AI Talks Understanding the EU AI Act

Cooley

Part II
Rules kicking in on May 2, 2025

Presented by Patrick Van Eecke and Bartholomäus Regenhardt

Patrick Van Eecke and Bartholomäus Regenhardt

Cyber / Data / Privacy, Brussels

Learn more ›

Patrick Van Eecke
pvaneecke@cooley.com
+32 2 486 7501

Bartholomäus Regenhardt
BRegenhardt@cooley.com
+32 2 486 7542

Our recording of January 30 webinar
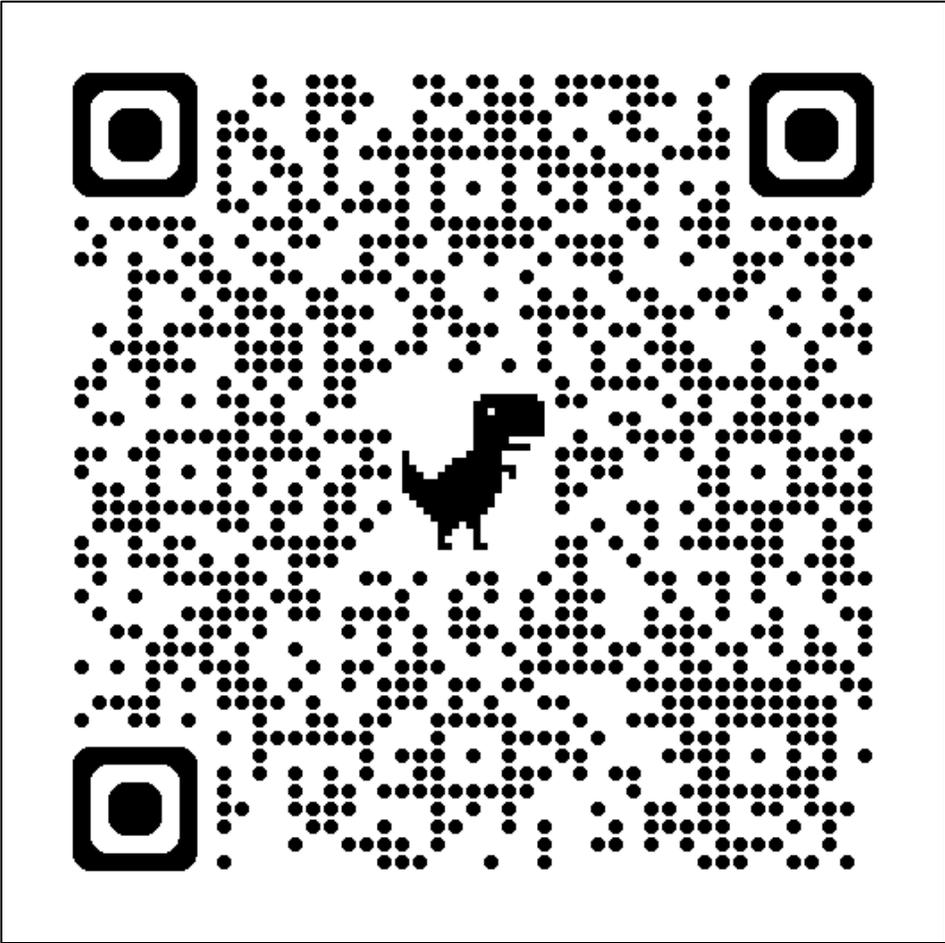
The EU AI Act

Cooley

EU AI Act: phased roll-out

13 June 2024 — AI Act formally adopted.

12 July 2024 — AI Act published in the Official Journal of the European Union.

1 August 2024 — AI Act entered into force.

2 Feb 2025 — AI literacy obligations kick off and enforcement of prohibited AI practices commences.

2 May 2025 — AI Codes of Practice initiated by the AI Office shall be ready.

2 August 2025
- GPAI governance rules and obligations apply for GPAI models on the market after this date.
- National competent authorities designated.

2024 | **2025**

2 August 2026 — The AI Act applies, with most other obligations taking effect from this date.

2 August 2027
- High-risk AI systems embedded in Annex III regulated products need to comply.
- GPAI models placed on the market before 2 August 2025 must comply.

2 August 2030 — High-risk AI systems for public authorities which were on the market before 2 August 2024 need to comply.

31 December 2030 — AI systems which are part of large-scale IT systems mentioned in Annex X of the AI Act, and were introduced before 2 August 2027, must comply.

2026 | **2027** | **2030**

EU AI Act in a nutshell

- **World's first comprehensive regulation of AI:** The European Union Artificial Intelligence Act (the "EU AI Act") is the world's first law to establish a comprehensive regulatory framework for AI.

- **Typical example of EU law**: 450 pages, almost 200 recitals, more than 100 articles and 13 Annexes.

- **Phased rollout:** Full implementation will be in place by 2 August 2026, with some specific requirements only to kick in in 2030.

- **Affects the entire value chain:** Places compliance responsibilities on a wide spectrum of stakeholders, including providers, deployers, importers, distributors, and product manufacturers.

- **Risk based system:** It classifies AI systems into different categories based on the level of risk they pose (unacceptable, high, limited and minimal): the higher the risk that an AI system poses to health, safety, fundamental rights, the environment, democracy and the rule of law, the stricter the rules.

- **Guardrails for general-purpose AI:** GPAI models must adhere to extra binding requirements for risk management, serious incident monitoring, and model evaluation.

- **Fines greater than GDPR:** Failure to comply with the EU AI Act may result in fines up to 35 million euros or 7% of worldwide turnover (whichever is higher), based on the specific violation.

- **Combination of national and centralized enforcement**: with an important role for the AI Office (European Commission) monitoring and enforcing GPAI requirements

- **In practice:** AI solutions for both commercial customer and internal use cases should be assessed against these requirements, including integrations with third party AI solutions for both of those use cases.
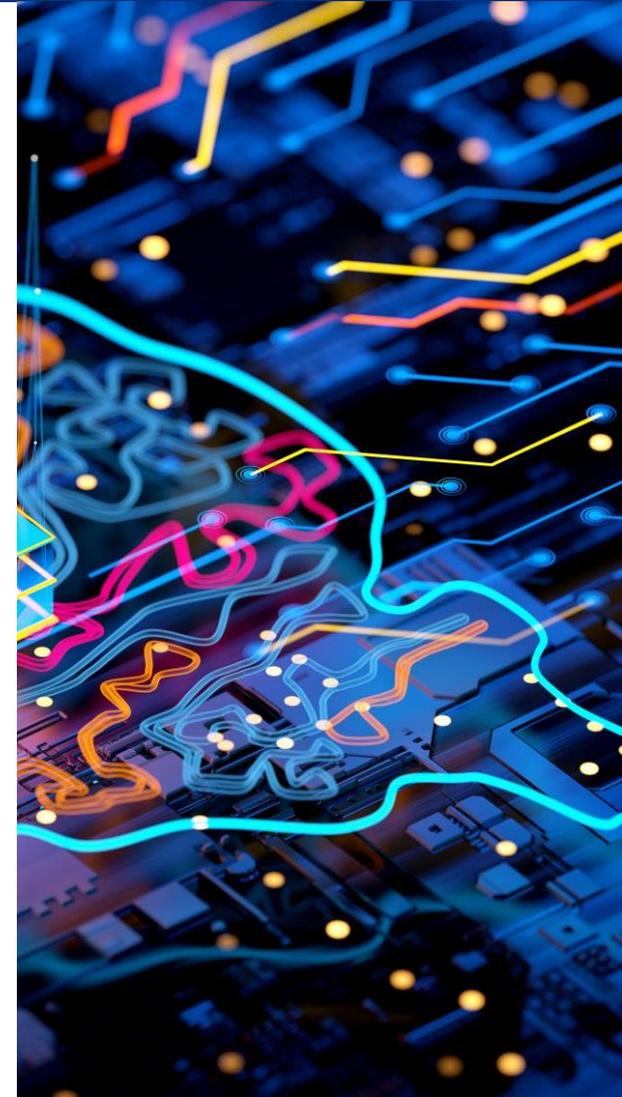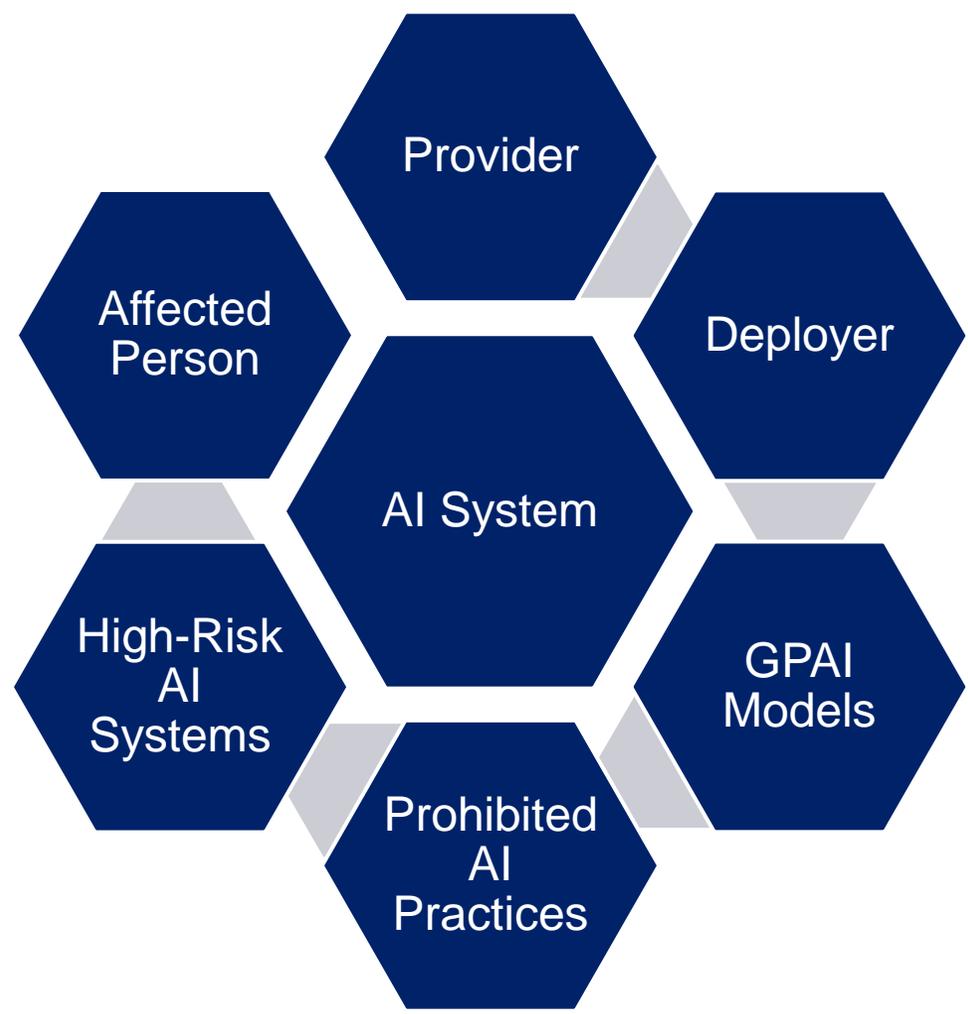
Scope of Application of EU AI Act

- EU AI Act has extraterritorial application and applies to:

  1. **providers** placing on the EU market or putting into service **AI systems** or placing on the market general-purpose AI models (**GPAI**) in the EU, whether or not the provider is located in EU;

     - *A provider is anyone who develops, sells or puts into service an AI system or a GPAI model*

  2. **deployers** of AI systems that have their place of establishment or are located within the EU;

     - *A deployer is anyone using an AI system under its authority (except if for personal non-professional activities)*

  3. providers and deployers of AI systems not based in the EU, but the **output** of the AI system is used in the EU

  4. It also applies to importers, distributors and product manufacturers of AI systems.

New concepts

- Provider
- Deployer
- Affected Person
- AI System
- GPAI Models
- High-Risk AI Systems
- Prohibited AI Practices

What has happened past 3 months?

Cooley

Since 2 February 2025

- Many companies kicked off their AI Act compliance efforts, by

  - Organizing AI literacy training for their staff (art.4 obligation)

  - Mapping and assessing their AI Systems for prohibited AI practices (art.5 obligation)

- Issues companies often confronted with:

  - How to ensure *a sufficient level of AI literacy* in practice?

  - What is an *AI System*?

  - What is a *prohibited AI practice?*

Help, how to ensure
a sufficient level of AI literacy
in practice?

Cooley

AI Literacy Obligations (art.4)

- AI Office publication

- Latest version: March 28, 2025

- Living repository of the AI literacy initiatives set up by members of the AI Pact, will be updated regularly

- Interesting:

  - Categorized based on implementation status: fully implemented, partially rolled our, or planned

  - Firmwide training plans have been rolled out at various companies.

  - Use of video/podcast resources and written handouts

  - Advanced training resources for technical employees involved in the development and/or maintenance of AI systems

  - No presumption of compliance with Article 4 / AI literacy obligations

- [Hyperlink to repository](#)

Living Repository of AI Literacy Practices – v. 28.03.2025 — EUROPEAN ARTIFICIAL INTELLIGENCE OFFICE

Living Repository of AI Literacy Practices
v.28.03.2025

Disclaimer

The following document is a **living repository** of AI literacy practices collected via a survey that was shared, for the time being, only with AI Pact pledgers. The list of practices here reported is therefore **non-exhaustive and will be** updated regularly.

The aim of this repository is exclusively to provide examples of ongoing AI literacy practices to **encourage learning and exchange** among providers and deployers of AI systems on AI literacy in light of Article 4* of the AI Act. The practices published so far were selected accordingly and divided alphabetically based on their different level of implementation (fully implemented, partially rolled-out, planned).

Please note that implementing the initiatives included in this repository does NOT automatically grant presumption of compliance with Article 4 of the AI Act. Moreover, please consider also that AI Pact pledges are non-legally binding voluntary declarations of engagement.

This living repository is part of a **broader effort of the EU AI Office to support the implementation of Article 4 of the AI Act.** Please see the AI Pact Events webpage for more information on upcoming webinars.

*Article 4 of the AI Act: Providers and deployers of AI systems shall take measures to ensure, to their best extent, 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 whom the AI systems are to be used.

AI Literacy Obligations

On the AI literacy approach

Status: Fully implemented

Target group: Organisation's staff

The AI Literacy Competency Framework is designed to enhance AI understanding across all levels of the organisation, ensuring staff is equipped to engage with AI technologies responsibly and effectively. The framework addresses diverse roles and technical expertise, tailoring learning initiatives to meet specific needs (see below).

- **Leadership:** the focus is on strategic insights, helping decision-makers understand the opportunities, risks, and ethical considerations of AI adoption.
- **Technical teams:** The framework should allow them to benefit from advanced knowledge of AI system functionality, enabling them to design, develop, and maintain systems in compliance with regulatory requirements.
- **Compliance and legal professionals:** The framework should enable them to gain tools to assess AI risk, uphold regulatory standards, and address ethical considerations in deployment.
- **HR teams:** The goal of the framework in this case is to ensure the team learns to navigate inclusivity and fairness in AI-driven decision-making processes, such as recruitment or performance evaluations. Frontline employees, who interact directly with AI systems, receive foundational training to understand their rights, obligations, and the practical impacts of AI in their roles.

The framework recognises the importance of inclusivity and diversity. It emphasises th datasets, equitable practices, and accessibility for underrepresented groups, includ minorities, and people with disabilities.

On the AI literacy approach

Status: Partially rolled-out

Target group: Organisation's staff

Our AI literacy practice is designed to be **role-based**. In line with our AI strategy, we have specific roles needed within the organisation to handle our projects. We then determined the unique **tasks and required knowledge of each role**, ensuring that our training is relevant and practical. Our AI literacy program is developed by AI experts, human resources team and team managers. Our practice does not account for specific gender identities, ethnic groups or people with disabilities.

How does the practice take into account the technical knowledge, experience, education, and training of the target group?

The AI literacy program is flexible to accommodate the diverse expertise of the company employees. Our program is finely granulated and **divided according to roles and functions**. We take into **consideration the technical backgrounds of our employees** to effectively address the needs of different teams. Moreover, we prefer interactive workshops for foundational knowledge. The content of each training session is discussed and customised with the training provider to ensure it aligns with our learning requirements and the technical backgrounds of the attendees.

How does the practice take into account the technical knowledge, experience, education, and training of the target group?

The practice is made available through our **e-learning platform** in a language and context that every employee can understand and relate to.

The practice includes an **advanced training program for selected employees that are involved in developing AI products**. This training is focusing on requirements from our Responsible Development Policy that again includes requirements from the G7 code-of-conduct. This policy is being adapted towards AI Act High Risk AI requirements and updates to the advanced training program will be made available after this update.

How does the practice take into account the context in which the AI system(s) is/are used?

The basic e-learning training program **is focused on the usage of AI, including risks, as a tool in the daily work**, but not specifically addressing the tasks involved in the development of AI systems. This is addressed in a separate program. Hence, the use and purpose in the basic training program has an outset in daily tasks like **presenting, summarising, or producing information**. The examples are specific for Customer Service, Content Creation and Summarisation, HR, Marketing, IT, Cyber security and Data Analysis. The training also highlights the risk-based approach of the AI Act and the focus on risks, use and purpose.

The **advanced training goes deeper into the requirements from our Responsible Development Policy** based on the G7 Code-of-conduct and will, before august 2025, be updated with requirements from the AI Act for high-risk AI systems with **examples on high risk uses cases from different sectors**, like law enforcement and city surveillance.

Help, what is an AI System?

Cooley

Guidelines on the "AI system"

- European Commission publication

- Published 6 February 2025, 12 pages.

- Aims to assist stakeholders, in determining whether a system constitutes an AI system within the meaning of the AI Act.

- Interesting:

    - Not binding. "*Any authoritative interpretation of the AI Act may ultimately only be given by the Court of Justice of the European Union (CJEU)*"

    - "*each system must be assessed based on its specific characteristics*"

    - approved, but not yet formally adopted

    - Will be updated taking into account "*practical experiences, new questions and use cases that arise*".

- [Hyperlink to Guidelines](#)
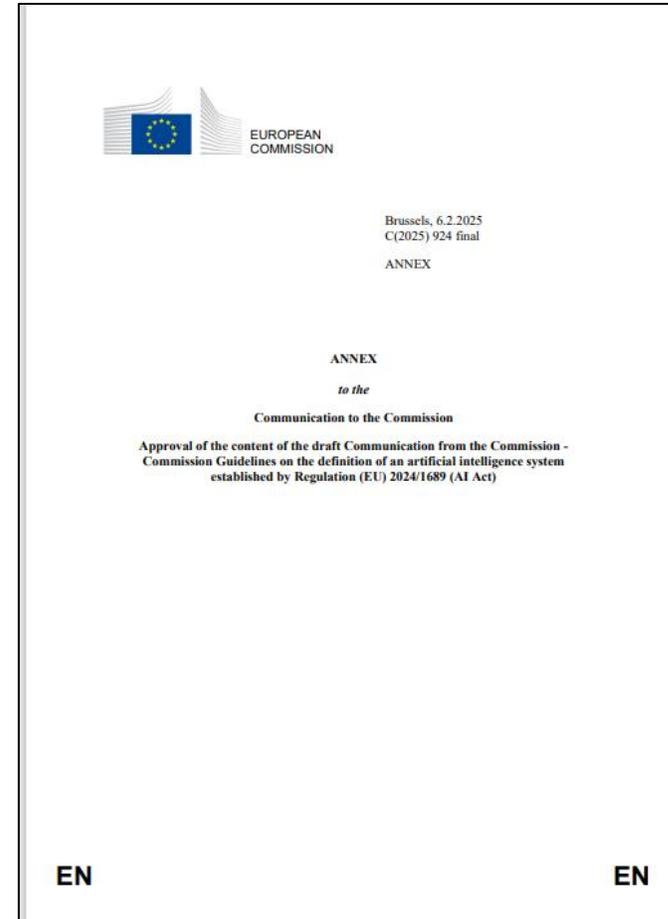
Guidelines on the "AI system"

- 7 criteria to be applied holistically

  - *"Each system must be assessed based on its specific characteristics"*

  - *"The seven elements set out in that definition are not required to be present continuously throughout both the "building" phase and the "use" phase of that lifecycle."*

  - *"Instead, the definition acknowledges that specific elements may appear at one phase, but may not persist across both phases."*

- Systems outside the scope of the AI system definition

  - *Recital 12: "simpler traditional software systems or programming approaches and should not cover systems that are based on the rules defined solely by natural persons to automatically execute operations."*

AI System definition

1. machine-based system
2. designed to operate with varying levels of autonomy
3. may exhibit adaptiveness after deployment
4. that, for explicit or implicit objectives
5. infers, from the input it receives,
6. how to generate outputs such as predictions, content, recommendations, or decisions
7. that can influence physical or virtual environments

Guidelines on the "AI system": out of scope

NOT AI SYSTEM: Systems for improving mathematical optimization

- Systems used to improve mathematical optimisation or to accelerate and approximate traditional, well established optimisation methods, such as linear or logistic regression methods
- **Example**: a satellite telecommunication system to optimize bandwidth allocation and resource management.

NOT AI SYSTEM: Basic data processing

- Systems that follow predefined, explicit instructions or operations. These systems are developed and deployed to execute tasks based on manual inputs or rules, without any 'learning, reasoning or modelling' at any stage of the system lifecycle.
- **Example**: a software system that applies statistical techniques to opinion polls or survey data to determine their validity, reliability, correlation, and statistical significance

NOT AI SYSTEM: Systems based on classical heuristics

- Unlike modern machine learning systems, which adjust their models based on input-output relationships, classical heuristic systems apply predefined rules or algorithms to derive solutions.
- **Example**: a chess program using a minimax algorithm with heuristic evaluation functions can assess board positions without requiring prior learning from data.

NOT AI SYSTEM: Simple prediction systems

- Machine-based systems whose performance can be achieved via a basic statistical learning rule
- **Example**: systems o predict future stock prices by using an estimator with the 'mean' strategy to establish a baseline prediction (e.g., always predicting the historical average price).

"AI washing" risk?

Help, what is a prohibited AI practice?

Cooley

Guidelines on "Prohibited AI practices" (art. 5)

- European Commission publication

- Published 4 February 2025, 140 pages!

- Interesting

  - Specifically address practices such as harmful manipulation, social scoring, and real-time remote biometric identification

  - Provides legal explanations and practical examples

  - Approved, but not yet formally adopted

  - Not binding. "*Any authoritative interpretation of the AI Act may ultimately only be given by the Court of Justice of the European Union (CJEU)*"

- [Hyperlink to the Guidelines](#)

Some examples

Subliminal techniques	An AI chatbot that impersonates a friend of a person or a relative with synthetic voice and tries to pretend it is the person causing scams and significant harms. An AI chatbot promotes self-harm to users or incentivises them to commit suicide or harm other persons or groups of persons by promoting terrorist content or incentivising violence against certain persons or groups of persons (i.e., minorities)
Harmful exploitation of vulnerabilities	An AI system targeting older people with deceptive personalised offers or scams, exploiting their reduced cognitive capacity aiming to influence them to make decisions they would not have taken otherwise that are likely to cause them significant financial harm An AI system that targets young users and uses addictive reinforced schedules with the objective of keeping them dependent on the application
Social scoring	A private credit agency uses an AI system to determine the creditworthiness of people and decide whether an individual should obtain a loan for housing based on unrelated personal characteristics. An insurance company collects spending and other financial information from a bank which is unrelated to the determination of eligibility of candidates for life insurance and which is used, using an AI system, to determine the price of the premium to be paid for such insurance.
Emotion recognition in the workplace or education	Using emotion recognition AI systems during the recruitment process is prohibited. An AI system that infers that an employee is unhappy, sad or angry towards customers (e.g. from body gestures, a frown or the lack of a smile) is prohibited Medical exception: An employer using AI-enabled devices or digital assistants at the workplace to measure anxiety based on measured stress levels when deploying dangerous machines or dealing with dangerous chemicals (due to exceptions for safety and medical reasons)

Enforcement?

- What if you do not comply with the AI Act obligations currently in force (Chapters 1 and 2)?

- Chapter on fines and penalties not applicable yet!

  - Chapter XII on fines and penalties: applies from August 2, 2025 (except art. 101)

  - Article 101 Fines for providers of general-purpose AI models: applies from August 2, 2026

  - Is non-compliance with article 4 (AI literacy) sanctionable anyhow?

- National authorities not designated yet!

  - Member States must designate their national competent authorities by August 2, 2025.

  - European Commission: "*In this interim period, there will also be no market surveillance authorities to monitor whether the prohibitions are being properly complied with.*"

- However: claims and injunctions

  - European Commission: "*the prohibitions themselves have direct effect and thus enable affected parties to enforce them in national courts and request interim injunctions against the prohibited practices*"


21

Code of Practice for GPAI
New milestone: May 2, 2025

Cooley

General-Purpose AI (GPAI) Models

- GPAI models = "*an AI model […] trained with a large amount of data using self-supervision at scale, that displays **significant generality** and is capable of competently performing 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**"*

- At least a billion parameters and trained with a large amount of data using self-supervision at scale

- Examples: Large generative AI models

- GPAI models with **systemic risk**
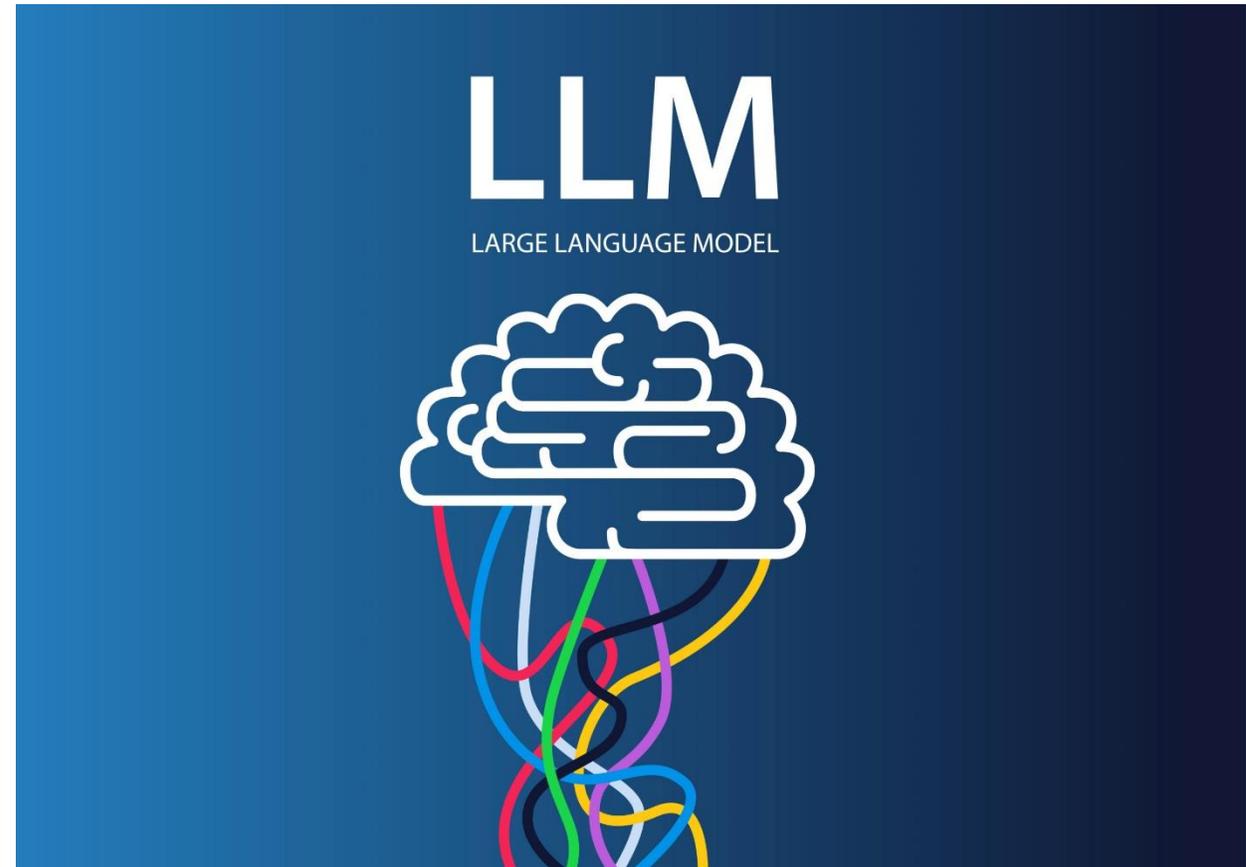
Provider

Definition

a natural or legal person, public authority, agency or other body that

- *develops* an AI system or a **general-purpose AI model**, or

- that has an AI system or a **general-purpose AI model** *developed* and places it on the market, or

- puts the AI system into service under its own name or trademark, whether for payment or free of charge.

Explanation

A developer is the entity that designs, develops, or builds a GPAI model, including writing the code, designing the model, providing technical documentation and instructions for use and making decisions regarding the functionality and purpose of the GPAI model.

If a GPAI model is fine-tuned or modified, will this make me a GPAI provider?

Downstream entities that fine-tune or otherwise modify an existing GPAI may become **providers of new models**

Where GPAI model is modified or fine-tuned

    obligations for providers of GPAI are limited to the **modification or fine-tuning**

    e.g.: complementing the already existing technical documentation with information on the modifications

Regardless of whether a downstream entity is deemed to be a provider of the **GPAI model →** **must always comply** with obligations for **AI systems**

What are the obligations for providers of GPAI models?

- **Technical information** about GPAI model to provide to

  - **AI Office** and **national competent authorities** (Annex **XI**)

  - **downstream providers** who integrate it in AI system (Annex **XII**)

- **Copyright policy**

- Make publicly available a sufficiently detailed **summary about the content used for training the GPAI model**
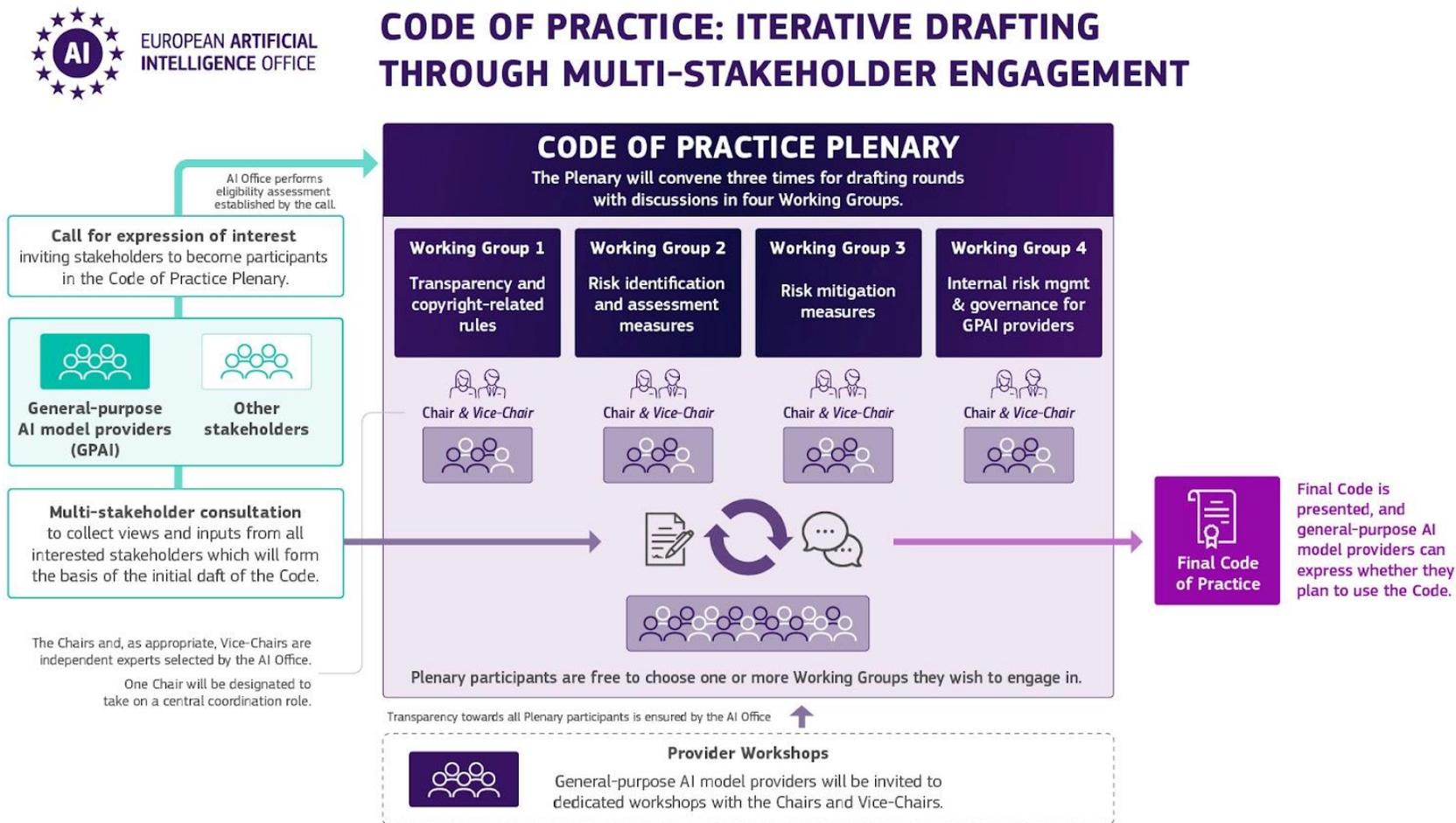
What is the GPAI Code of Practice (GPAI CoP)?

- **Voluntary compliance** framework

- How **providers of GPAI models** (with systemic risk) may comply with their obligations

- The AI Office is facilitating the drawing-up of this GPAI CoP

- **Four working groups** chaired by independent experts

- Nearly **1000 stakeholders** involved

Drafting of the GPAI CoP

Drafting of the GPAI CoP

Commission admits AI code of practice could be delayed
By Pieter Haeck · Apr 28, 2025, 4:05 PM · View in your browser

The European Commission said today it "cannot commit" to meeting a Friday deadline for new rules covering the most advanced artificial intelligence models.

Dr... Foundation and Structure (November 2023)

Draft 3 – Pre-Final Draft (March 2025)

Trump Administration Pressures Europe to Ditch AI Rulebook

Trump and the EU are increasingly clashing over the latter's role as the world's chief digital rulemaker, and the President has lambasted the bloc's tech regulations and fines as unfairly targeting US companies. *Photographer: Al Drago/Bloomberg*

By Gian Volpicelli, Samuel Stolton, and Alberto Nardelli
April 25, 2025 at 2:50 PM GMT+2
Updated on April 26, 2025 at 7:10 PM GMT+2

Focuse...
- Initia... trans... and s...
- High... rathe... oblig...

...used on:
...larifying the distinction ...etween GPAI models ...nd downstream ...pplications
...ore detailed ...ommitments on risk ...anagement, model ...valuation, and incident ...onitoring
...ddressing open-source ...xemptions and innovation flexibility

...transp... copyright obliga...
- Implementation and governance
- Inclusion of a Model Documentation Form to streamline reporting
- Specific risk mitigation commitments for systemic risk GPAI models

# What are the legal effects of the GPAI CoP?

- Adherence = means to **demonstrate compliance** with the AI Act, while

  ___not___ **providing a presumption of conformity** with the AI Act

- AI Office may take a provider's adherence to the GPAI CoP into account when

  - **monitoring its effective implementation and compliance**

  - **fixing the amount of fines** depending on the specific circumstances

GPAI CoP

1 - Commitments - Third Draft General-Purpose AI Code of Practice

Download

2 - Transparency - Third Draft General-Purpose AI Code of Practice

Download

3 - Copyright - Third Draft General-Purpose AI Code of Practice

Download

4 - Safety and Security - Third Draft General-Purpose AI Code of Practice

Download

Transparency obligations: AI System/GPAI Model
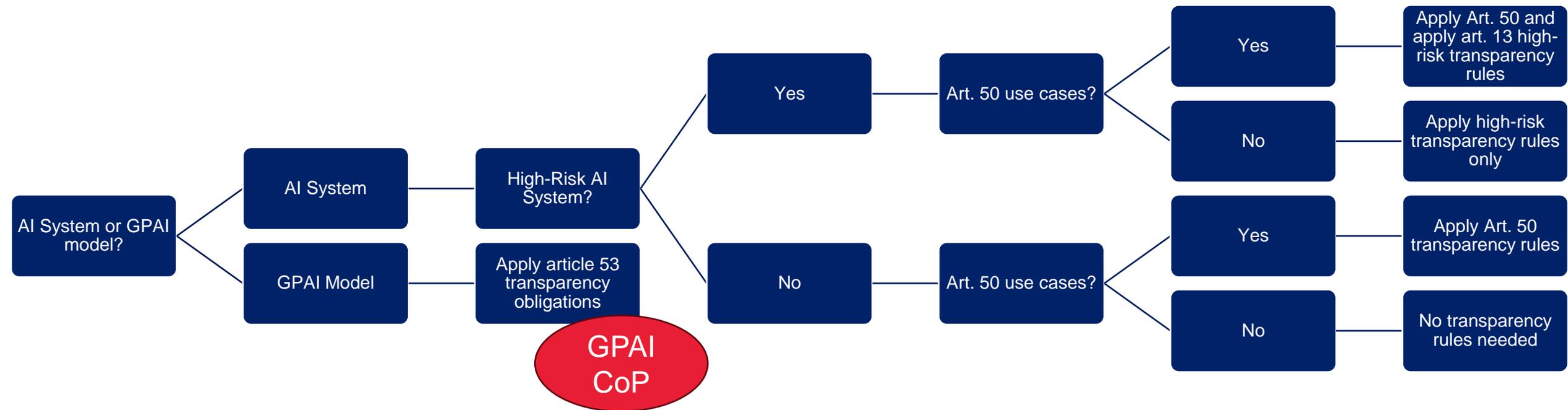
Transparency

- **Drawing up and keeping up-to-date model documentation**

  - "Information and Documentation about the General-Purpose AI Model" (**Model Documentation Form**)

  - Required to update form and keep previous version for 10 years

- **Providing relevant information**

  - Publicly disclose contact information for the AI Office and downstream providers to request access to the Model Documentation

  - Share information with AI Office and/or downstream providers subject to confidentiality obligations

  - Optional publication of certain data from Model Documentation Form

- **Ensuring quality, integrity, and security of information**

  - Documented information should be controlled for quality and integrity, retained as evidence of compliance with obligations of the AI Act, and protected from unintended alteration

- Measures do *not apply* to providers of **open-source** GPAI models, unless they are GPAI models with systemic risk
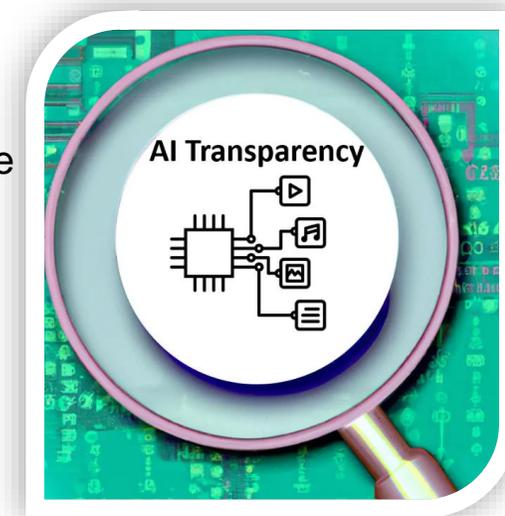
ANNEX XI

Technical documentation referred to in Article 53(1), point (a) — technical documentation for providers of general-purpose AI models

Section 1

Information to be provided by all providers of general-purpose AI models

The technical documentation referred to in Article 53(1), point (a) shall contain at least the following information as appropriate to the size and risk profile of the model:

1. A general description of the general-purpose AI model including:

   (a) the tasks that the model is intended to perform and the type and nature of AI systems in which it can be integrated;

   (b) the acceptable use policies applicable;

   (c) the date of release and methods of distribution;

   (d) the architecture and number of parameters;

   (e) the modality (e.g. text, image) and format of inputs and outputs;

   the licence.

ANNEX XII

Transparency information referred to in Article 53(1), point (b) — technical documentation for providers of general-purpose AI models to downstream providers that integrate the model into their AI system

The information referred to in Article 53(1), point (b) shall contain at least the following:

1. A general description of the general-purpose AI model including:

   (a) the tasks that the model is intended to perform and the type and nature of AI systems into which it can be integrated;

   (b) the acceptable use policies applicable;

   (c) the date of release and methods of distribution;

   (d) how the model interacts, or can be used to interact, with hardware or software that is not part of the model itself, where applicable;

   (e) the versions of relevant software related to the use of the general-purpose AI model, where applicable;

   (f) the architecture and number of parameters;

   (g) the modality (e.g. text, image) and format of inputs and outputs;

   (h) the licence for the model.

Model Documentation Form

This Form includes all the information to be documented as part of Measure 1.1. Crosses on the right indicate whether the information documented is intended for the AI Office (AIO), national competent authorities (NCAs) or downstream providers (DPs), namely providers of AI systems who intend to integrate the general-purpose AI model into their AI systems. Whilst information intended for DPs should be made available to them proactively, information intended for the AIO or NCAs is only to be made available following a request from the AIO, either ex officio or based on a request to the AIO from NCAs. Such requests will state the legal basis and purpose of the request and will concern only items from the Form strictly necessary for the AIO to fulfil its tasks under the AI Act at the time of the request, or for NCAs to exercise their supervisory tasks under the AI Act at the time of the request, in particular to assess compliance of high-risk AI systems built on general-purpose AI models where the provider of the system is different from the provider of the model.

Any elements of information from the Model Documentation Form shared with the AIO, NCAs or DPs shall be treated in accordance with the confidentiality obligations and trade secret protections set out in Article 78.

Date the document was last updated:　　　　**Document version number:**

General information	AIO	NCAs	DPs
Legal name for the model provider:	☒	☒	☒
Model family: The identifier, if any, for the collection of models (e.g. Llama).	☒	☒	☒
Versioned model name: The unique identifier for the model (e.g. Llama 3.1-405B).	☒	☒	☒
Model authenticity: Evidence that establishes the provenance and authenticity of the model (e.g. a secure hash if binaries are distributed, the URL endpoint in the case of a service), where available.	☒	☒	☐
Release date: Date when the model was first released through any distribution channel.	☒	☒	☒
Union market release: Date when the model was placed on the Union market.	☒	☒	☒
Model dependencies: The list of other general-purpose AI models that the model builds upon, if any (e.g. the list for llama-3.1-nemotron-70b would be [llama-3.1] and the list for llama-3.1 would be empty). For each listed model dependency, please include a copy or link to the associated Model Documentation or indicate that the Model Documentation is not accessible.	☒	☒	☒

Model properties	AIO	NCAs	DPs
Model architecture: A general description of the model architecture, e.g. a transformer architecture. [Recommended 20 words]	☒	☒	☒
If the model is a general-purpose AI model with systemic risk, provide a detailed description of the model architecture, specifying where it departs from standard architectures where applicable. If the model is not a general-purpose AI model with systemic risk, write 'N/A'.	☒	☐	☐
Design specification of the model: A general description of the key design choices of the model, including rationale and assumptions made, to provide basic understanding into how the model was designed. [Recommended 100 words]	☒	☒	☐
Input modalities: For each selected modality, please include maximum input size or write 'N/A' if not defined. ☐ Text ☐ Images ☐ Audio ☐ Video — If any other please specify:	☒	☒	☒
Maximum size: / Maximum size: / Maximum size: / Maximum size: / Maximum size:	☐	☐	☒
Output modalities: ☐ Text ☐ Images ☐ Audio ☐ Video — If any other please specify:	☒	☒	☒

Copyright

- Draw up, keep up-to-date and implement a **copyright policy** + make publicly available a **summary of the copyright policy**

- Reproduce and extract **only lawfully accessible copyright-protected** content when crawling the web

  - Crawlers respect technologies restricting access to copyrighted materials, such as paywalls

  - Exclude so-called "piracy domains", i.e. business models that provide copyright-infringing materials

- Identify and comply with **rights reservations** when crawling the web

  - Respect text and data mining opt-out declared by rightsholders (generally allowed under

    EU copyright law, but rightsholders may declare to opt-out)

- Obtain adequate information about **protected content not web-crawled** by the Signatory

  - Make reasonable efforts to obtain information as to whether web crawlers used to gather the information complied with a robot.txt

- **Mitigate** the risk of production of **copyright-infringing output** (contractually prohibiting prohibit a copyright-infringing use of their GPAI model for downstream providers)

- Designate a **point of contact** and enable the lodging of complaints

The EU AI Act and the GPAI CoP

AI Act

- Binding legislation adopted by the EU

- Establishes a comprehensive regulatory framework for AI across the EU

- Introduces a risk-based classification system for AI systems and GPAI models

- Imposes a mandatory obligation on providers and deployers of AI (AI systems and GPAI models)

> The GPAI CoP is **a bridge connecting the regulatory goals of the AI Act with the practical needs of AI providers/developers**. Following the GPAI CoP can demonstrate good-faith efforts to comply with the AI Act, potentially reducing the risk of enforcement or penalties.

EU AI Code of Practice

- A non-binding, voluntary framework created to help providers of GPAI models comply with the AI Act – particularly Articles 53 and 55

- Developed by independent experts with broad stakeholders' input (including industry, civil society and academia).

- Offers practical tools, documentation templates, and commitments for:
  - Transparency (e.g., training data summaries, and copyright information),
  - Copyright,
  - Safety and risk management for systemic GPAI models.

- Designed to operationalize the AI Act's legal requirements, making them easier to apply in practice

- Initially expected to be finalized in May 2025

41

The AI Liability Directive saga!

- **August 2022:** Initial draft of AI Liability Directive was published in 2022

    - To set clear rules for who is responsible when AI causes harm ("ex-post" whilst AI Act is preventing harm)

- **October 2024:** revised draft

    - Regulation instead of Directive; broader scope; objective liability

- **February 2025:** withdrawn

    - EU Commission Work Program 2025; withdrawal of AI Liability Directive

- **April 2025:** Back on the agenda?

    - Civil society organisations (incl BEUC) as well as some EP members push to have AI Liability Directive back on the agenda

- **To be continued!**

EUROPEAN COMMISSION

Brussels, 28.9.2022
COM
2022

Proposal for a

DIRECTIVE OF THE EUROPEAN PARLIAME

on adapting non-contractual civil liability rul **(AI Liability Directiv**

(Text with EEA relevan

{SEC(2022) 344 final} - {SWD(2022) 318 final}
{SWD(2022) 320 fina

Open Letter to the European Commission on the announced withdrawal of the AI liability Directive

7 April 2025

Dear Executive Vice-President Virkkunen,
Dear Commissioner McGrath,

We, the undersigned representatives of civil society, are writing to express our concerns regarding the European Commission's announcement to withdraw the proposal for a directive on adapting non-contractual civil liability rules to artificial intelligence (AILD).[1]

While the proposal could be improved, we are concerned with this decision and urge the European Commission to immediately begin preparatory work on **new AI liability rules** in line with the Better Regulation policy. The EU needs rules to address the legal gaps left by the AILD withdrawal and ensure a fairer, simpler path to compensation for all people affected by AI systems, including consumers in the EU, in case of harm by an AI system.

Why clear AI liability rules matter

Today, many people face a daunting task if they are harmed by an AI system and try to seek compensation. This happens because it is very difficult, if not impossible, for the large majority of people to prove that it was the *faulty* behaviour of the AI operator that led to a certain harm.

That is too heavy a burden. For example, it is unrealistic to expect a consumer who has been discriminated against by an AI system used by an insurance company to prove that it was this specific AI system that led to some form of harm. Similarly, it is unfeasible for a citizen seeking welfare assistance to demonstrate that a risk assessment system led to an unjustified deprivation of their benefits. This is why any new AI liability rules replacing the AILD should at the very least include a **non-fault based liability approach**.

In addition, while the revised Product Liability Directive (PLD) also applies to AI systems, it is not comprehensive enough. Important legal gaps remain. For example, the PLD does not allow for claims against the deployer of the AI system (e.g. bank, insurance or public institution using an AI system from another provider), which would be the obvious point of contact for the affected person in case of harm. The PLD would not apply in case of specific harms, such as discrimination.

Key takeaways

☑ Assess whether you are in scope of the AI Act

☑ Assess whether AI system or GPAI model obligations apply

☑ Assess your role: are you a provider or a deployer

☑ Assess whether you risk to engage in prohibited practices

☑ Train your staff and other people involved

☑ Consider EU privilege rules when documenting

☑ Join our next webinar on July 31, 2025.

Patrick Van Eecke

Cyber/data/privacy and Government regulatory & policy, Brussels

Learn more >

Patrick co-chairs Cooley's global cyber/data/privacy practice. Patrick has more than 30 years of experience guiding clients on complex issues spanning data protection, cyber, electronic commerce, digital advertising and electronic signatures. He advises startups, scaleups and multinationals in diverse industry sectors, from technology and life sciences to communications, entertainment, retail and consumer products. He also has significant experience representing telecommunications companies, internet service providers, software developers, governments and companies using IT-related services. In addition, Patrick is involved in diverse consulting projects for the European Commission, national governments and multinational global corporations.

Prior to joining Cooley, Patrick was the co-chair of a global top 10 firm's data privacy and cybersecurity practice. For several years, he has been consistently recognized as a Band 1 and Tier 1 data protection and cyber authority by Chambers Europe and The Legal 500 EMEA, respectively. Recognition also includes in November 2024 winning Data Privacy Lawyer of the Year award at the Lexology Index Awards.

Patrick is a regular speaker at national and international conferences, and he often is asked to comment on internet and cyber law-related issues in the press.

Bartholomäus Regenhardt

Cyber/data/privacy and Government regulatory & policy, Brussels

Learn more >

Bartholomäus advises international clients on a wide range of digital-related matters, with a focus on General Data Protection Regulation (GDPR) implementation, artificial intelligence (AI), cross-border transfers of personal data, cybersecurity, ecommerce and digital health. His clients include startups, scaleups and multinationals in diverse industries, and he has a strong track record in the technology, telecommunications and biotechnology sectors.

Bartholomäus counsels clients on compliance and risk management projects in the financial and life sciences sectors, as well as on long-term innovative projects involving large-scale data processing activities. He advises on the new European legal frameworks, including the AI Act, Data Act and Digital Services Act, and legal challenges posed by cloud computing, electronic contracting, electronic signatures, cryptocurrencies and blockchain in a European context.

Bartholomäus is qualified to practice in Germany and Belgium, and he is fluent in German and English.

Before joining Cooley, Bartholomäus was an in-house counsel in the data privacy and cybersecurity practice of a German bank in Düsseldorf.

Cooley