebruk av PO fra sandbox i Art 54

*Article 54*

*Further processing of personal data for developing certain AI systems in the public interest in the AI regulatory sandbox*

1. In the AI regulatory sandbox personal data lawfully collected for other purposes shall be processed for the purposes of developing and testing certain innovative AI systems in the sandbox under the following conditions:

   (a) the innovative AI systems shall be developed for safeguarding substantial public interest in one or more of the following areas:

      (i) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, under the control and responsibility of the competent authorities. The processing shall be based on Member State or Union law;

      (ii) public safety and public health, including disease prevention, control and treatment;

      (iii) a high level of protection and improvement of the quality of the environment;

   (b) the data processed are necessary for complying with one or more of the

AIA gjelder for

Provider (developer, utvikler)

Deployers (tidl. Users)
(De som importerer og bruker)

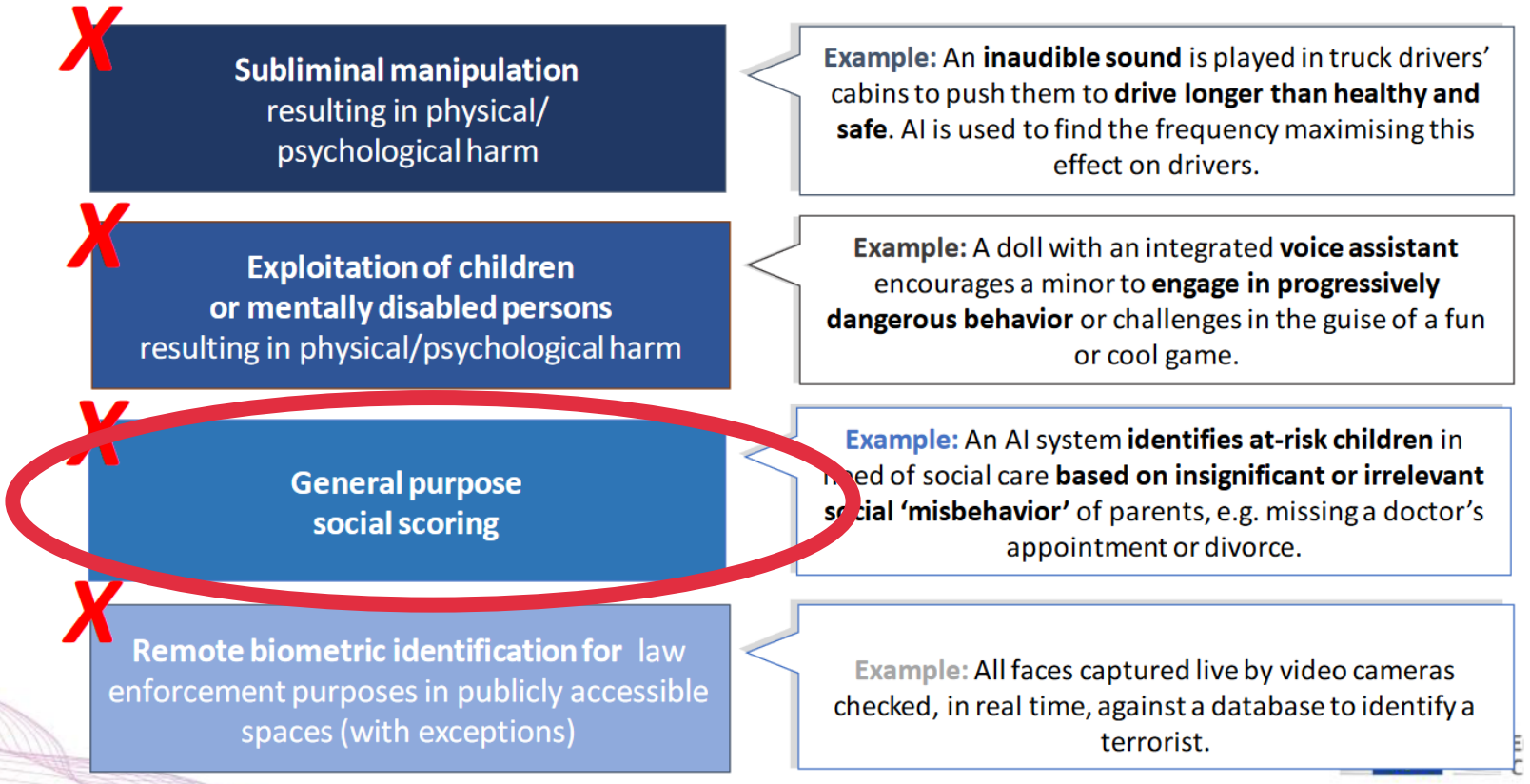
Unntak: personal non-professional activity

## Høye bøtesatser

- Brudd på regelverket om forbudt AI - opp til 40 millioner euro eller 7 % av årlig omsetningen
- Brudd på art. 10 og 13 om transparens og personvern - opp til 20 millioner euro eller 4 % av årlig omsetning
- Andre brudd på AI Act kan gi bøter opp til 10 millioner euro eller 2 % av årlig omsetning

# Forbudt AI

# AI that contradicts EU values is prohibited (Title II, Article 5)



# Utvidet av parlamentet

- Real-time remote biometric identification systems in publicly accessible spaces (mye debattert)
- Analysis of recorded footage of publicly accessible spaces through 'post' remote biometric identification systems, with a narrow exception linked to specific and particularly serious crime and subject to a pre-judicial authorization
- Biometric categorization systems using sensitive characteristics
- Predictive policing systems (based on profiling, location, or past criminal behavior)
- Emotion recognition systems in law enforcement, border management, the workplace, and educational institutions
- Untargeted scraping of facial images from the Internet or closed-circuit television footage to create facial recognition databases.

# Recital 9

..viktig hva som er offentlig sted..

(9) For the purposes of this Regulation the notion of publicly accessible space should be understood as referring to any physical place that is accessible to the public, irrespective of whether the place in question is privately or publicly owned ***and regardless of the potential capacity restrictions***. Therefore, the notion does not cover places that are private in nature and normally not freely accessible for third parties, including law enforcement authorities, unless those parties have been specifically invited or authorised, such as homes, private clubs, offices, warehouses and factories. Online spaces are not covered either, as they are not physical spaces. However, the mere fact that certain conditions for accessing a particular space may apply, such as admission tickets or age restrictions, does not mean that the space is not publicly accessible within the meaning of this Regulation. Consequently, in addition to public spaces such as streets, relevant parts of government buildings and most transport infrastructure, spaces such as cinemas, theatres, ***sports grounds, schools, universities, relevant parts of hospitals and banks, amusement parks, festivals,*** shops and shopping centres are normally also publicly accessible. Whether a given space is accessible to the public should however be determined on a case-by-case basis, having regard to the specificities of the individual situation at hand.

# Recital 16

(16) The placing on the market, putting into service or use of certain AI systems ***with the objective to or the effect of materially distorting*** human behaviour, whereby physical or psychological harms are likely to occur, should be forbidden. ***This limitation should be understood to include neuro-technologies assisted by AI systems that are used to monitor, use, or influence neural data gathered through brain-computer interfaces insofar as they are materially distorting the behaviour of a natural person in a manner that causes or is likely to cause that person or another person significant harm.*** Such AI systems deploy subliminal components individuals cannot perceive or exploit vulnerabilities of ***individuals*** and ***specific groups of persons*** due to their ***known or predicted personality traits,*** age, physical or mental incapacities***, social or economic situation***. They do so with the intention to ***or the effect of*** materially ***distorting*** the behaviour of a person and in a manner that causes or is likely to cause ***significant*** harm to that or another person ***or groups of persons, including harms that may be accumulated over time.*** The intention ***to distort the behaviour*** may not be presumed if the distortion results from factors external to the AI system which are outside of the control of the provider or the user***, such as factors that may not be reasonably foreseen and mitigated by the provider or the deployer of the AI system. In any case, it is not necessary for the provider or the deployer to have the intention to cause the significant harm, as long as such harm results from the manipulative or exploitative AI-enabled practices. The prohibitions for such AI practices is complementary to the provisions contained in Directive 2005/29/EC, according to which unfair commercial practices are prohibited, irrespective of whether they carried out having recourse to AI systems or otherwise. In such setting, lawful commercial practices, for example in the field of advertising, that are in compliance with Union law should not in themselves be regarded as violating prohibition.*** Research for legitimate purposes in relation to such AI systems should not be stifled by the prohibition, if such research does not amount to use of the AI system in human- machine relations that exposes natural persons to harm and such research is carried out in accordance with recognised ethical standards for scientific research ***and on the basis of specific informed consent of the individuals that are exposed to them or, where applicable, of their legal guardian.***

## Recital 16 a (new)

***(16a) AI systems that categorise natural persons by assigning them to specific categories, according to known or inferred sensitive or protected characteristics are particularly intrusive, violate human dignity and hold great risk of discrimination. Such characteristics include gender, gender identity, race, ethnic origin, migration or citizenship status, political orientation, sexual orientation, religion, disability or any other grounds on which discrimination is prohibited under Article 21 of the Charter of Fundamental Rights of the European Union, as well as under Article 9 of Regulation (EU)2016/769. Such systems should therefore be prohibited.***

# Høyrisiko AI

# Hva er høyrisiko

# Hva er høyrisiko?

## Se AIA Annex III

Parlamentet presiserer høyrisikoområder i Annex III til å være AI-systemer som kan gi betydelig skade på

- Folks helse (kommisjonen foreslo også vurdering og rating i forsikring, det er nå utelatt)
- Sikkerhet
- Grunnleggende rettigheter
- **Miljøet**
- Påvirke velgere og valgresultatet
- For anbefalingssystemer som brukes av sosiale medieplattformer som er utpekt som "veldig store nettplattformer" ihht DSA

# Og ekstra krav

Parlamentet:

Et AI-system er ikke automatisk høyrisiko fordi det er oppført i vedlegg III

Det må også utgjøre en **betydelig risiko** for skade på helse, sikkerhet og grunnleggende rettigheter eller **miljøet**

Se art 3 om betydelig risiko

Kommisjonen skal gi retningslinjer for betydelig risiko er

Article 3 – paragraph 1 – point 1 b (new)

***(1b) 'significant risk' means a risk that is significant as a result of the combination of its severity, intensity, probability of occurrence, and duration of its effects, and its the ability to affect an individual, a plurality of persons or to affect a particular group of persons;***

# Recital 27

(27) High-risk AI systems should only be placed on the Union market***,*** put into service ***or used*** if they comply with certain mandatory requirements. Those requirements should ensure that high-risk AI systems available in the Union or whose output is otherwise used in the Union do not pose unacceptable risks to important Union public interests as recognised and protected by Union law***, including fundamental rights, democracy, the rule or law or the environment. In order to ensure alignment with sectoral legislation and avoid duplications, requirements for high-risk AI systems should take into account sectoral legislation laying down requirements for high-risk AI systems included in the scope of this Regulation, such as Regulation (EU) 2017/745 on Medical Devices and Regulation (EU) 2017/746 on In Vitro Diagnostic Devices or Directive 2006/42/EC on Machinery***. AI systems identified as high-risk should be limited to those that have a significant harmful impact on the health, safety and fundamental rights of persons in the Union and such limitation minimises any potential restriction to international trade, if any. ***Given the rapid pace of technological development, as well as the potential changes in the use of AI systems, the list of high-risk areas and use-cases in Annex III should nonetheless be subject to permanent review through the exercise of regular assessment.***

# Recital 32 a (new)

***(32a) Providers whose AI systems fall under one of the areas and use cases listed in Annex III that consider their system does not pose a significant risk of harm to the health, safety, fundamental rights or the environment should inform the national supervisory authorities by submitting a reasoned notification. This could take the form of a one-page summary of the relevant information on the AI system in question, including its intended purpose and why it would not pose a significant risk of harm to the health, safety, fundamental rights or the environment. The Commission should specify criteria to enable companies to assess whether their system would pose such risks, as well as develop an easy to use and standardised template for the notification. Providers should submit the notification as early as possible and in any case prior to the placing of the AI system on the market or its putting into service, ideally at the development stage, and they should be free to place it on the market at any given time after the notification. However, if the authority estimates the AI system in question was misclassified, it should object to the notification within a period of three months. The objection should be substantiated and duly explain why the AI system has been misclassified. The provider should retain the right to appeal by providing further arguments. If after the three months there has been no objection to the notification, national supervisory authorities could still intervene if the AI system presents a risk at national level, as for any other AI system on the market. National supervisory authorities should submit annual reports to the AI Office detailing the notifications received and the decisions taken.***

## Recital 33 a (new)

***(33a) As biometric data constitute a special category of sensitive personal data in accordance with Regulation 2016/679, it is appropriate to classify as high-risk several critical use-cases of biometric and biometrics-based systems. AI systems intended to be used for biometric identification of natural persons and AI systems intended to be used to make inferences about personal characteristics of natural persons on the basis of biometric or biometrics-based data, including emotion recognition systems, with the exception of those which are prohibited under this Regulation should therefore be classified as high-risk. This should not include AI systems intended to be used for biometric verification, which includes authentication, whose sole purpose is to confirm that a specific natural person is the person he or she claims to be and to confirm the identity of a natural person for the sole purpose of having access to a service, a device or premises (one-to-one verification). Biometric and biometrics-based systems which are provided for under Union law to enable cybersecurity and personal data protection measures should not be considered as posing a significant risk of harm to the health, safety and fundamental rights.***

# Recital 35

(35) ***Deployment of AI systems in education is important in order to help modernise entire education systems, to increase educational quality, both offline and online and to accelerate digital education, thus also making it available to a broader audience .*** AI systems used in education or vocational training, notably for determining access ***or materially influence decisions on admission*** or assigning persons to educational and vocational training institutions or to evaluate persons on tests as part of or as a precondition for their education ***or to assess the appropriate level of education for an individual and materially influence the level of education and training that individuals will receive or be able to access or to monitor and detect prohibited behaviour of students during tests*** should be ***classified as high-risk AI systems***, since they may determine the educational and professional course of a person's life and therefore affect their ability to secure their livelihood. When improperly designed and used, such systems ***can be particularly intrusive and*** may violate the right to education and training as well as the right not to be discriminated against and perpetuate historical patterns of discrimination***, for example against women, certain age groups, persons with disabilities, or persons of certain racial or ethnic origins or sexual orientation***.

# Recital 36

(36) AI systems used in employment, workers management and access to self-employment, notably for the recruitment and selection of persons, for making decisions ***or materially influence decisions on initiation,*** promotion and termination and for ***personalised*** task allocation ***based on individual behaviour, personal traits or biometric data***, monitoring or evaluation of persons in work-related contractual relationships, should also be classified as high-risk, since those systems may appreciably impact future career prospects***,*** livelihoods of these persons ***and workers' rights***. Relevant work-related contractual relationships should ***meaningfully*** involve employees and persons providing services through platforms as referred to in the Commission Work Programme 2021. Throughout the recruitment process and in the evaluation, promotion, or retention of persons in work-related contractual relationships, such systems may perpetuate historical patterns of discrimination, for example against women, certain age groups, persons with disabilities, or persons of certain racial or ethnic origins or sexual orientation. AI systems used to monitor the performance and behaviour of these persons may also ***undermine the essence of their fundamental*** rights to data protection and privacy. ***This Regulation applies without prejudice to Union and Member State competences to provide for more specific rules for the use of AI- systems in the employment context.***

# Recital 40 b (new)

***(40b) Considering the scale of natural persons using the services provided by social media platforms designated as very large online platforms, such online platforms can be used in a way that strongly influences safety online, the shaping of public opinion and discourse, election and democratic processes and societal concerns. It is therefore appropriate that AI systems used by those online platforms in their recommender systems are subject to this Regulation so as to ensure that the AI systems comply with the requirements laid down under this Regulation, including the technical requirements on data governance, technical documentation and traceability, transparency, human oversight, accuracy and robustness. Compliance with this Regulation should enable such very large online platforms to comply with their broader risk assessment and risk- mitigation obligations in Article 34 and 35 of Regulation EU 2022/2065. The obligations in this Regulation are without prejudice to Regulation (EU) 2022/2065 and should complement the obligations required under the Regulation (EU) 2022/2065 when the social media platform has been designated as a very large online platform. Given the European-wide impact of social media platforms designated as very large online platforms, the authorities designated under Regulation (EU) 2022/2065 should act as enforcement authorities for the purposes of enforcing this provision.***

# Recital 46

(46) Having ***comprehensible*** information on how high-risk AI systems have been developed and how they perform throughout their ***lifetime*** is essential to verify compliance with the requirements under this Regulation. This requires keeping records and the availability of a technical documentation, containing information which is necessary to assess the compliance of the AI system with the relevant requirements. Such information should include the general characteristics, capabilities and limitations of the system, algorithms, data, training, testing and validation processes used as well as documentation on the relevant risk management system. The technical documentation should be kept up to date ***appropriately throughout the lifecycle of the AI system***. ***AI systems can have a large important environmental impact and high energy consumption during their lifecyle. In order to better apprehend the impact of AI systems on the environment, the technical documentation drafted by providers should include information on the energy consumption of the AI system, including the consumption during development and expected consumption during use. Such information should take into account the relevant Union and national legislation. This reported information should be comprehensible, comparable and verifiable and to that end, the Commission should develop guidelines on a harmonised methodology for calculation and reporting of this information. To ensure that a single documentation is possible, terms and definitions related to the required documentation and any required documentation in the relevant Union legislation should be aligned as much as possible.***

## Recital 47

(47) To address the opacity that may make certain AI systems incomprehensible to or too complex for natural persons, a certain degree of transparency should be required for high-risk AI systems. Users should be able to interpret the system output and use it appropriately. High-risk AI systems should therefore be accompanied by relevant documentation and instructions of use and include concise and clear information, including in relation to possible risks to fundamental rights and discrimination, where appropriate.

## Recital 47 a (new)

***(47a) Such requirements on transparency and on the explicability of AI decision-making should also help to counter the deterrent effects of digital asymmetry and so-called 'dark patterns' targeting individuals and their informed consent.***

# Recital 60

# Verdikjeder

(60) ***Within the AI value chain multiple entities often supply tools and services but also components or processes that are then incorporated by the provider into the AI system, including in relation to data collection and pre-processing, model training, model retraining, model testing and evaluation, integration into software, or other aspects of model development. The involved entities may make their offering commercially available directly or indirectly, through interfaces, such as Application Programming Interfaces (API), and distributed under free and open source licenses but also more and more by AI workforce platforms, trained parameters resale, DIY kits to build models or the offering of paying access to a model serving architecture to develop and train models.*** In the light of ***this*** complexity of the ***AI*** value chain, ***all*** relevant third parties, ***in particular those that are*** involved in the ***development,*** sale and the ***commercial*** supply of software tools***,*** components, pre-trained models ***or data incorporated into the AI system***, or providers of network services, should ***without compromising their own intellectual property rights or trade secrets, make available the required information, training or expertise and*** cooperate, as appropriate, with providers to enable their ***control over all*** compliance ***relevant aspects of the AI system that falls*** under this Regulation. ***To allow a cost- effective AI value chain governance, the level of control shall be explicitly disclosed by each third party that supplies the provider with a tool, service, component or process that is later incorporated by the provider into the AI system.***

# Særlig om kontraktsvilkår for høyrisiko

# Recital 60 b (new)

***(60b) Rules on contractual terms should take into account the principle of contractual freedom as an essential concept in business-to-business relationships. Therefore, not all contractual terms should be subject to an unfairness test, but only to those terms that are unilaterally imposed on micro, small and medium-sized enterprises and start-ups. This concerns 'take-it-or-leave-it' situations where one party supplies a certain contractual term and the micro, small or medium-sized enterprise and start-up cannot influence the content of that term despite an attempt to negotiate it. A contractual term that is simply provided by one party and accepted by the micro, small, medium-sized enterprise or a start-up or a term that is negotiated and subsequently agreed in an amended way between contracting parties should not be considered as unilaterally imposed.***

Recital 60 d (new)
..liste over unfair terms

***(60d) Criteria to identify unfair contractual terms should be applied only to excessive contractual terms, where a stronger bargaining position is abused. The vast majority of contractual terms that are commercially more favourable to one party than to the other, including those that are normal in business-to- business contracts, are a normal expression of the principle of contractual freedom and continue to apply. If a contractual term is not included in the list of terms that are always considered unfair, the general unfairness provision applies. In this regard, the terms listed as unfair terms should serve as a yardstick to interpret the general unfairness provision.***

Hva må overholdes – Høyrisiko

Mye dokumentasjon, Se Title III, kap 2 og 3 (art 8-30)

**Gjelder providers, deployers, importører, users (ikke alt for alle)**

- Risk management system
- Dokumentere trening, validation og testdata
- Teknisk dok – vise compliance – **egen (lang) liste over dette i Annex IV**
- Record-keeping – logs while working, monitor operation

## Særlig om logger

High-risk AI systems shall be designed and developed with, the logging capabilities enabling

- the recording of energy consumption,
- the measurement or calculation of resource use
- environmental impact of the high-risk AI system

..during all phases of the system's lifecycle

# Særlig om logger

For high-risk AI systems referred to in paragraph 1, point (a) of Annex III, the logging capabilities shall provide, at a minimum:

(a) recording of the period of each use of the system (start date and time and end date and time of each use);
(b) the reference database against which input data has been checked by the system;
(c) the input data for which the search has led to a match;
(d) the identification of the natural persons involved in the verification of the results, as referred to in Article 14 (5)

# Logs, art 20

Providers of high-risk AI systems shall keep the logs automatically generated by their high-risk AI systems, to the extent such logs are under their control by virtue of a contractual arrangement with the user or otherwise by law. The logs shall be kept for a period that is appropriate in the light of the intended purpose of high-risk AI system and applicable legal obligations under Union or national law

# Art 29

Deployers og users pålegges omfattende vilkår, lignende developer, monitorering, (Art 29(3)), beholde logger for å demonstrere compliance (Art 29(5)),

Deployers of high-risk AI systems shall keep the logs automatically generated by that high-risk AI system, to the extent that such logs are under their control and are required for ensuring and demonstrating compliance with this Regulation, for ex-post audits of any reasonably foreseeable malfunction, incidents or misuses of the system, or for ensuring and monitoring for the proper functioning of the system throughout its lifecycle. Without prejudice to applicable Union or national law, the logs shall be kept for a period of at least six months. The retention period shall be in accordance with industry standards and appropriate to the intended purpose of the high-risk AI system

## **Transparens**, Art 13

Instructions for use

Information on:

- the identity and the contact details of the provider and, where applicable, of its authorised representative

- Characteristics, capabilities and limitations of performance of the high-risk AI system, its purpose; level of accuracy, robustness and cybersecurity to which the high-risk AI system has been tested, and any known and foreseeable circumstances that may have an impact on that expected level of accuracy, robustness and cybersecurity; any known or foreseeable circumstance which may lead to risks to the health and safety or fundamental rights; when appropriate, specifications for the input data, or any other relevant information in terms of the training, validation and testing data sets used, taking into account the intended purpose of the AI system, the human oversight measures , the expected lifetime of the AI system and any necessary maintenance and care measures to ensure the proper functioning

Human oversight - designed and developed in such a way, including with appropriate human-machine interface tools, that they can be effectively overseen by natural persons

En rekke (umulige?) krav om oversight i art 14(4)

Art 17 – Quality management system

## Art 19 conformity asessment

For providers - systems undergo the relevant conformity assessment procedure in accordance with Article 43, prior to their placing on the market or putting into service.

Providers shall draw up an EU declaration of conformity in accordance with CE marking of conformity

..egne retningslinjer i Art 43 og mye i Annexene
..mulighet for å be tredjepart om hjelp

Art 26

Before placing a high-risk AI system on the market, importers of such system shall ensure that:

(a) the appropriate conformity assessment procedure has been carried out by the provider of that AI system

(b) the provider has drawn up the technical documentation in accordance with Annex IV;

(c) the system bears the required conformity marking and is accompanied by the required documentation and instructions of use

**«FRIA»**

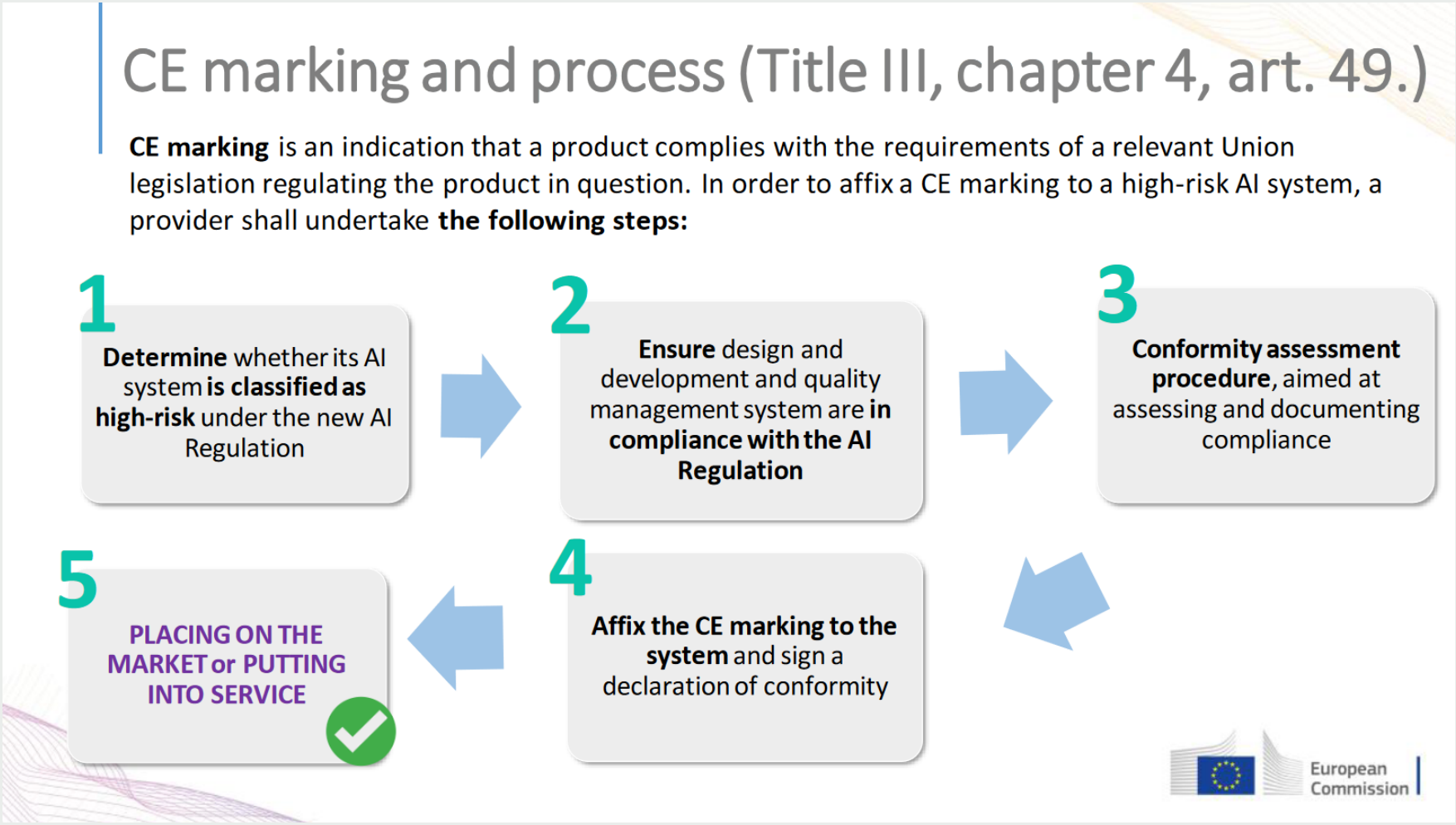
Art 29 a
om Fundamental Rights Impact Asessment

(a) a clear outline of the intended purpose for which the system will be used;
(b) a clear outline of the intended geographic and temporal scope of the system's use;
(c) categories of natural persons and groups likely to be affected by the use of the system;
(d) verification that the use of the system is compliant with relevant Union and national law on fundamental rights;
(e) the reasonably foreseeable impact on fundamental rights of putting the highrisk AI system into use;
(f) specific risks of harm likely to impact marginalised persons or vulnerable groups;
(g) reasonably foreseeable adverse impact of the use of the system on the environment;
(h) detailed plan as to how the harms and the negative impact on fundamental rights identified will be mitigated
(i) governance system the deployer will put in place, including human oversight, complaint-handling and redress

# Recital 64

(64) Given the ***complexity of high-risk AI systems and the risks that are associated to them, it is essential to develop a more adequate capacity for the application of third party conformity assessment for high-risk AI systems. However, given the current*** experience of professional pre- market certifiers in the field of product safety and the different nature of risks involved, it is appropriate to limit, at least in an initial phase of application of this Regulation, the scope of application of third-party conformity assessment for high- risk AI systems other than those related to products. Therefore, the conformity assessment of such systems should be carried out as a general rule by the provider under its own responsibility, with the only exception of AI systems intended to be used for the remote biometric identification of persons, ***or AI systems intended to be used to make inferences about personal characteristics of natural persons on the basis of biometric or biometrics-based data, including emotion recognition systems*** for which the involvement of a notified body in the conformity assessment should be foreseen, to the extent they are not prohibited.

.. + FRIA…


CE marking and process (Title III, chapter 4, art. 49.)
CE marking is an indication that a product complies with the requirements of a relevant Union legislation regulating the product in question. In order to affix a CE marking to a high-risk AI system, a provider shall undertake the following steps:
1
Determine whether its AI system is classified as high-risk under the new AI Regulation
2
Ensure design and development and quality management system are in compliance with the AI Regulation
3
Conformity assessment procedure, aimed at assessing and documenting compliance
4
Affix the CE marking to the system and sign a declaration of conformity
5
PLACING ON THE MARKET or PUTTING INTO SERVICE
European Commission

# Begrenset/Limited risiko

**TITLE IV**

**TRANSPARENCY OBLIGATIONS FOR CERTAIN AI SYSTEMS**

*Article 52*
*Transparency obligations for certain AI systems*

Art 52

- Systemer som interagerer med mennesker – chatbots
- Deep-fakes
- Emotion recognition system (..banksak..), biometric categorization system

- Krav til transparens

..noe strengere krav fra Parlamentet, men egentlig ganske få krav?

# Article 52 – paragraph 3 – subparagraph 1

3. Users of an AI system that generates or manipulates ***text***, audio or ***visual*** content that would falsely appear to be authentic or truthful ***and which features depictions of people appearing to say or do things they did not say or do, without their consent*** ('deep fake'), shall disclose ***in an appropriate, timely, clear and visible manner*** that the content has been artificially generated or manipulated***, as well as, whenever possible, the name of the natural or legal person that generated or manipulated it***. ***Disclosure shall mean labelling the content in a way that informs that the content is inauthentic and that is clearly visible for the recipient of that content. To label the content, users shall take into account the generally acknowledged state of the art and relevant harmonised standards and specifications.***

Article 52 – paragraph 3 b (new)

***3b. The information referred to in paragraphs 1 to 3 shall be provided to the natural persons at the latest at the time of the first interaction or exposure. It shall be accessible to vulnerable persons, such as persons with disabilities or children, complete, where relevant and appropriate, with intervention or flagging procedures for the exposed natural person taking into account the generally acknowledged state of the art and relevant harmonised standards and common specifications.***

# Noen kommentarer til slutt

# Lifecycle of AI systems and relevant obligations


| | |
|---|---|
| **Design in line with requirements** | Ensure AI systems **perform consistently for their intended purpose** and are **in compliance with the requirements** put forward in the Regulation |
| **Conformity assessment** | **Ex ante** conformity assessment |
| **Post-market monitoring** | Providers to **actively and systematically collect, document and analyse relevant data** on the reliability, performance and safety of AI systems throughout their lifetime, and to **evaluate continuous compliance of AI systems with the Regulation** |
| **Incident report system** | **Report serious incidents as well as malfunctioning leading to breaches to fundamental rights** (as a basis for investigations conducted by competent authorities). |
| **New conformity assessment** | **New conformity assessment** in case of **substantial modification** (modification to the intended purpose or change affecting compliance of the AI system with the Regulation) by providers or any third party, including when changes are **outside the "predefined range" indicated by the provider for continuously learning AI systems.** |

# Fremover

Hvilken type aktør er du?

Kan du tilby den kontroll som kreves?

Kan du gjenta kontroll løpende for å se om noe må vurderes på nytt ?

Kommer AI-as-a-Service?

Tilbakevirkende kraft? Antakelig slik som GDPR fikk

# Schjødt

**Eva Jarbekk**
Partner/lawyer,
Head of privacy & information security
m: +47 900 51 011
d: +47 23 01 18 29
eva.jarbekk@schjodt.com