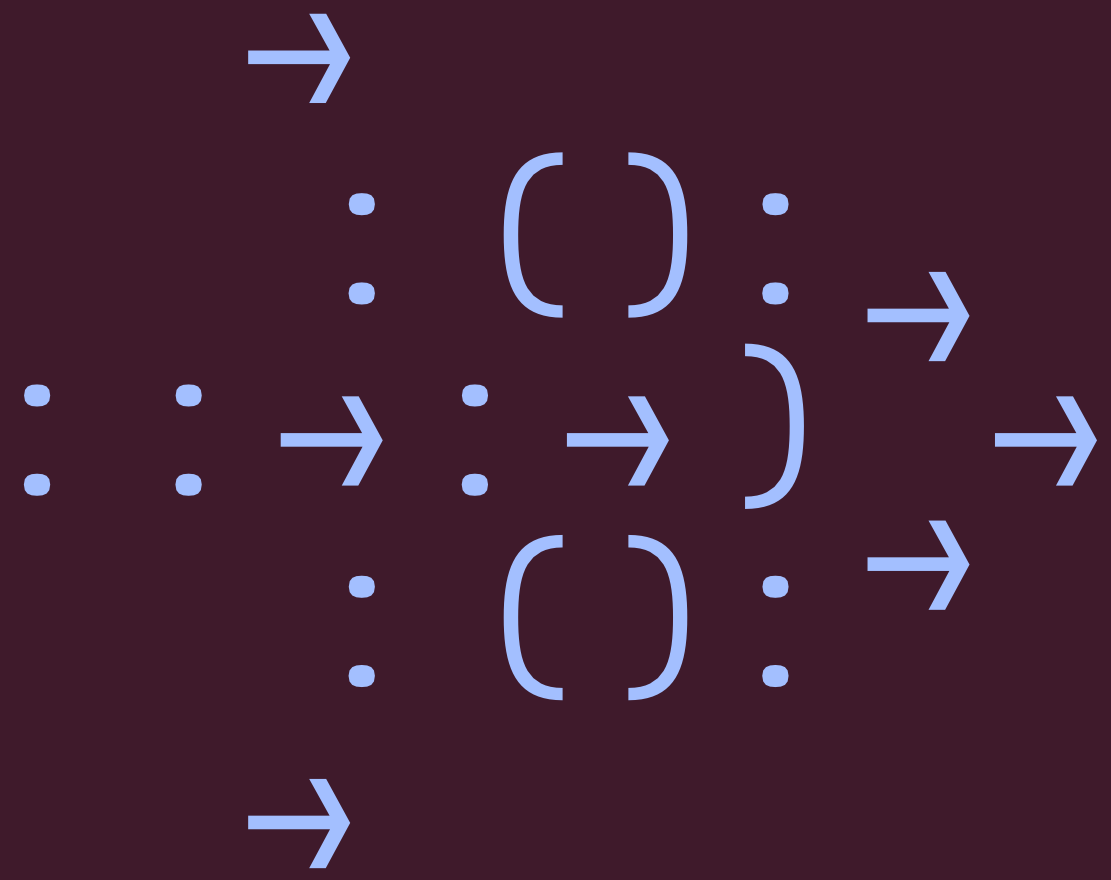


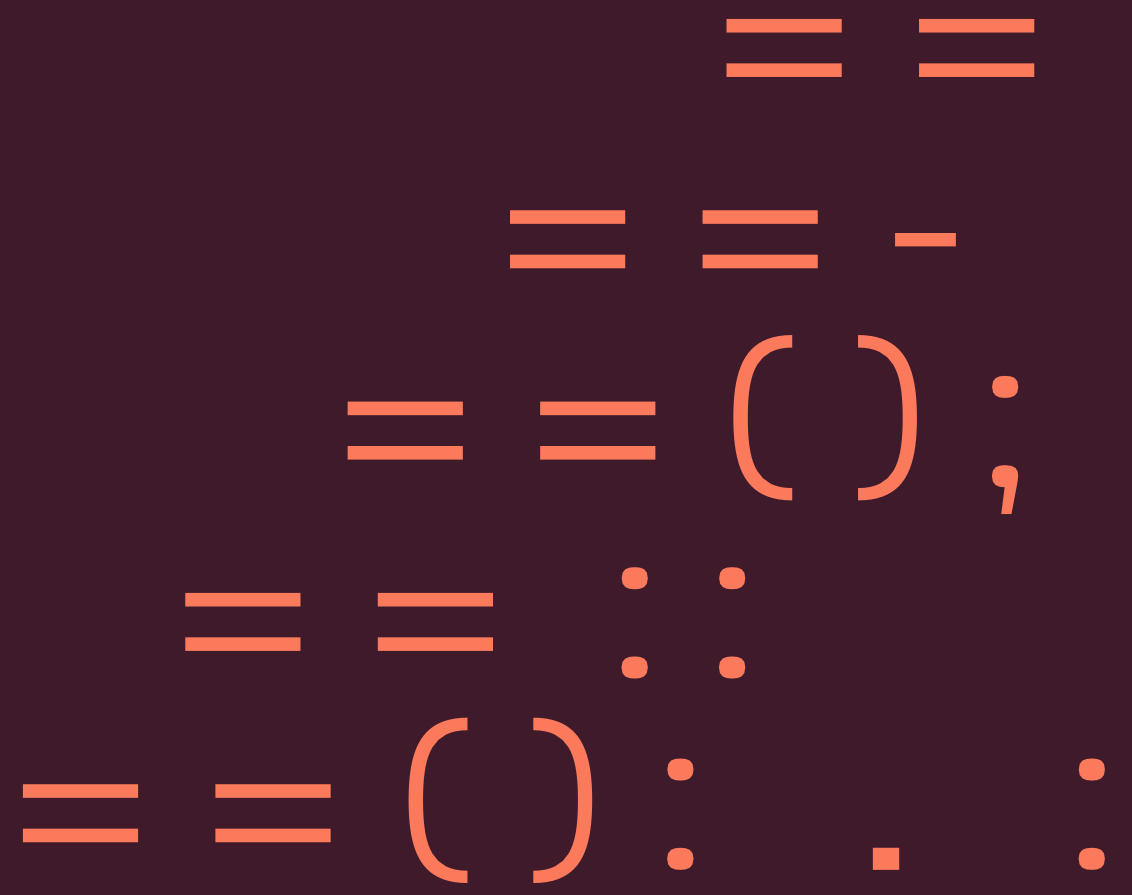
YODA Workshop

Intro to the AI Act

13-05-2026

Agenda

- Overall look at regulatory structure
- Guidance – national & EU
- The Digital Omnibus and implementation timeline



The purpose of the regulation and background

Background

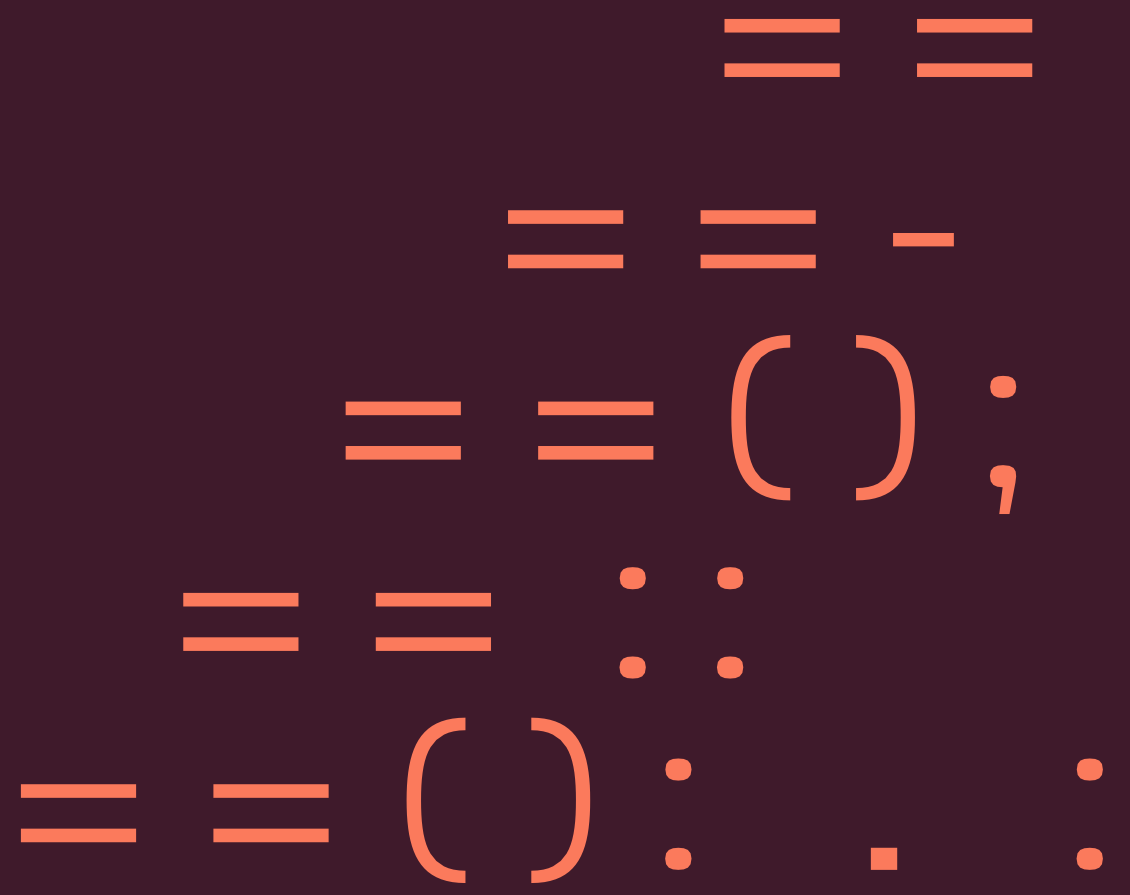
Regulating a fast paced industry

Application

- Entry into force on 1 August 2024
- Phased implementation

Purpose

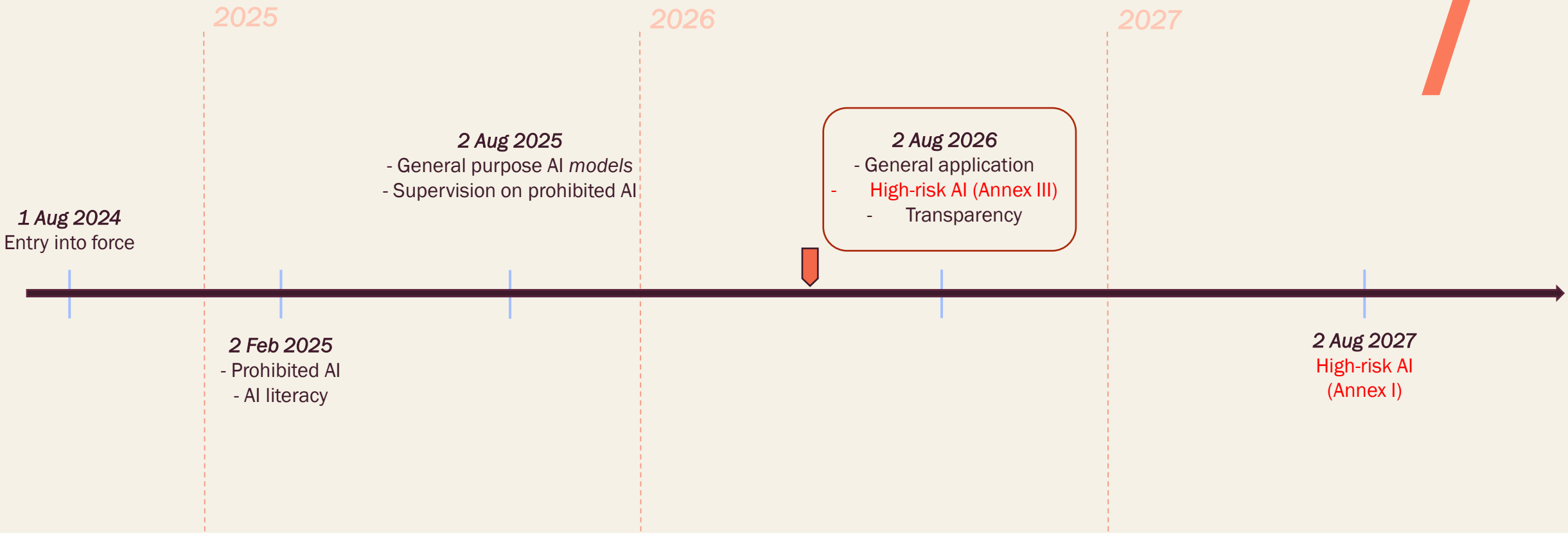
- Improve the functioning of the internal market
- Promote trustworthy AI
- Protect fundamental rights
- Support innovation

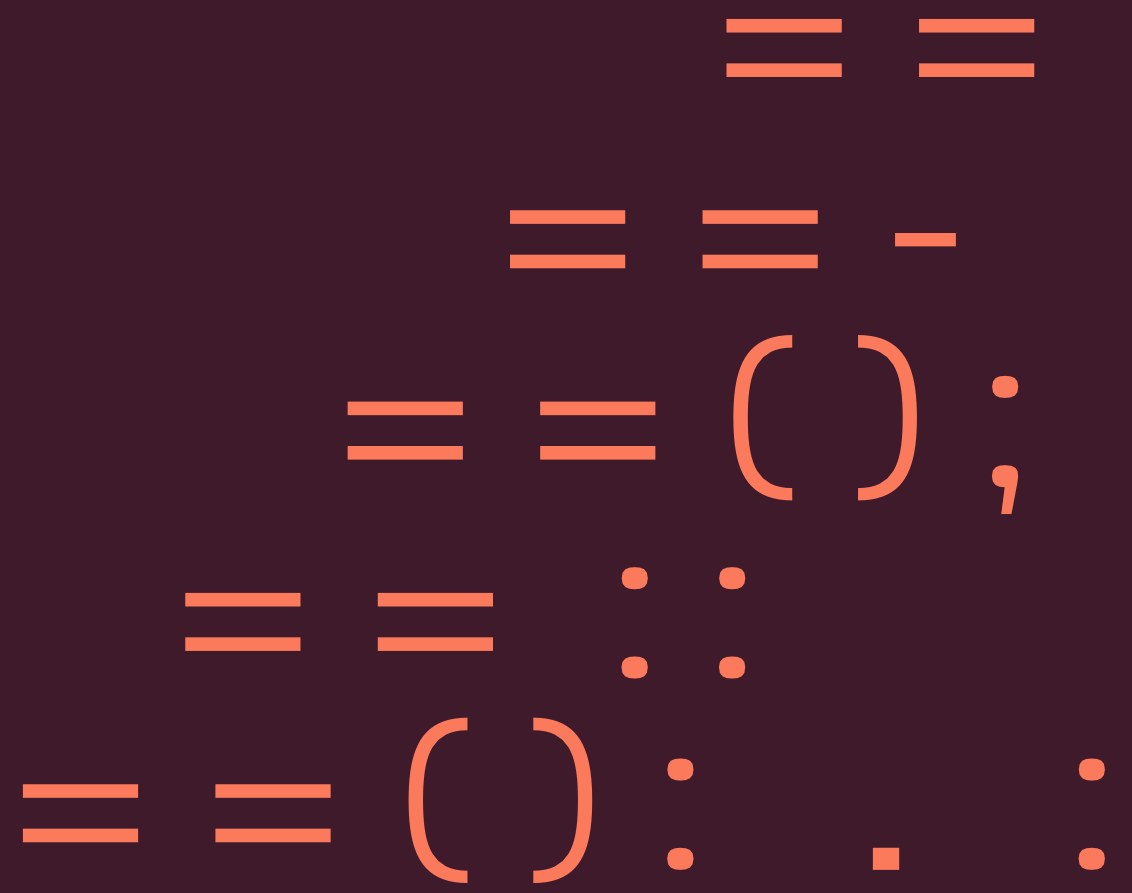


Timeline

AI Act overview

When do the rules apply?

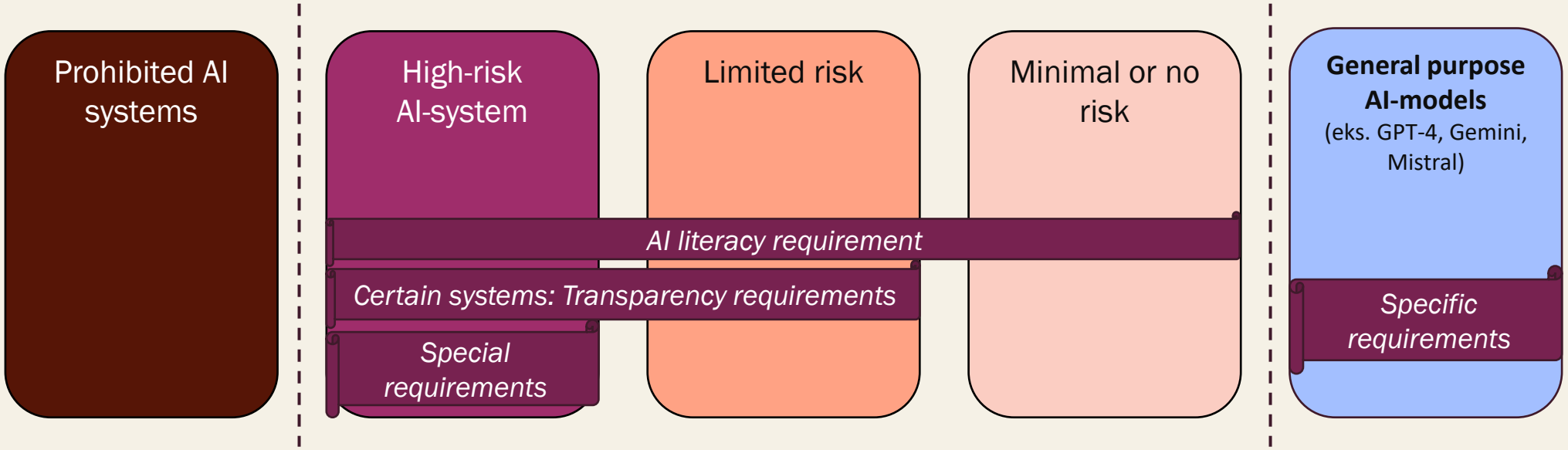


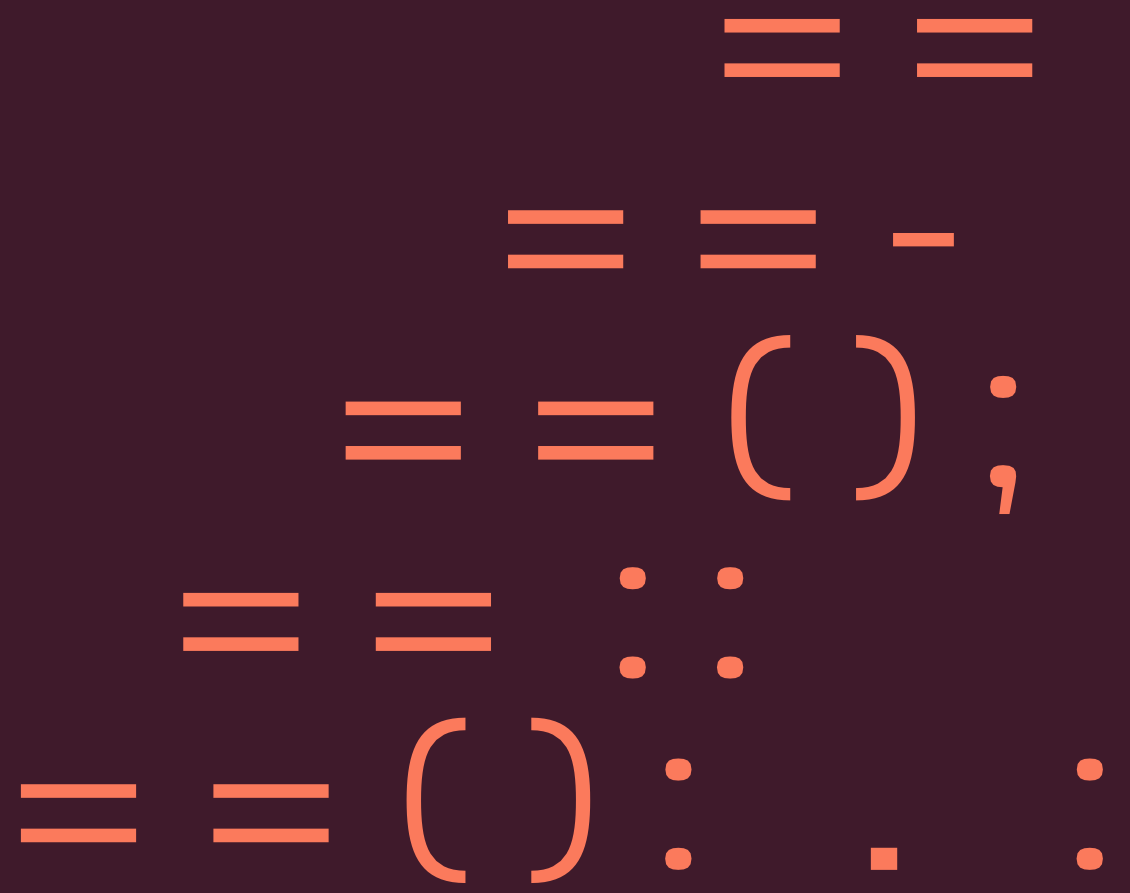


The risk-based approach

A risk-based approach

Obligations depending on risk of use





Prohibited AI practice

Prohibited AI practices (unacceptable risk)

Prohibited AI

(art. 5)

- a) Harmful manipulation
- b) Exploiting vulnerable persons
- c) Social scoring
- d) Predict risk of criminal offence based solely on profiling
- e) Create or expand facial recognition databases through untagreted scraping of facial images
- f) Emotion recognition in workplaces and education
- g) Biometric categorisation to deduce race, sexual orientation etc.
- h) Real-time biometric identification in public spaces

note! *Denmark is only partially bound by d), g) and h).*

Prohibited AI practices (unacceptable risk)

Prohibited AI

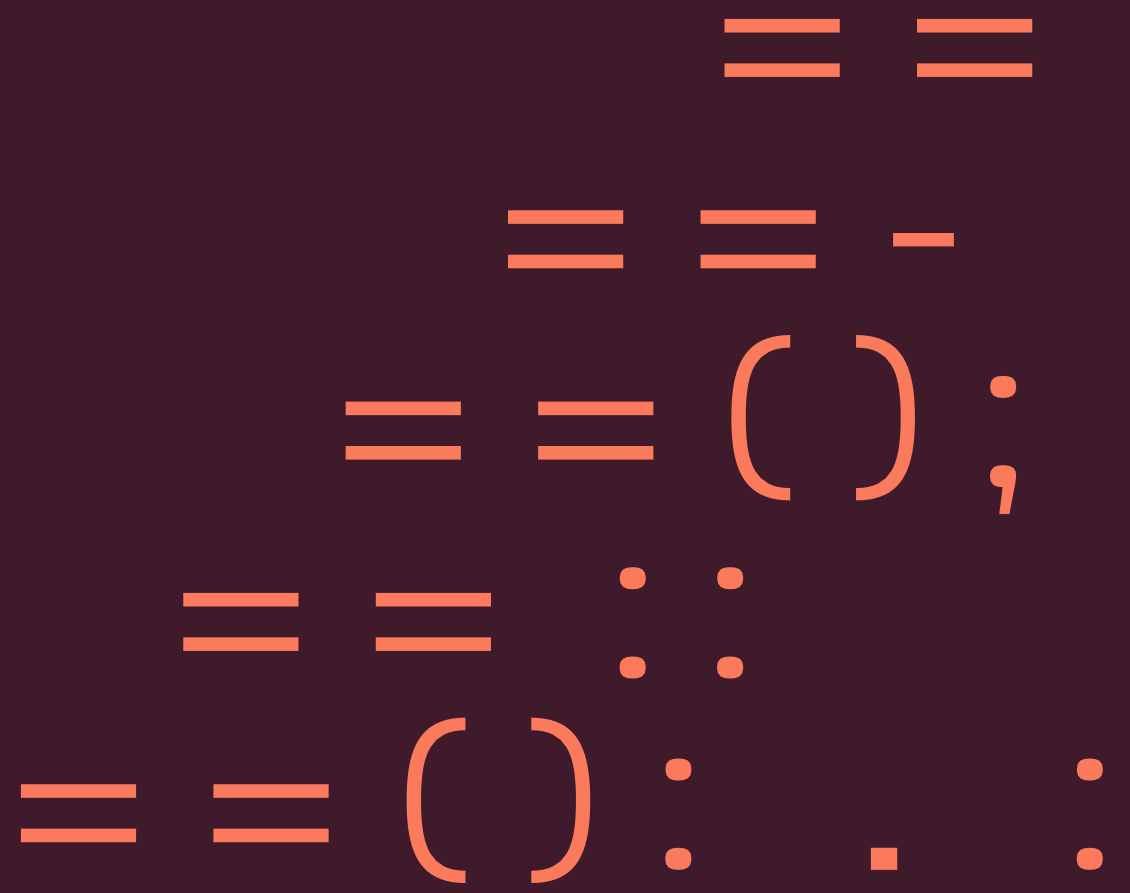
(art. 5)

- a) Harmful manipulation
- b) Exploiting vulnerable persons
- c) Social scoring
- d) Predict risk of criminal offence based solely on profiling

EXAMPLE: HARMFUL MANIPULATION

- AI systems that use: **subliminal techniques** that operate beyond human consciousness,
- or deliberately **manipulative** or **deceptive** techniques,
- with the intention or effect of distorting behaviour, thereby causing, or with a reasonable likelihood of causing, **significant harm**

note! *Denmark is only partially bound by d), g) and h).*



High-risk AI-systems

High-risk AI systems

High-risk AI systems

(art. 6)

Annex III (2 August 2026)

1. Biometrics
2. Safety components in critical infrastructure
3. Education
4. Employment
5. Essential services and benefits
6. Law enforcement
7. Migration, asylum and border control
8. Justice and democratic processes

Annex I (2 August 2027)

1. Machinery
2. Toys
3. Recreational craft and personal watercraft
4. Lifts
5. Protective systems in explosive atmosphere
6. Radio equipment
7. Pressure equipment
8. Cable way installations
9. Personal protective equipment
10. Appliances burning gaseous fuels
11. Medical devices
12. In vitro diagnostics medical devices

Obligations for *providers* of high-risk AI systems

- Risk management system (art. 9)
- Data og data governance (art. 10)
- Technical documentation (art. 11)
- Record-keeping (art. 12)
- Transparency and information to deployers (art. 13)
- Human oversight (art. 14)
- Accuracy, robustness and cybersecurity (art. 15)

*From **deployer** to **provider** if you*

put your name or trademark on a high-risk AI system,

make substantial modifications to a system already on the market,

modify the intended purpose of an AI system not classified as high-risk in such way that it becomes high-risk.

Examples of obligations of *deployers* of high-risk AI

High-risk AI systems

(art. 6)

Human oversight

- Deployers shall assign human oversight to natural persons who have the necessary competence, training and authority, as well as the necessary support.

Monitor the operations of the system

- Monitor on the basis of the instructions for use and, where relevant, inform providers.

Keeping logs

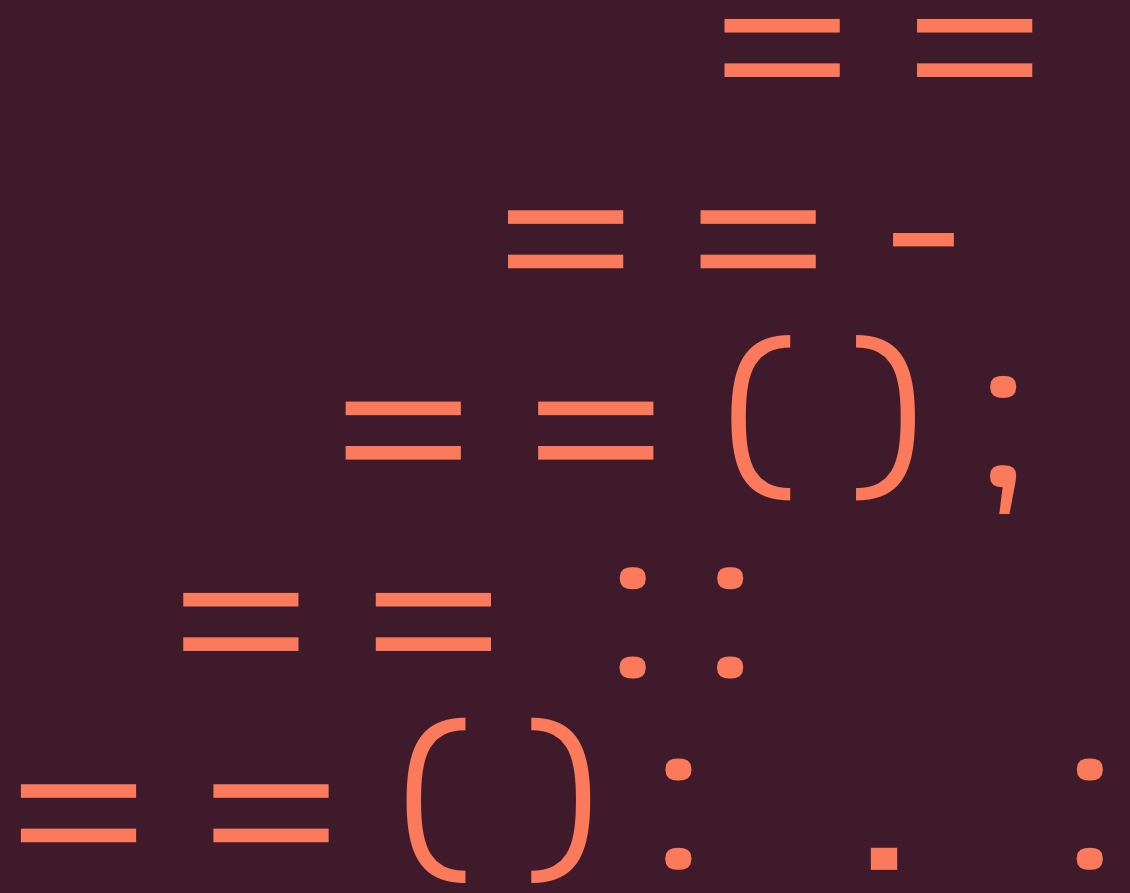
- Keep the logs automatically generated by the high-risk AI system (to the extent such logs are under their control)

Fundamental Rights Impact Assessment (FRIA)

- Public bodies or private entities providing public services
- Systems for credit evaluation/scoring and life and health insurance

Registration in EU Database

- Public authorities to register themselves and the system before using a high-risk AI system

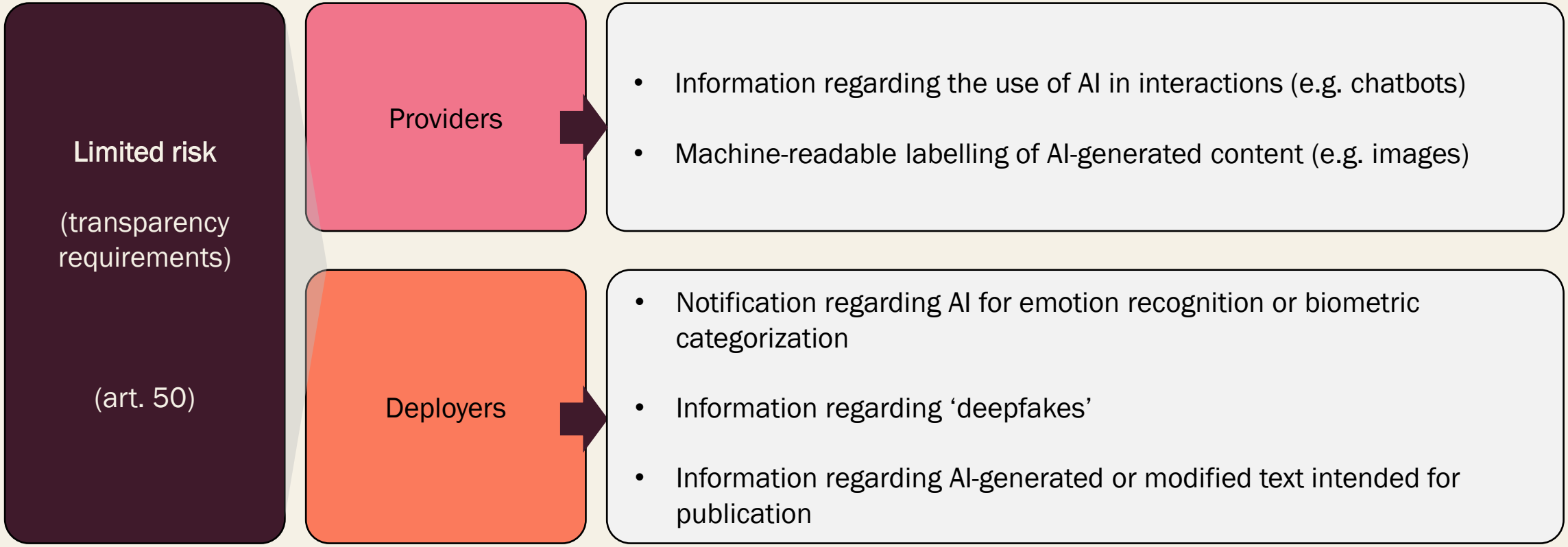


Limited risk

Transparency requirements

Let’s revisit the risk-based approach….

Openness and transparency in AI



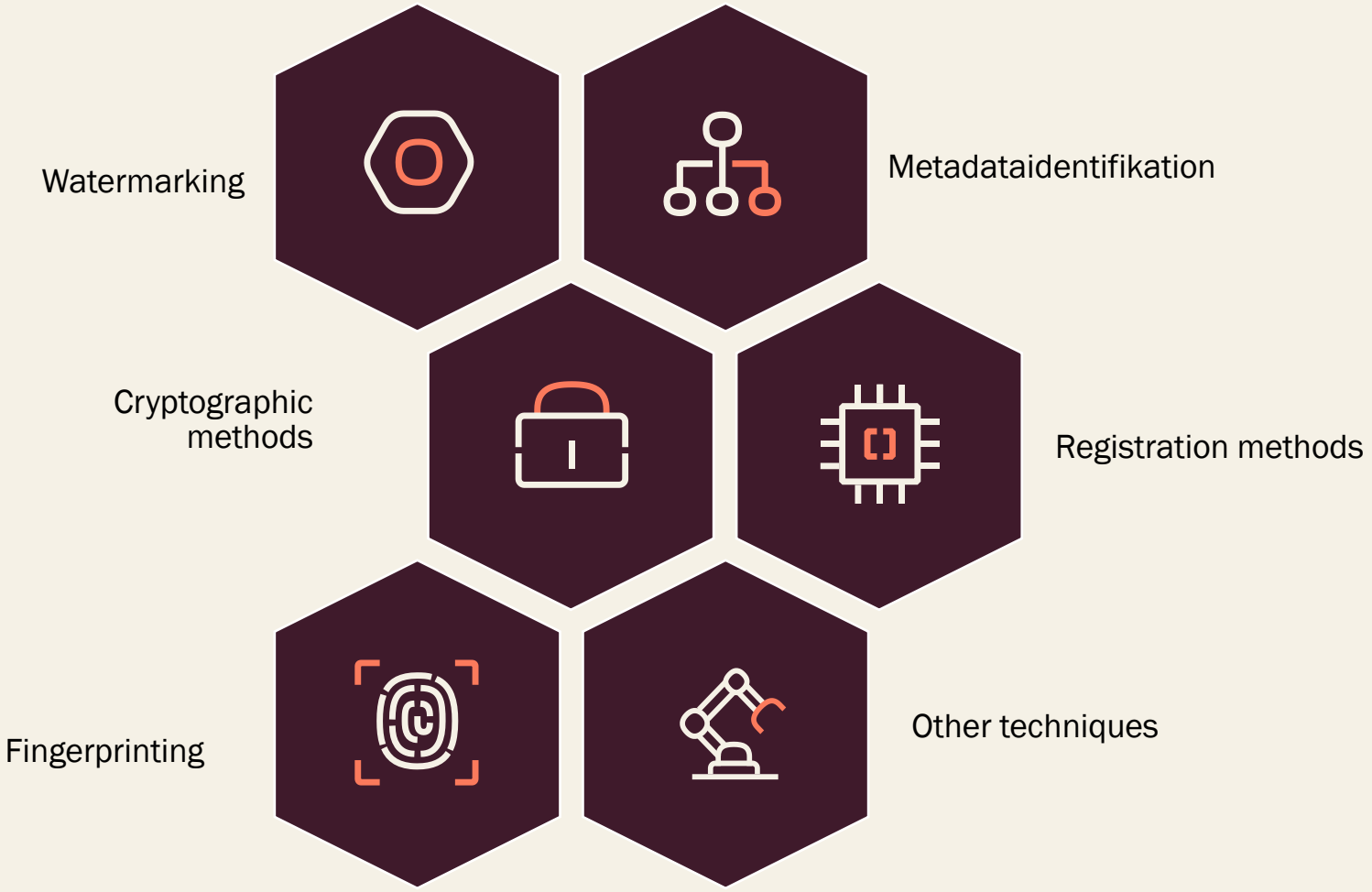
NB An AI system may be subject to both the requirements for high-risk AI systems and the transparency obligations

Which techniques can be deployed?

- Article 50(2)

- Techniques and methods should be sufficiently reliable, effective and robust

- Taking into account the different types of content, as well as constraints and market developments in this area



Key Takeaways

- What are the most important points?

1 Focus on risk mitigation

The aim is to prevent deception, manipulation and misinformation through information and labelling requirements.

2 Role and system dependent requirements

Transparency requirements vary depending on your role and how the AI system is used.

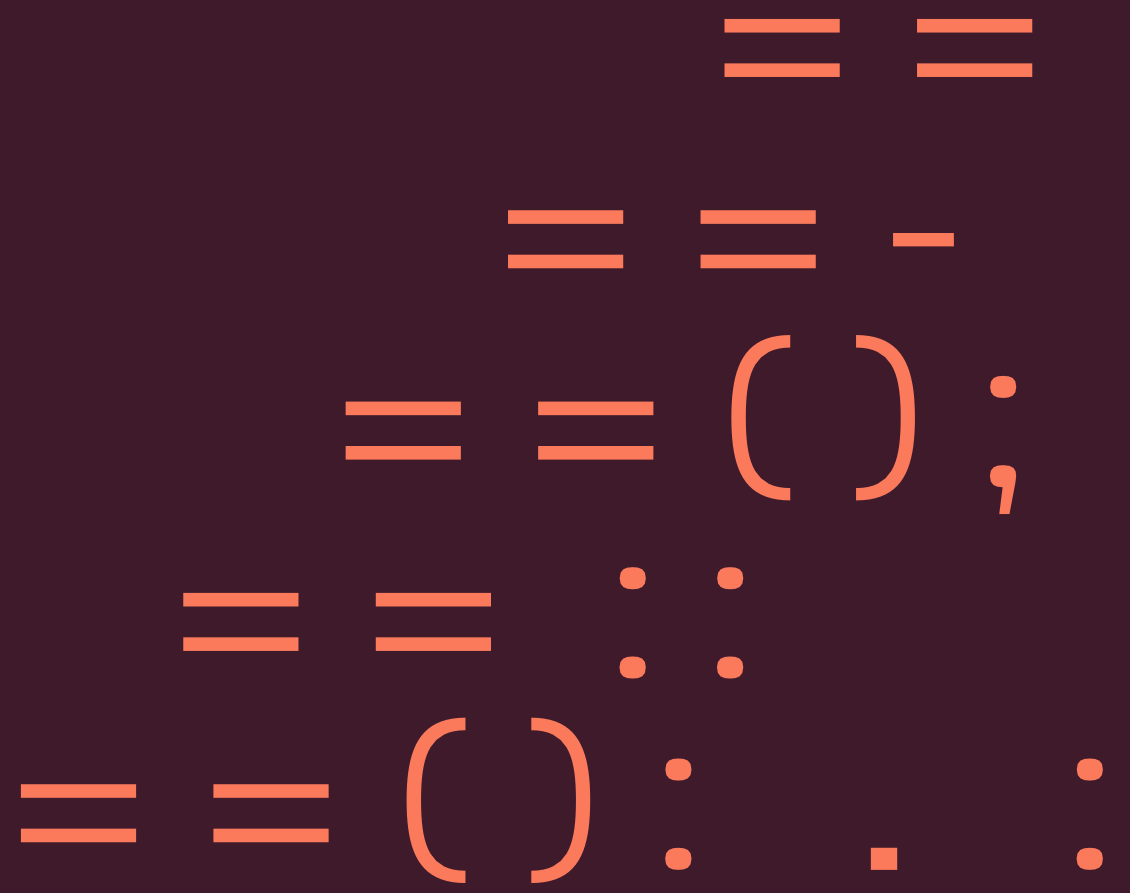
3 Awaiting interpretation and guidance

The interpretative framework remains limited – we are awaiting guidelines and a Code of Practice.

Guidelines are expected to go into public hearing this week.

4 Active follow-up

We are closely monitoring the implementation through a new working group set up by the AI Office



Guidance and guidelines

EU-guidelines, Code of Conduct & news

- The European Commission is working on:
  - Guidelines
  - Code of Practice

The AI Service Desk

- A Commision platform that:
  - Enables stakeholders to submit questions to the AI Office
  - Includes key tools: Compliance Checker & AI Act Explorer

Implementation and guidelines

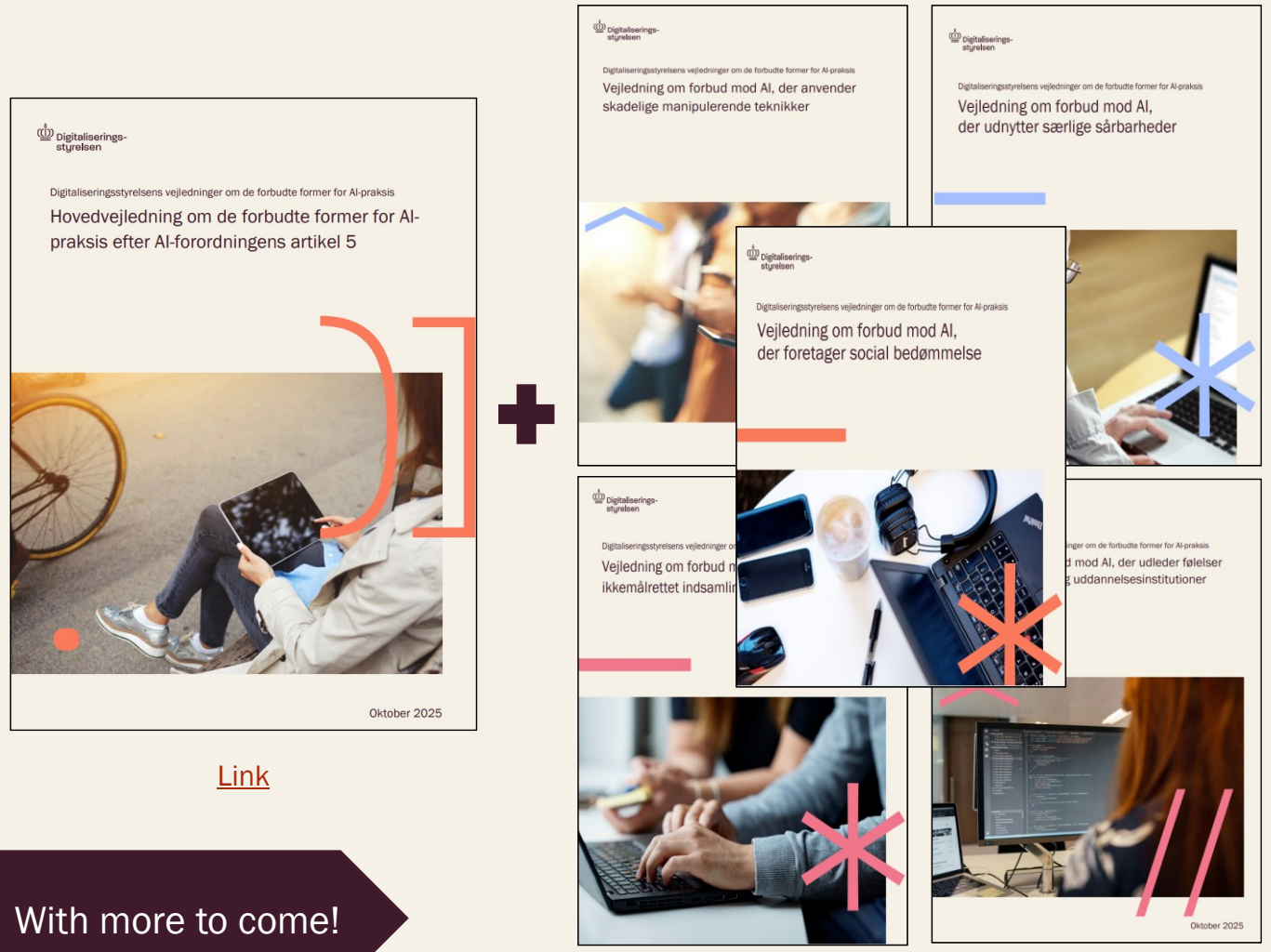
Guidelines from the Commission

Guidelines on **prohibited AI practices** (Art. 5)	Guidelines on the **definition of an AI-system** (Art. 2)	Guidelines on requirements for providers **general purpose AI models** (Art. 53–55)
• Published on 4 February 2025 • Published in Danish	• Published on 6 February 2025 • Published in Danish	• Published on 18 July 2025 • Published in Danish

On the way

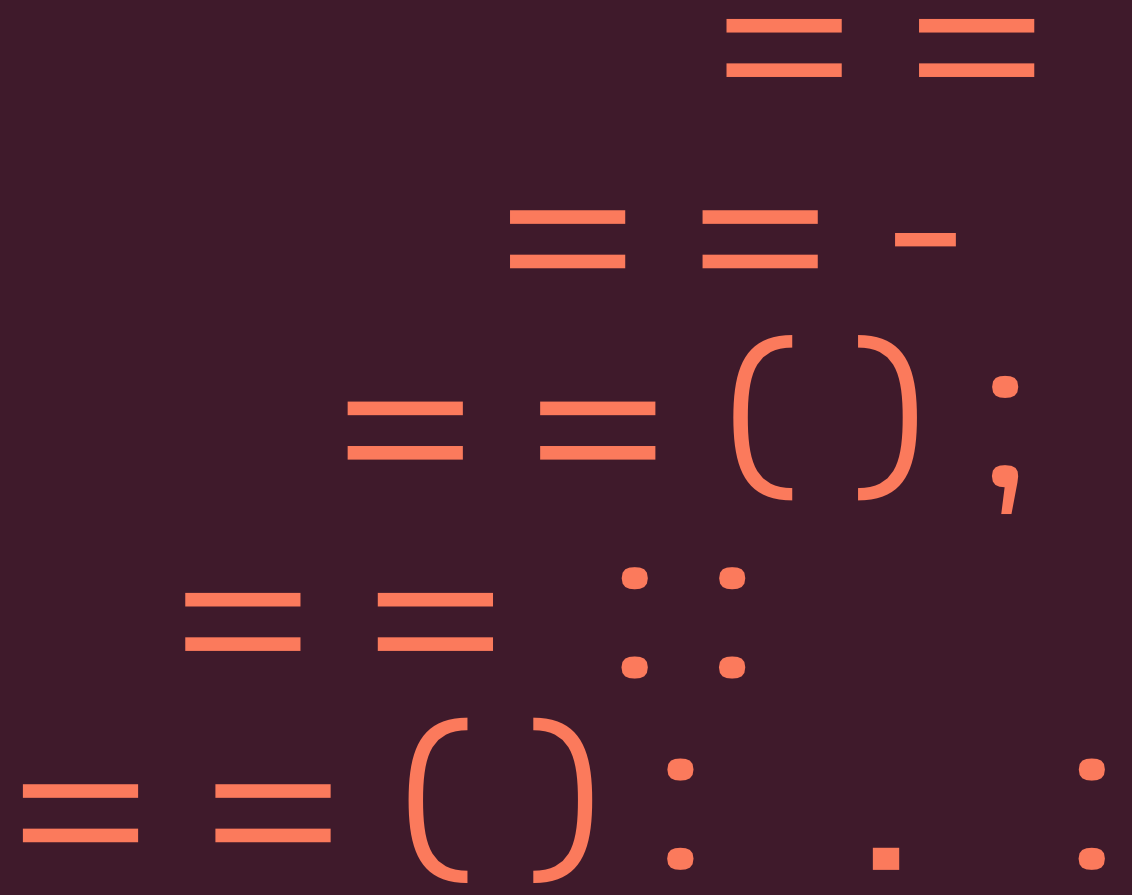
Code of practice for transparency obligations
Guidelines for transparency obligations
Guidelines for classification of high-risk AI systems

National guidelines and guidance pack on prohibited AI practices



Link

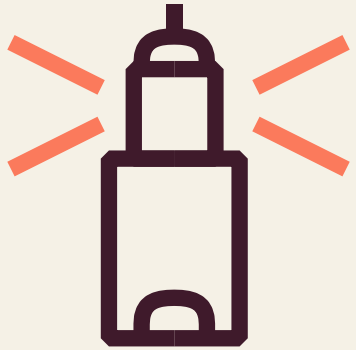
With more to come!

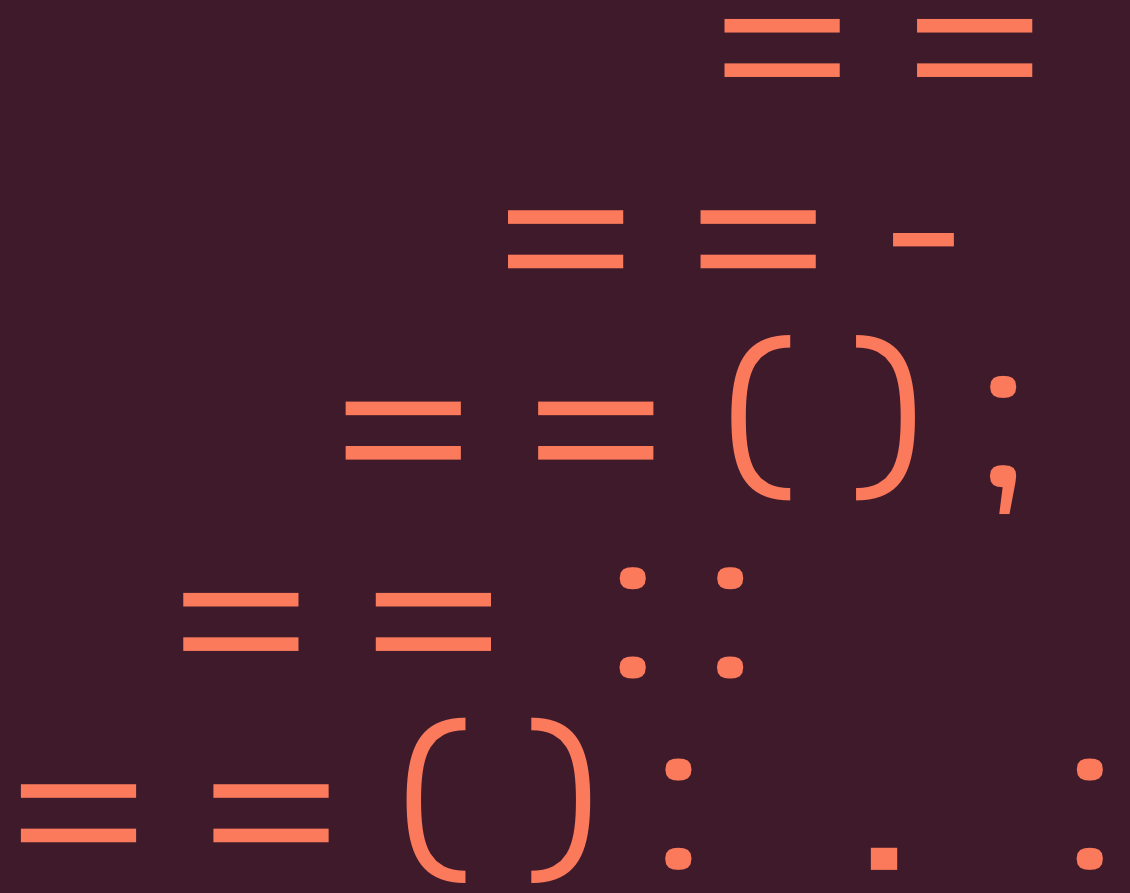


The Digital Omnibus

Key takeaways from the proposed Digital Omnibus

- New timeline:
  - →High-risk requirements for annex III moved from august 2026 to december 2027
  - →High risk requirements for annex I moved to august 2028
- New transition period for watermarking requirement for generative AI already placed on the market (extended 6 months)
- 2 new prohibited practices on harmful AI uses,
- Expanded data use for bias detection and revised AI literacy requirements



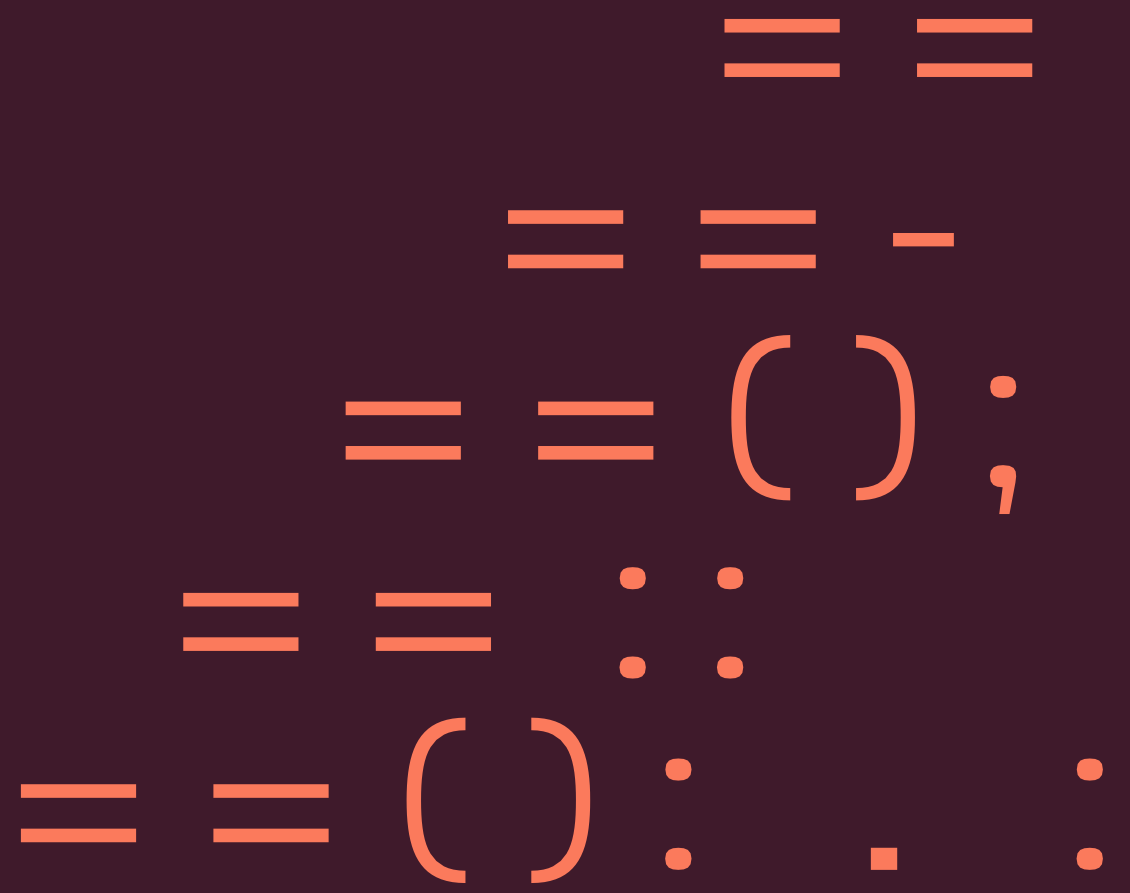


Regulatory Sandbox

Implementation

Regulatory sandbox

- The Agency for Digital Government and the Data Protection Agency have established a free regulatory sandbox for AI.
- Companies and public authorities can apply for relevant expertise and guidance on GDPR and risk classification under the AI Act free of charge.
- The sandbox aims to support innovation and the use of good AI solutions, thereby helping to ensure the responsible and lawful use of AI solutions.
- Once a sandbox process has been completed, the experiences gained from the process will be communicated to the public, for example in a report, so that others can benefit from them.



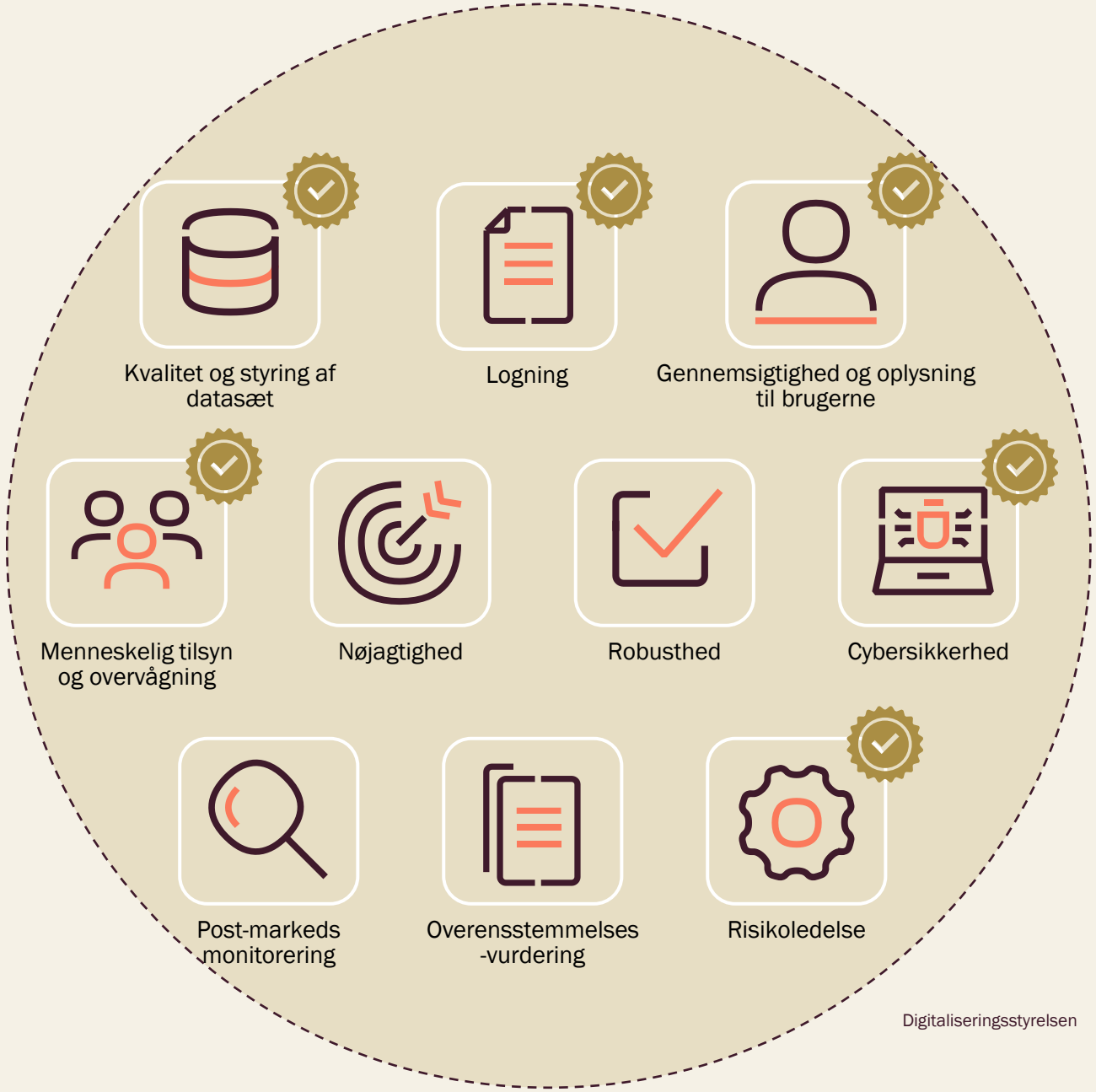
Standards

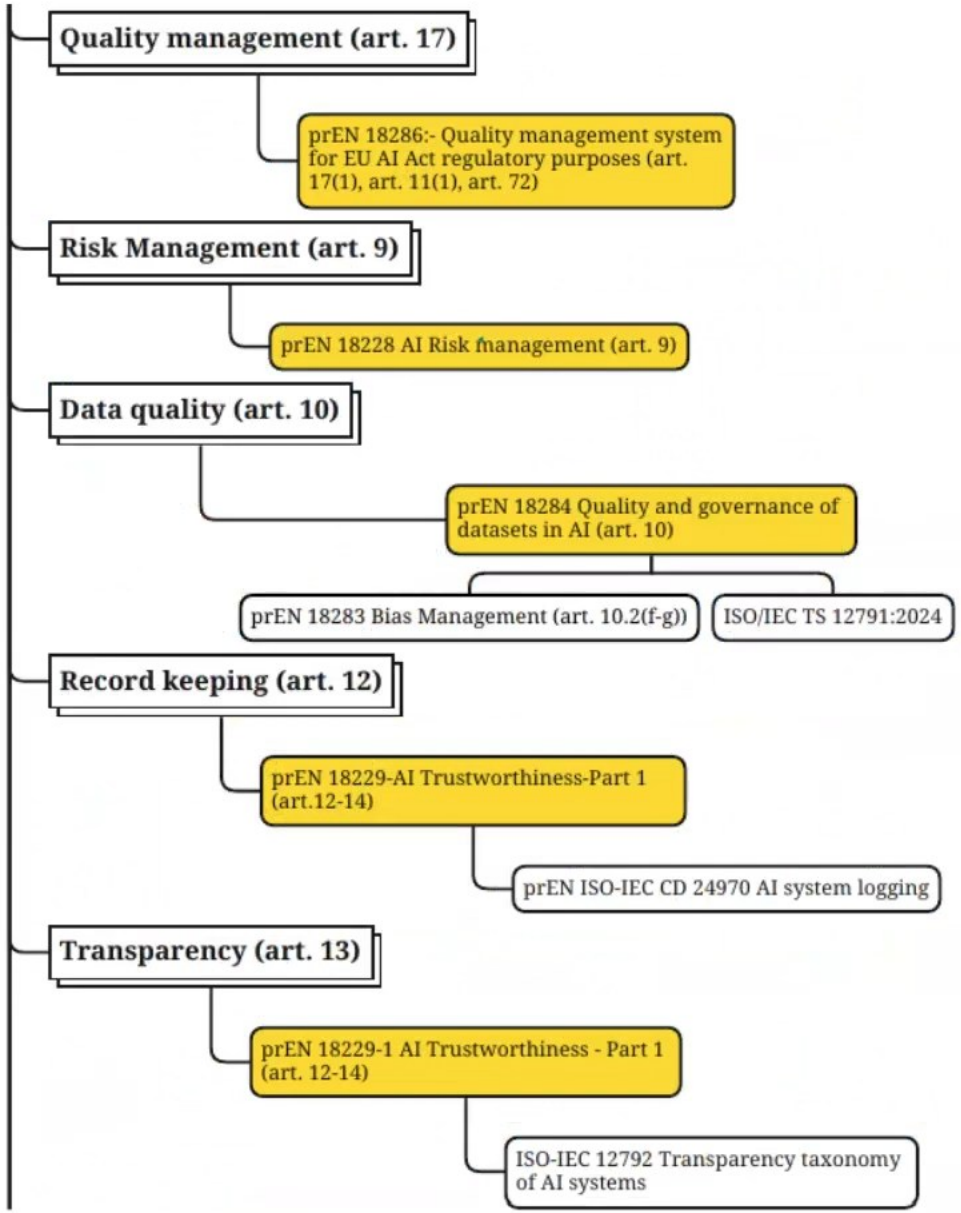
Standardisation request

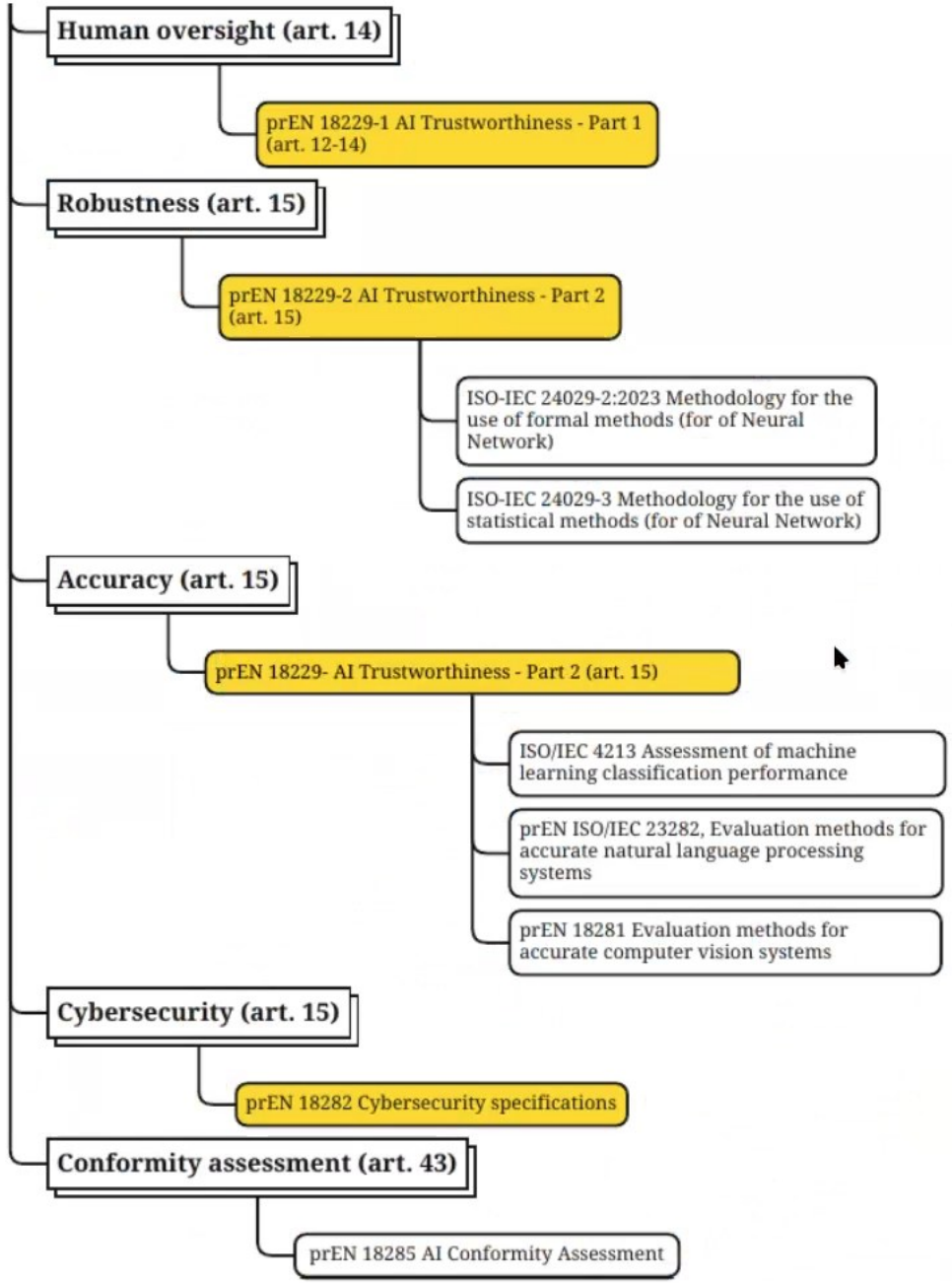
Almost ready for Final Vote
- *Quality Management System*

Public enquiries ongoing or about to start:
- *Risk Management System*
- *Computer Vision: Methods and Taxonomy*
- *Cybersecurity*

Følg med hos Dansk Standard
DS følger udviklingen tæt og vejleder om de kommende standarder via Dansk Standards Udvalg for Kunstig intelligens




Quality management (art. 17)
prEN 18286:- Quality management system for EU AI Act regulatory purposes (art. 17(1), art. 11(1), art. 72)
Risk Management (art. 9)
prEN 18228 AI Risk management (art. 9)
Data quality (art. 10)
prEN 18284 Quality and governance of datasets in AI (art. 10)
prEN 18283 Bias Management (art. 10.2(f-g))
ISO/IEC TS 12791:2024
Record keeping (art. 12)
prEN 18229-AI Trustworthiness-Part 1 (art.12-14)
prEN ISO-IEC CD 24970 AI system logging
Transparency (art. 13)
prEN 18229-1 AI Trustworthiness - Part 1 (art. 12-14)
ISO-IEC 12792 Transparency taxonomy of AI systems


Human oversight (art. 14)
prEN 18229-1 AI Trustworthiness - Part 1 (art. 12-14)
Robustness (art. 15)
prEN 18229-2 AI Trustworthiness - Part 2 (art. 15)
ISO-IEC 24029-2:2023 Methodology for the use of formal methods (for of Neural Network)
ISO-IEC 24029-3 Methodology for the use of statistical methods (for of Neural Network)
Accuracy (art. 15)
prEN 18229- AI Trustworthiness - Part 2 (art. 15)
ISO/IEC 4213 Assessment of machine learning classification performance
prEN ISO/IEC 23282, Evaluation methods for accurate natural language processing systems
prEN 18281 Evaluation methods for accurate computer vision systems
Cybersecurity (art. 15)
prEN 18282 Cybersecurity specifications
Conformity assessment (art. 43)
prEN 18285 AI Conformity Assessment

Udvalg

Udvalg for Kunstig intelligens (S-855)

Udviklingen af internationale standarder for kunstig intelligens er i fuld gang. Du kan få indsigt i morgendagens standarder og komme helt tæt på de europæiske standarder, der skal understøtte EU's kommende regulering af kunstig intelligens.

Er du interesseret i at deltage i udvalget? →

Næste møde

17 sep

Kontakt

Kim Skov Hilding

Chefkonsulent | Chief Consultant

Standardisering | Digital & Bæredygtighed

E: ksk@ds.dk

T: 39 96 62 17

Arbejdsområde

På den internationale bane er der allerede udgivet standarder om terminologi, 'use cases', risikovurdering og robusthed indenfor kunstig intelligens. Der er mange nye spændende standarder under udvikling om bl.a. datakvalitet, bias og en ledelsesstandard, som du kan få forhåndsviden omkring og påvirke - blot for at nævne nogle få.

Den kommende europæiske regulering skal sætte EU-krav til ansvarlig anvendelse af kunstig intelligens på det europæiske marked og skal sikre, at kunstig intelligens er både juridisk, etisk og teknisk robust, samtidig med at de europæiske værdier respekteres. Det er præcis til denne opgave, at den dansk-ledede europæiske standardiseringsgruppe, CEN-CENELEC JTC 21 Artificial Intelligence, er sat i verden.

Dansk Standard ønsker at være bannerfører for, at europæiske værdier respekteres og repræsenteres i de kommende europæiske standarder, og sammen med vores medlemsvirksomheder arbejder vi både proaktivt og strategisk i den europæiske standardiseringsgruppe.

Udvalget er ansvarligt for at diskutere og beslutte den danske holdning til både europæiske og internationale standarder for kunstig intelligens og forankre de danske fingeraftryk og mærkesager heri. Udvalget bidrager til udviklingen af nationale guidelines om fx gennemsigtighed, bias, mv.

- DS/PAS 2500-1:2020 - Kunstig intelligens Del 1: Gennemsigtighed
- DS/PAS 2500-2:2020 - Kunstig intelligens Del 2: Beslutningsstøttende anvendelse i offentlig sagsbehandling
- DS/PAS 2500-3:2023 - Kunstig intelligens Del 3: Bias
- DS/PAS 2500-4:2025 - Kunstig intelligens Del 4: AI-færdigheder

På følgende links, kan du læse mere om de standardiseringskomiteer, som udvalget følger:

- Internationalt: ISO/IEC JTC 1/SC 42 Artificial intelligence
- Europæisk: CEN-CENELEC JTC 21 Artificial Intelligence

Udbytte

Som medlem får du mulighed for at deltage i ovenstående komiteer samt de underliggende arbejdsgrupper, hvor standardernes indhold diskuteres og skrives. Du får således både adgang til et internationalt, europæisk og dansk netværk. Sidstnævnte mødes fire gange årligt, hvor vi foruden standardisering har spændende temaer på dagsordenen.

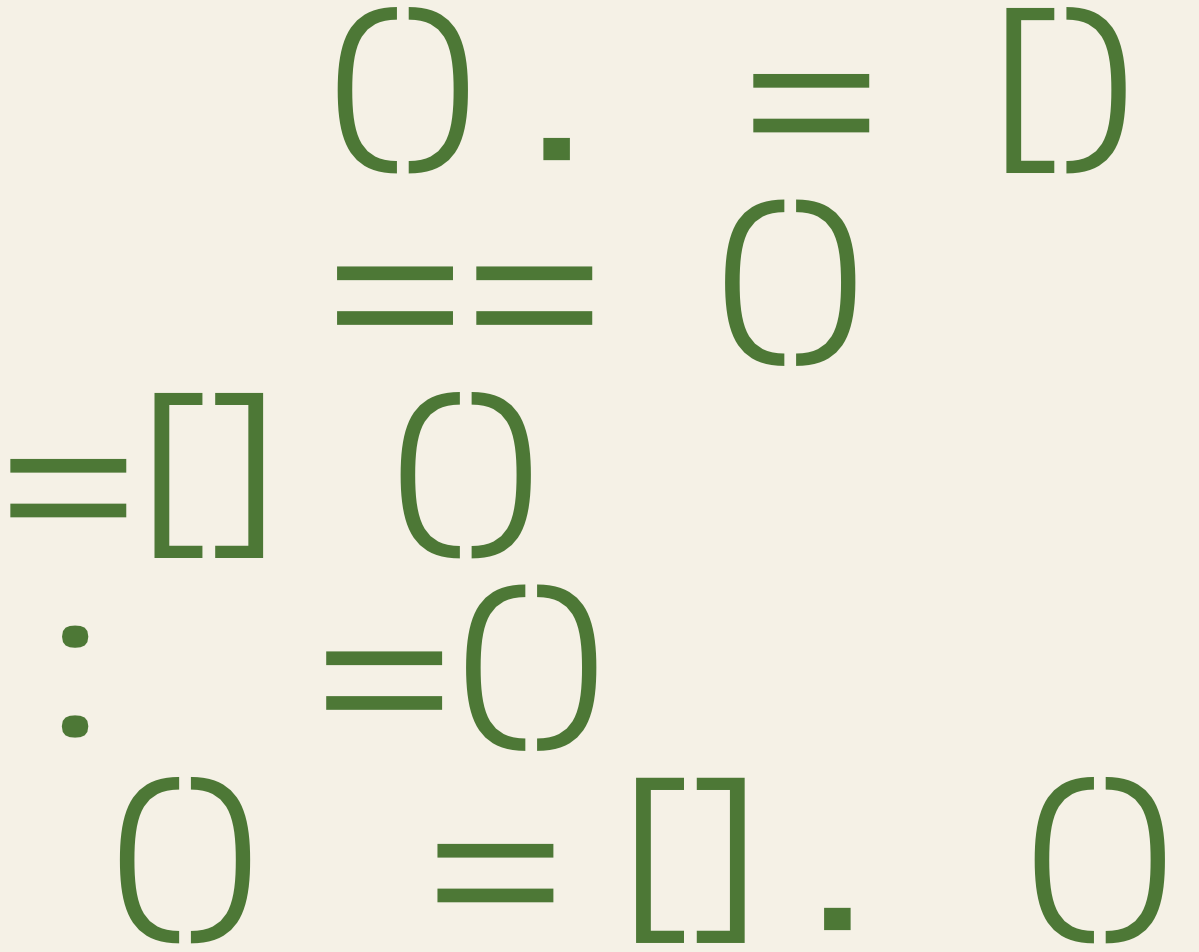
Målgruppe

Udvalgsarbejdet er åbent for alle med interesse i kunstig intelligens, deltagerne spænder bredt over SMV'er, testinstitutter, forskere, producenter, ingeniører til rådgivere og myndigheder. Til højre kan du finde navnene på de virksomheder og organisationer der deltager.

Deltagere

2021.AI ApS
AI Rådgivning ApS
Anders Vidstrup
Børns Vilkår
Copenhagen Business School
Digitaliseringsstyrelsen
Dimitra Sotiraki
Ey Godkendt Revisionspartnerselskab
Fellowmind Denmark A/S
Focus Advokater P/S
Force Technology
Forsikring & Pension
Fredericia Maskinmesterskole
GN Hearing A/S
Grundfos A/S
Grundfos Holding A/S
Halfspace.IO ApS
HK Danmark
IDA Learning
Institut For Menneskerettigheder -Danmarks Nationa
IT Univers ApS
It-Universitetet I København
Københavns Universitet, Datalogisk Institut
Milestone Systems A/S
Neurospace ApS
NorMed Consulting
Novo Nordisk A/S
Piedboeuf ApS
Plesner Advokatpartnerselskab
Reynolds & Moore A/S
Roskilde Universitet
Skatteforvaltningen - UFST
Syddansk Universitet
TDC NET
Teknologisk Institut, Odense
Aalborg Uni Institut for Arkitektur og Medieteknо
Aalborg Universitet
Aarhus Universitet

Jeg vil gerne vide mere om udvalget →



Digitaliseringsstyrelsen

Does the solution fall within the scope of the Regulation?

Does the system constitute an "AI system" or a "general-purpose AI model"?

01

Is the AI solution exempt from the Regulation?

Does the solution fall under an exemption referred to in Article 2 of the Regulation?

02

Assess the system's risk category

Should the AI system be classified as a prohibited practice, high risk (including exceptions), limited risk, or minimal/no risk?

03

Identify your relevant role in the AI value chain

Are you a provider, operator, manufacturer of a product, authorised representative or importer?

04

Identify the relevant requirements

Which requirements in the Regulation are relevant to your specific project?

05

Spørgsmål?

AIA@digst.dk