The EU AI Act: an introduction

December 2024

Krisztina Baracsi, VP EU Affairs

Agenda

1. AIA basics & implementation timeline
2. Rationale & legislative logic
3. The risk-based approach
4. Definitions
5. Prohibited AI systems
6. High-risk AI systems & their requirements
7. Responsibilities along the value chain
8. GPAI models and systems
9. Enforcement & penalties
10. Ongoing initiatives: guidance & knowledge sharing

The EU AI Act: the basics

- Adopted by EU legislators in H1 2024
- Entered into force on Aug 1, 2024
- Directly applicable regulation in the EU
  - No implementing legislation needed in EU Member States
  - Norway (EEA): needs to be implemented
- Applies to AI put on the market/used in the EU
- Complements existing applicable rules (e.g. GDPR, NIS2, sectoral legislation

EU AI Act: entry into force, application dates

July 12 2024
Publication in the Official Journal

Aug 1 2024
Entry into force

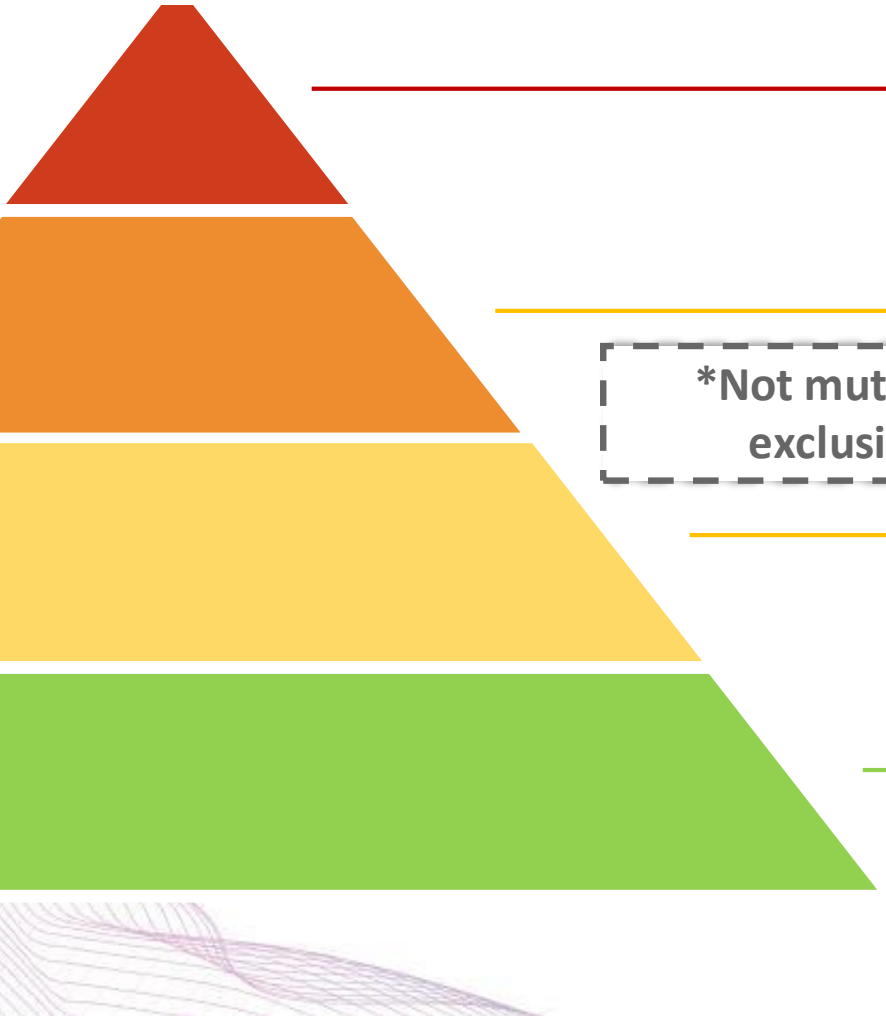
Feb 1 2025
Phase out prohibited systems

Aug 1 2025
GPAI obligations applicable

Aug 1 2026
All of AIA applicable, incl. rules on high-risk AI (except Annex II)

Aug 1 2027
Rules on high-risk per Annex II (regulated products) applicable)

The risk-based approach of the AI Act



*Not mutually exclusive

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

AI with specific transparency obligations
'Impersonation' (bots)

Permitted but subject to information/transparency Obligations

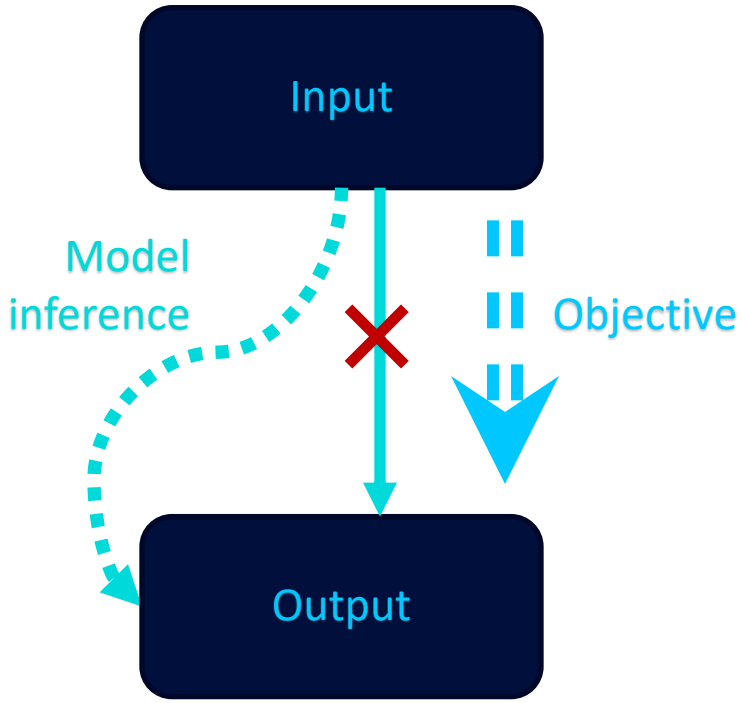
Minimal or no risk

Permitted with no restrictions

Rules for GPAI models/systems

European Commission

Definitions: AI system



Unlike human-defined rule-based systems, AI systems have a **degree of autonomy** when accomplishing their task.

An **AI system** is a **machine-based** system 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.**

Different AI systems vary in their levels of **autonomy** and **adaptiveness** after deployment.

OECD.AI Policy Observatory

Definitions: general purpose AI models and systems

General purpose AI models
(e.g. GPT 4)

- Trained with a large amount of data using self supervision at scale
- Displays significant generality
- Capable to competently perform a wide range of distinct tasks
- Regardless of the way the model is placed on the market
- Can be integrated into a variety of downstream systems or applications
- Does not cover models used for research, development or prototyping, before market release

General purpose AI systems
(e.g. Chat GPT)

- AI system based on a GPAI model
- Capable to serve a variety of purposes
- For direct use or for integration in other AI systems

"AI models are essential components of AI systems, but they don't constitute an AI system on their own. AI models require the addition of further components, such as for ex a user interface, to become AI systems. AI models are typically integrated into and form part of AI systems."

I. Prohibited AI systems

1. AI systems deploying **subliminal/manipulative techniques** aimed at distorting behavior
2. **Social scoring**
3. **Predictive policing**
4. Creation/expansion of **facial recognition databases** through untargeted scraping of facial images from the internet/CCTV footage
5. **Emotion recognition at work/school:** AI systems that infer emotions of a natural person in the workplace or educational institutions, except for medical or safety reasons
6. **Biometric categorization:** AI systems categorizing natural persons based on the biometric data to deduce race, political opinions, trade union membership, religion, sex life or sexual orientation
7. **Biometric identification by law enforcement**: use or real-time remote biometric identification systems in publicly accessible spaces for law enforcement purposes, unless strictly necessary

II. High-risk AI systems

1. SAFETY COMPONENTS OF REGULATED PRODUCTS (Annex II)

Regulated products subject to 3rd party assessment under sectoral product safety regulation

- E.g. radio equipment (network equipment and terminals)

2. CERTAIN (STAND ALONE) AI SYSTEMS IN THE FOLLOWING FIELDS (Annex III)

1. Biometric identification and categorization of natural persons
   - AI systems intended to be used for emotion recognition
2. Critical infrastructure
   - Safety components in the management and operation of critical digital infrastructure
3. Education and vocational training
4. Employment, workers management and access to self-employment
   - recruitment/selection: placing targeted job adverts, analysing filtering job applications, evaluating candidates
   - decisions affecting work relationship, task allocation, monitoring/evaluating employee performance/behavior
5. Access to and enjoyment of essential private services and essential public services and benefits
   - AI systems used to evaluate the creditworthiness of NPs, ex fraud detection
6. Law enforcement
7. Migration, asylum and border control management
8. Administration of justice and democratic processes

Exception for decision-support systems

- IF no significant risk of harm to the health, safety or fundamental rights
- IF no material influence on the outcome of decision-making
  a) improve the result of a previously completed human activity;
  b) perform a narrow procedural task (e.g. translation)
  c) detect decision-making patterns or deviations from prior decision-making patterns and is not meant to replace or influence the previously completed human assessment without proper human review; or
  d) perform a preparatory task to an assessment (e.g. select candidates w/concrete qualification)
- **EXCEPT** if the system performs profiling of natural persons

III. AI systems subject to transparency req's vis-à-vis customers

1. **AI systems that directly interact with customers (chat-bots)**
   - Customers need to be informed that they are interacting with an AI system unless this is obvious in the circumstances/context
   - Providers to design/develops AI systems in such a way
2. **Emotion recognition/biometric categorization systems**
   - Deployers need to inform customers exposed to such systems
3. Watermarking for generative AI systems
   - AI systems/GPAI systems generating synthetic audio, image, video or text
   - Outputs must be marked and detectable as artificially generated - responsibility lies with the provider
   - "Deepfakes": deployers to disclose it as such

Requirements on high-risk AI systems

1. **RISK MANAGEMENT SYSTEM:** set up & maintain RMS, may be part of existing one
2. **DATA GOVERNANCE:** use high-quality training, validation and testing data (relevant, representative)
3. **TECHNICAL DOCUMENTATION**: draw up documentation and design logging features
4. **RECORD KEEPING**: allow for automatic recording of events (traceability & auditability),
5. **TRANSPARENCY**: provide instructions for use for deployers & facilitate their compliance
6. **HUMAN OVERSIGHT**: measures built into the system and/or to be implemented by deployers
7. **ACCURACY, ROBUSTNESS & CYBERSECURITY**

The Who's Who under the EU AI Act

AI Value Chain

Provider

Persons♦ developing AI Systems or GPAI✦ Models for Release* under its name (for free or commercial use)

Deployer

Persons that use** AI Systems under its authority

Manufacturer

Persons that provide, distribute, or use AI Systems in the EU with their products under their own name or trademark

Importer

EU Persons that Release AI Systems bearing non-EU based Provider's name and mark

Distributor

Persons that make AI Systems available in the EU Market

Representative

EU Persons appointed by Provider to perform obligations under the EU AI Act

♦ Persons = a natural or legal person, public authority, agency, or other body

* Release = places on the market or puts into service

✦ GPAI = General Purpose AI

** Other than for personal, non-professional activity

BAKER DONELSON

Obligations on providers and deployers of high-risk AI systems

PROVIDER

- Compliance with the requirements on high-risk AI system
- Set up **quality management system**
- Draw up and maintain **documentation**
- **Keep logs** to enable deployers to monitor the operation
- Carry out **conformity assessment procedure**
- **Affix CE marking** to indicate conformity
- **Register** the high-risk AI system **in the EU database**
- Conduct **post-market monitoring**
- **Collaborate with** market surveillance **authorities**

DEPLOYER

- **Operate** high-risk AI system **in line with instructions of use**
- Assign sufficiently qualified staff to **human oversight** (to the extent they exercise control over the system)
- Ensure **input data is relevant and sufficiently representative** (to the extent it exercises control over the input data)
- **Monitor operation** for possible risks, inform provider
- **Inform provider/authorities** about serious incidents
- **Keep logs** to the extent they are under their control
- **Inform workers' representatives & affected workers** if high-risk AI systems are put into service at the workplace
- **Inform individuals** if they are subject to decisions made by high-risk AI system
- Perform **fundamental rights impact assessment** in certain cases

Transfer of provider responsibilities to deployers

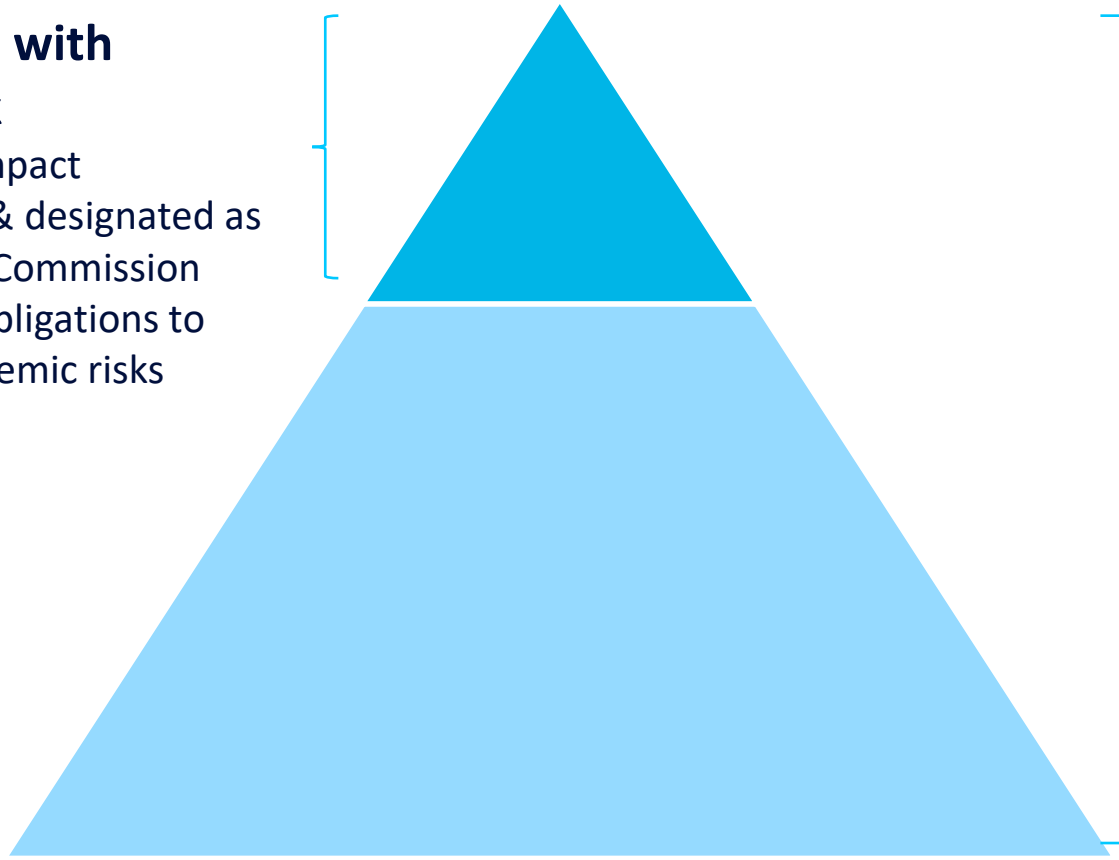
- **Deployers may in certain cases become providers** and be subject to their obligations
  1. **Substantial modification of a high-risk AI system** already placed on the market/put into service in a way that it remains a high-risk system
     - SUBSTANTIAL MODIFICATION:

       *"A **change** to the AI system after its placing on the market/putting into service which is **not foreseen in the initial conformity assessment** by the provider and as a result of which the compliance of the AI system with the requirements is affected **or results in a modification to the intended purpose** for which the AI system has been assessed"*
  2. **Modification of the intended purpose** of an AI system or GPAI system in such a way that it becomes a high-risk AI system
- In such cases the original provider is subject to a **cooperation obligation**
  - Make available all necessary information and provide the reasonably expected technical access and other assistance that are required for the fulfillment of the obligations under here – subject to IPR & trade secret protection

GPAI models and their obligations

GPAI models with systemic risk

- Have high impact capabilities & designated as such by the Commission
- Additional obligations to manage systemic risks



Obligations for all GPAI model providers

(exceptions for open source)

- Maintain technical documentation incl training & testing results
- Detailed summary about the content used for training
- Make available information for downstream providers
  - Enable understanding of capabilities and limitations
  - Enable compliance with obligations
- Copyright policy
- Authorised representative for non-EU GPAI providers

High impact capability: cumulative compute used for training measured in FLOPs is greater than 10^25

Responsibilities along the value chain related to GPAI models and systems

Provider of a GPAI model

Develops/has developed a GPAI model and places it on the market

- Obligations for providers or all models (irrespective of risk)
- Make available documentation to downstream providers, but no cooperation obligation
- No transfer of model provider role if the model is integrated into high-risk AI system

Downstream provider

Provider of an AI system (incl GPAIS) which integrates a GPAI model (incl its own)

- To benefit from the documentation/information made available by GPAI model provider
- Subject to general obligations of providers in case model integrated into high-risk AI system

Provider of a GPAI system

Develops and places on the market a GPAIS

- No general obligations on GPAI systems (exc. watermarking for generative GPAIS)
- Transfer of provider role if the intended purpose of the GPAIS is modified by a new provider to a high-risk AI system
- GPAI system provider has a cooperation obligation: make available information, provide technical access/other assistance

Enforcement and governance

- **National competent authorities:** responsible for enforcement at national level
  - MSs to designate one or several market surveillance authority with necessary staffing and competence
- **European Artificial Intelligence Board:** ensures consistent application across the EU
  - National competent authority representatives & EDPS
  - Issues recommendations & opinions
- **European Commission AI Office**: exclusive power to supervise and enforce the AIA wrt GPAI models
- **Advisory Forum: p**rovides technical expertise to the Board
  - Appointed by the EC, balanced selection of industry, civil society & academia
- **Scientific Panel of Independent Experts:** advises the AI Office esp re GPAI, support market surveillance authorities on their request
  - Independent AI experts selected by the Commission

Penalties

- **Up to 15 million EUR/3% of total worldwide annual turnover –** non-compliance with high-risk & transparency requirements
- **Up to 35 million EUR/7% of total worldwide annual turnover** – non-compliance with prohibited AI rules
- Conditions of levying fines is to be specified by Member States

Upcoming Commission guidance/implementing acts

- Guidelines on high-risk AI – within 18 months after entry into force
  - Guidance on the practical implementation of the rules on classification of high-risk AI, incl a comprehensive list of practical examples of high-risk and non-high risk use cases
- Guidelines on the practical implementation of the AIA (Art 96)
  - prohibited practices as per Art 5.
  - application of the definition of an AI system
  - requirements and obligations on high-risk AI systems, incl responsibilities along the value chain
  - provisions related to substantial modification
  - transparency obligations (Art 50)
  - detailed information on the relationship of the AIA with relevant Union law, incl the consistency of their enforcement
- Code of Practice for providers of GPAI models

Telenor signs up to the EU AI Pact

AI Pact = framework to prepare AI Act's implementation

Pillar I	*Pillar II*
Gathering and exchanging with AI Pact network	**Facilitating and communicatin company pledges**
• Organisation of workshops gathering organisations that have expressed an interest in the Pact • Creation and management of a dedicated online space for exchanging best practices	• Creation of templates and monitoring schemes • Organisation of meetings with interested frontrunning companies • Communication strategy to advertise the pledges

- Voluntary pledge to start implementing core aspects of the EU AI Act
- Knowledge sharing by the EU AI Office
- Best practice sharing with Europe's leading companies on Responsible AI

Thank you!

krisztina.baracsi@telenor.com