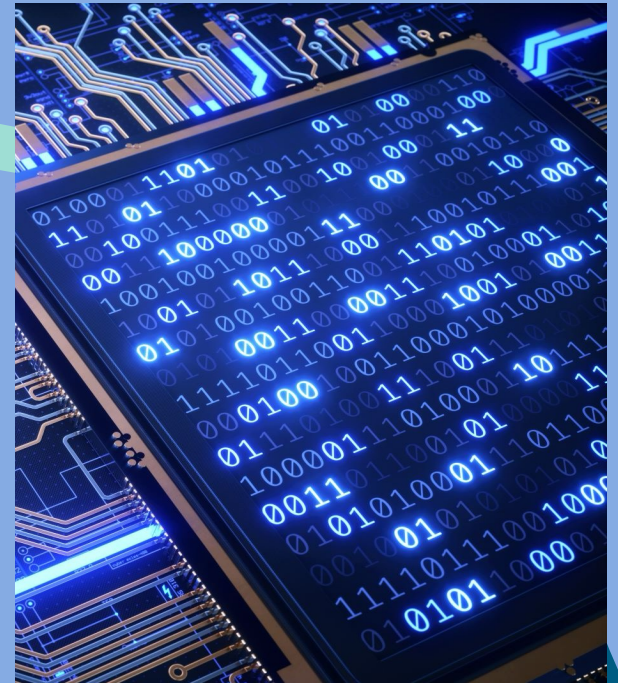


Bird & Bird

Navigating AI Governance: Insights on the EU AI Act

July 14, 2025

Presentation followed by a panel discussion



Welcome video

PLACEHOLDER FOR VIDEO PROJECTION

Speakers & Presenters

Moderation



Chris de Mauny

*US Co-Head & IP Partner
at Bird & Bird LLP*



Isabel Hahn

*Policy Officer for AI at EU Delegation
to the United States*

Presenters and panelists



Vincent Rezzouk-Hammachi

*US Co-Head &
Global Head of Privacy Solutions
at Bird & Bird LLP*



Danielle Kehl

*Senior Counsel, AI Policy &
Regulation, OpenAI*



Matt Tonner

Senior Director, AI Legal, Salesforce

Bird & Bird

European Union
Artificial Intelligence
Act: *a guide*

7 April 2025



1. AI Act Overview and Essentials

The AI Act: Too soon or too late?

Is the EU overregulating AI?

The EU is overregulating AI

Caution and control are being overemphasised above economic and technological opportunity

ARTILLERY ROW By **Pieter Cleppe** 9 June, 2024



Earlier this year, the European Parliament [voted](#) in favour of the EU Artificial Intelligence Act or “AI Act”. With this, the EU becomes the first jurisdiction comprehensively regulating AI. What the EU [hopes](#) is that the EU’s legislative approach will influence other jurisdictions through the so-called “[Brussels effect](#)”, whereby regulated entities, especially corporations, end up complying with EU laws even outside the EU, mostly due to the size of the EU’s single market.

[Home](#) > [News](#) > The AI Act: Is It a Golden Standard or Just Another Over-Regulation Symphony from Brussels?

THE AI ACT: IS IT A GOLDEN STANDARD OR JUST ANOTHER OVER-REGULATION SYMPHONY FROM BRUSSELS?

M. Metin Uzun, PhD candidate, University of Exeter
3 July 2023



AI Act framework

AI regulation in a nutshell



- Different approaches worldwide to **AI regulation** (e.g. UK/US/EU/China)
- EU decided to adopt AI-specific **product safety regulation** that follows a **risk-based approach**
- **Majority of AI applications** and tools will not be covered; the main burden falling on **providers** (as opposed to deployers, for example) of certain AI systems or models (i.e. high-risk AI and GPAI models)
- EP proposal to include **general principles for all AI systems** was removed at the last minute (e.g. human agency, oversight and transparency)
- But: **More stringent technical and documentary requirements** especially on high-risk AI systems (e.g. assessments of the impact on fundamental rights and conformity assessments)

Scope of the Act

Who is subject to it?



Providers in or outside the EU where they place on the market or put into service AI systems or GPAI models in the EU

Providers and Deployers outside the EU where the output produced by the AI system is used in the EU

Deployers established or located in the EU

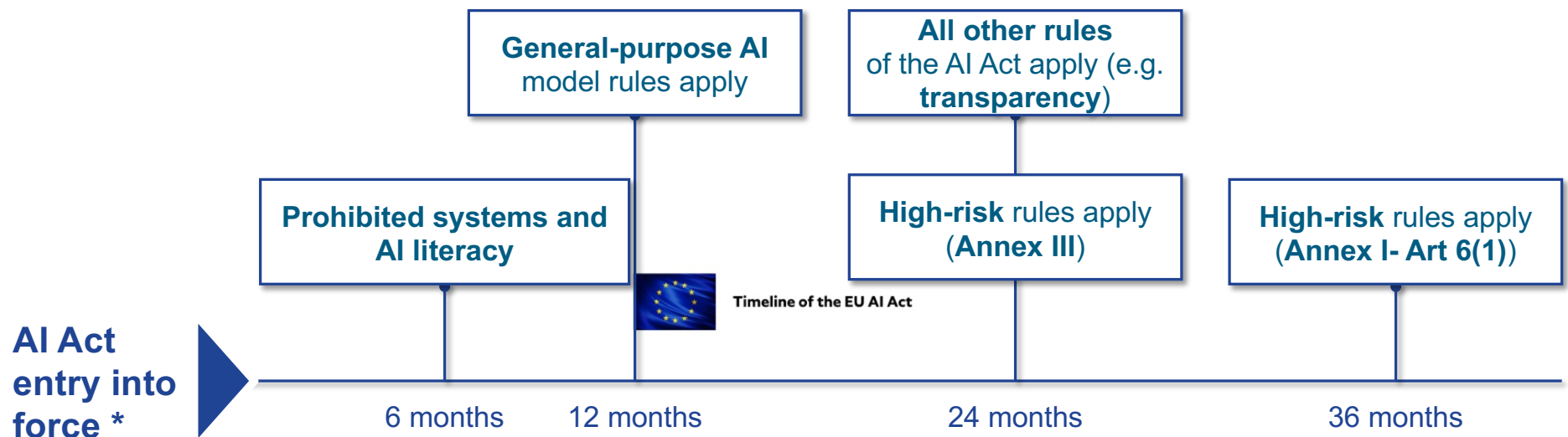
Importers and Distributors of AI Systems

Product manufacturers integrating an AI system into their product under their own name or trademark and putting on the market or putting to use

Authorised Representatives of the providers outside the EU

Timelines

When will it apply?



1 August 2024

Scope of the Act

Who is NOT subject to it and which systems are out of scope?

High risk systems that are already on the market **prior to August 2026** unless a significant change is made to them.

AI systems and models, including their output, specifically developed and put into service for the sole purpose of **scientific research and development**

Public authorities in a third country or international organisations that use AI systems in the framework of international cooperation or agreements for law enforcement and judicial cooperation with the EU or EU member states

Individuals who use the AI system in the course of a purely **personal, non-professional activity**

AI systems to be exclusively used for **military, defence or national security purposes** regardless of the type of entity carrying out this activity

Definition of AI systems

Which systems are in scope of the AI Act?

*"**AI system**' means a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments."*

Key elements:

"Infers" - AI systems can produce outputs not pre-determined by strict algorithms

"Autonomy" - AI systems can operate with a degree of autonomy

Intentionally broad definition:

to avoid becoming outdated, technology-neutral approach, moving away from a pre-defined list of AI techniques (following OECD definition)

Commission guidelines:

Guidelines to aid in the application of the AI system definition developed by the Commission

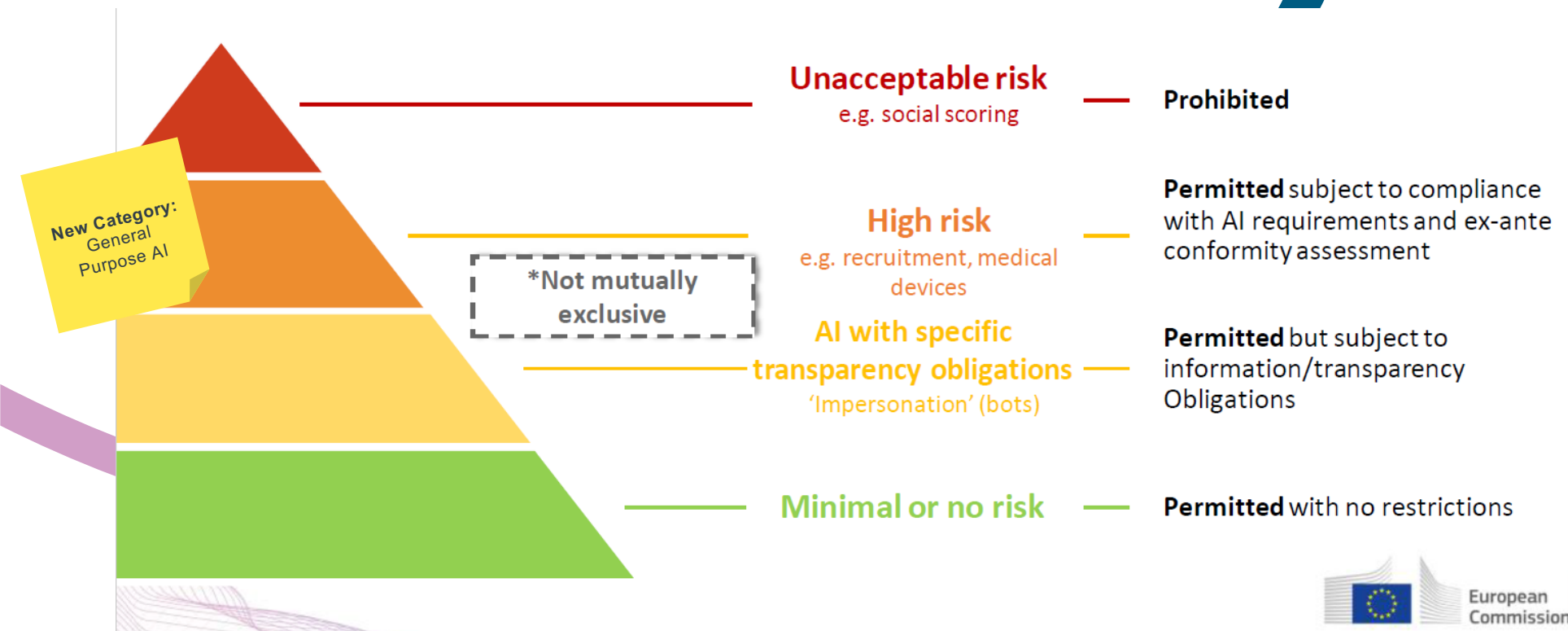
Economic operators in scope

The AI Act impacts the entire AI ecosystem

	Provider (most obligations)	Deployer (deployment, data quality and monitoring obligations)	Providers and deployers	Distributors and importers (verification obligations)
Meaning	develops AI systems or a GPAI model, or has one developed , and subsequently places it on the market or puts it into service under its own name or trademark	use an AI system under their authority . This category excludes personal, non-professional use of AI systems	See columns to the left	Importer: Located in the EU and place on the market an AI system carrying the name or trademark of someone established outside the Union Distributor: Neither provider nor importer but make AI systems available
Territoriality	placing AI systems on the EU market - irrespective of whether established in the EU or a third country	in the EU , under whose authority the system is used	established in a third country , where the output of the AI system is used in the EU	making available/placing AI systems on the EU market

Risk-based approach of the AI Act

AI system classification under the AI Act



Prohibited AI Systems

What is banned?

Subliminal, manipulative or deceptive AI systems: that distort human behaviour materially and subvert free-choice

Exploiting vulnerabilities: due to age, disability or socio-economic background and causes them significant harm

Social scoring based on social behaviour or known/ inferred/ predicted traits: leading to negative treatment in unrelated contexts/or are unjustified/ or disproportionate

Predicting criminality: on the basis of profiling or assessing personality traits and characteristics

ARTICLE 5

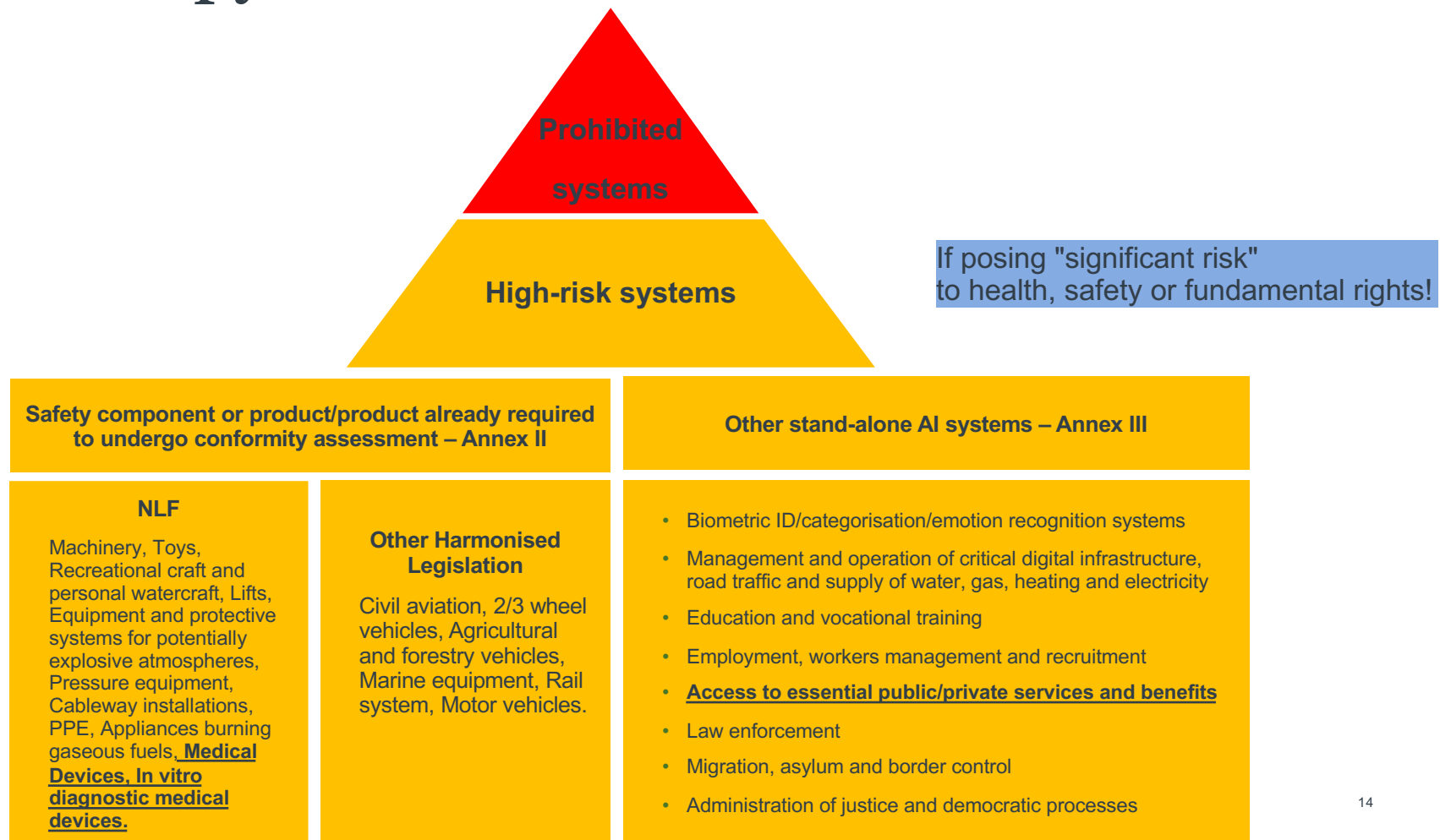
Scraping the web or CCTV footage: to create or expand facial recognition database

Inferring emotions in workplace or schools: except for health and safety reasons

Biometric categorisation: based on certain sensitive data (e.g. race, political opinions, trade union membership, religion, sexual orientation etc.) except for labelling or filtering legally acquired datasets

Real-time remote biometric identification systems in publicly accessible spaces by the law enforcement –subject to exceptions

The AI risk pyramid



Sweet escape?

High-risk but not regulated as such

NB: Only for Annex III systems!

No significant risk of harm, to the health, safety or fundamental rights of natural persons, including by not materially influencing the outcome of decision making:

1. the AI system is intended to perform a **narrow procedural task**;
2. the AI system is intended to **improve** the result of a **previously completed human activity**;
3. the AI system is intended to detect decisionmaking patterns or deviations from prior decisionmaking patterns and is **not meant to replace or influence the previously completed human assessment**, without proper human review; and/or
4. the AI system is intended to perform a **preparatory task** to an assessment relevant for the purpose of high-risk use case.

NB: no escape if the AI system performs **profiling** of natural persons!

Key compliance factors for high-risk AI

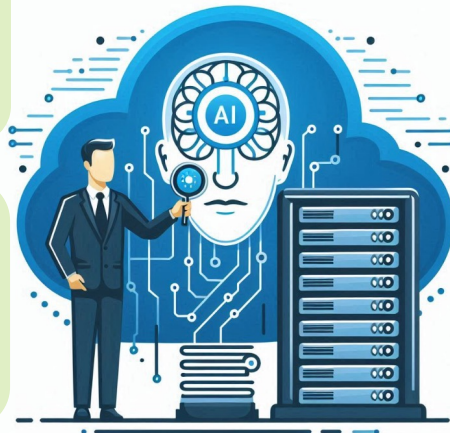
What are the technical and organizational requirements for high-risk AI

- **High-risk AI systems** must meet Articles 9-15 throughout the life cycle of an AI system; potential tensions and trade-offs must be addressed adequately
- Products covered by certain **product safety legislation**: Integration of AI Act requirements into conformity assessments of such relevant EU product safety laws:

Risk Management:
Identification, analysis, and mitigation strategies are critical

Data Governance: For data training or testing (relevance, representativeness, free of errors and complete (best efforts))

Technical Documentation/Record keeping: TD to demonstrate compliance, and RK for traceability and post-market surveillance



Transparency: Systems should be designed for deployers to comprehend outputs; instructions for use required


Human Oversight:
Technically and/or organizationally, proportionate to the risks, the level of autonomy and the context of use

Accuracy, Robustness and Cybersecurity:
Systems should maintain accuracy, security, and ensure resilience

Key compliance factors for high-risk AI

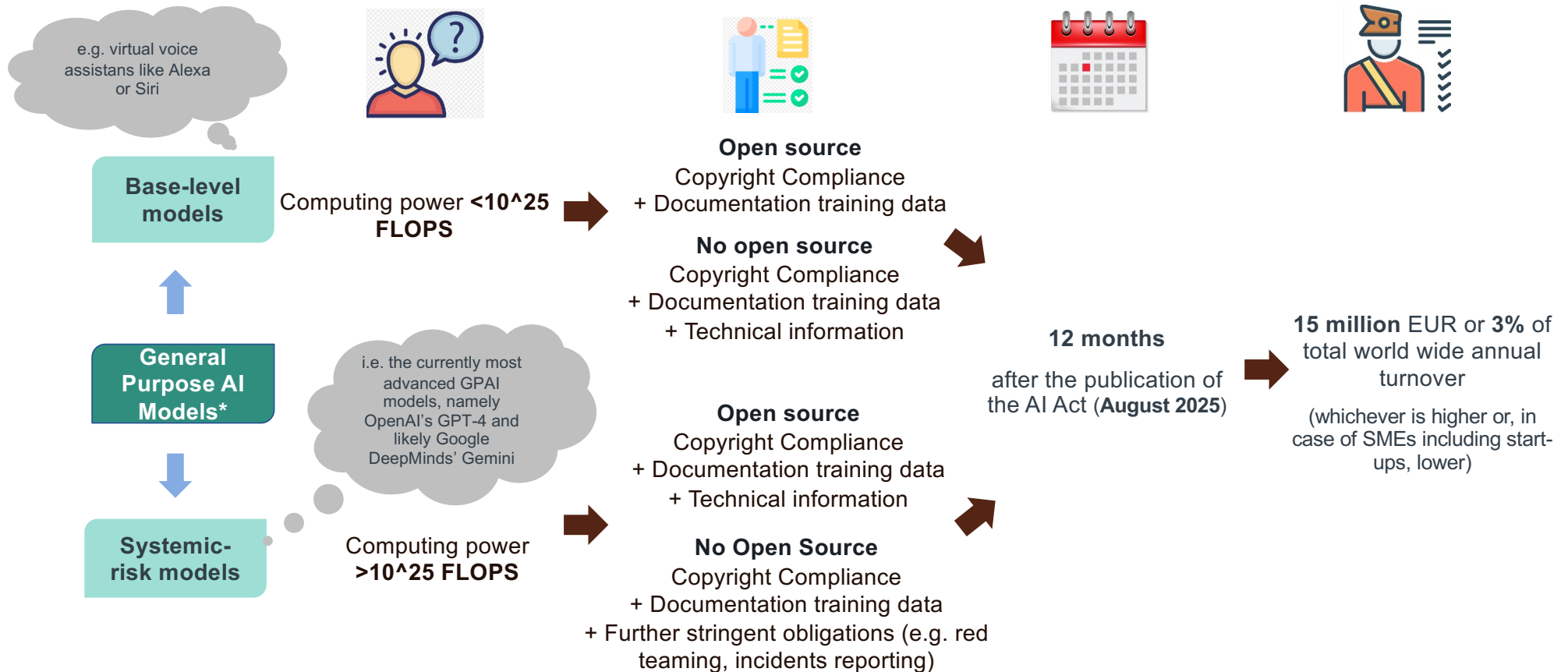
What are the requirements for economic operators of high-risk AI?



Provider obligations	Deployer obligations	Importers	Distributors
must ensure the previous technical and organizational requirements for high-risk and, in addition , AI quality management, post-market monitoring, corrective actions, authority cooperation, system registration, and conformity assessments	must ensure that an AI system's real-world application adheres to the design by the provider and complies with operational regulations of the provider , e.g. input data control, monitoring and incident reporting or record keeping  Role shift - deployer using AI systems may unknowingly assume the responsibilities of high-risk AI system providers due to certain actions	must verify the conformity of the systems (have the appropriate conformity assessments been conducted), checking the Provider's technical documentation , and ensuring the necessary CE marking, EU declaration of conformity, and instructions for use are in place. Importers must also carefully manage the system to maintain compliance and take corrective actions , and cooperate fully with competent authorities by providing necessary information and documentation	must i.a. verify critical elements before making a high-risk AI system available, including the CE marking, EU declaration of conformity, instructions for use . Distributors have otherwise the same obligation as importers (column to the left).

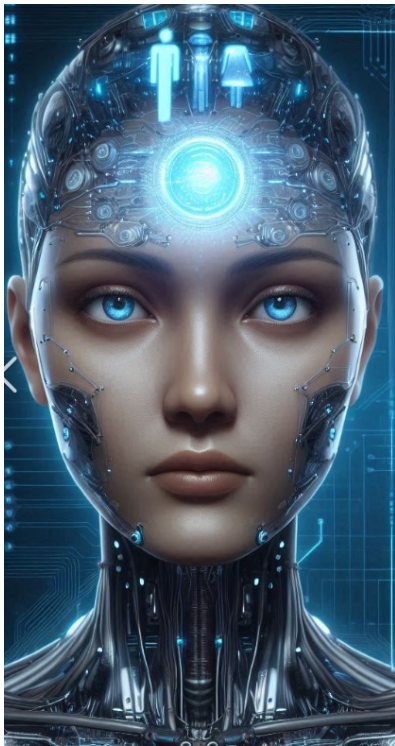
AI Act compliance for GPAI model provider

Requirements for so-called general purpose AI models



Transparency obligations for AI Systems

Which AI systems and who must adhere to specific transparency requirements?



- ✓ **Human-Interaction AI systems:** **Provider** of AI systems interacting with humans must clearly disclose they are AI, unless obvious to the user
- ✓ **Marking of AI-generated media:** **Provider** of AI systems that generate synthetic content must mark their outputs in a machine-readable format
- ✓ **Emotion recognition and biometric categorisation:** **Deployers** must inform users when they interact with these AI systems
- ✓ **Labelling of content containing deep fakes:** **Deployers** using AI to generate or manipulate content that resembles existing entities must disclose the content's artificial origin

Overview on Enforcement

What are the fines for non-compliance?

- Breaches of the **prohibitions**: fines of up to €35,000,000 EUR or up to 7% of worldwide annual turnover for the preceding year, whichever is higher.
- Breaches of **obligations for providers of high-risk systems and transparency obligations**: fines of up to €15,000,000 or up to 3% of worldwide annual turnover for the preceding year, whichever is higher.
- Supply of **incorrect, incomplete or misleading information** to authorities: fines of up to €7,500,000 or, up to 1% of worldwide annual turnover for the preceding year, whichever is higher.
- For **SMEs and start-ups**: the thresholds will be the lower figure mentioned above.
- N.B. The data protection authorities have been putting their hands up for regulating the AI Act (e.g. Dutch DPA, CNIL, German DPAs)- potentially GDPR style enforcement if the same regulators regulate the AI Act.

Key Takeaways

What are the mechanisms to help with AI Act compliance?

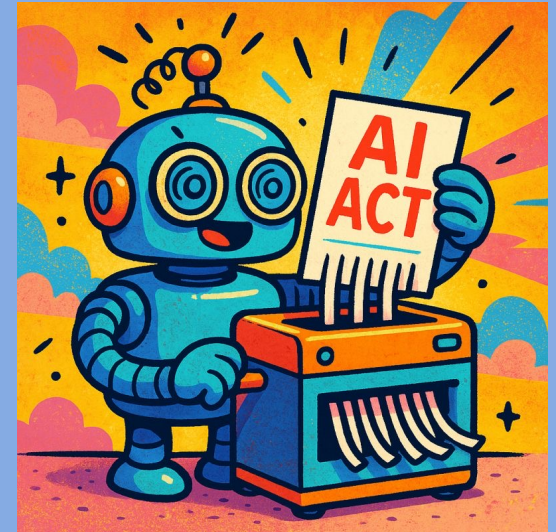
- AI Act applies **cross-sector** but only in a **targeted manner**
- AI Act compliance to be assessed **as early as possible**; **holistic AI compliance** required, including particularly DP and IP, amongst others (consider also that DP regulators are gearing up to enforce the AI Act – risk increase also under GDPR?)
- In terms of **stifling innovation**, the AI Act has several tools to allow taking actionable steps, which are work in progress, though:
 - **Standardisation:** Technical standards to establish presumption of conformity (CEN/CENELEC);
 - **Guidelines:** Commission guidelines to specify cross-sectoral AI Act (e.g. definition of high-risk and exemptions)
 - **AI regulatory sandboxing:** Testing innovative technologies in controlled frameworks and taking advantage of exemptions from administrative fines
 - **Regulatory oversight:** AI Office and local regulators; enforcement depends on equipment of regulators (which may support implementation)

Copyright obligations for providers of general-purpose AI systems



- Providers of a general-purpose AI model must:
 - have "*a policy to comply with Union copyright law*", including complying with opt-outs from the EU's commercial TDM exception using "state of the art technologies" - Recital (105) and Article 53(1)(c).
 - disclose details of the content used for training - Recital (107) and Article 53(1)(d).
 - "*for example by listing the main data collections or sets that went into training the model, such as large private or public databases or data archives, and by providing a narrative explanation about other data sources used*"
- The AI Office has released the code of practice explaining the level of detail required for training data disclosures on Thursday last week.
- No exception for open source general-purpose AI models - Recital (104).
- Providers fine-tuning general-purpose AI models need to disclose the new training data sources - Recital (109).

2. Panel discussion

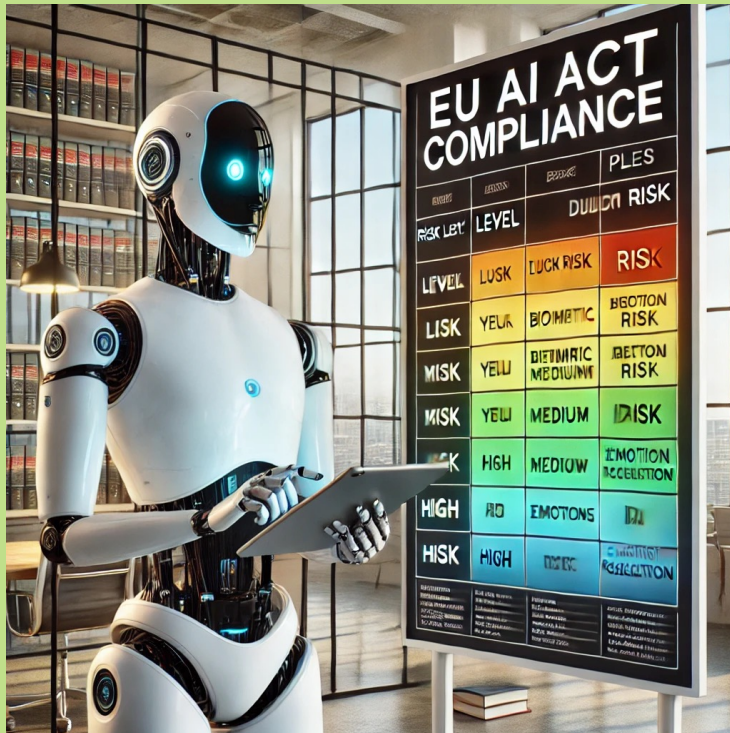




Theme 1

EU AI Act: Overall impact on the speakers and/or their organization

Audience Poll



Theme 2

Provider & Deployers: key factors in determining risk and the key obligations

Practical steps: Assessing the impact of the AI Act

6 steps towards AI Act compliance

1. AI system inventory

List the AI systems (as defined in the AI Act) that your business is using, developing, deploying, supplying, distributing and/or importing

2. Scope

Assess whether and how your business is in scope of the Act

3. Actor

Assess your business' role for each AI system in scope (provider, deployer etc)

4. Risk classification model

Classify the level of risk for each relevant AI system

5. Obligations

Identify which obligations in the Act you need to comply with

6. Ensure compliance

Ensure that your AI practices are compliant with the requirements of the Act



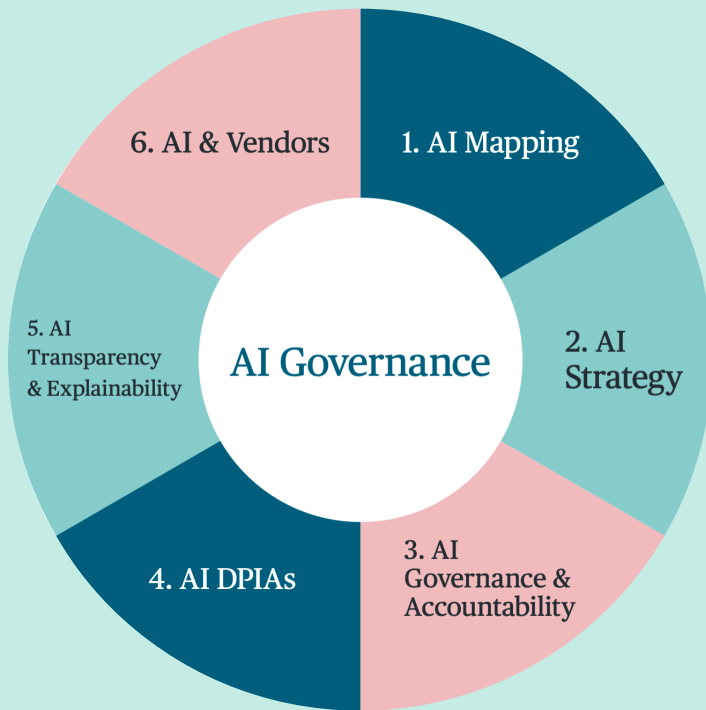
Theme 3

A few words about the enforcement by EU institutions and national regulators



Theme 4

Practical steps to reduce the risk of enforcement



Theme 6

Adopting an effective AI Governance framework

Audience Poll

AI Governance in practice



Taking Inventory: Map AI systems presently in use in all business functions, across both employee and client interactions.



Establish clear Policies and Guidelines: Establish organization's priorities and acceptable risk levels, create AI procurement policies, risk management policies, system decommissioning policies and policies for developing bespoke systems. Key point is to articulate ethical principles relevant to the company and making sure policies align.



Conduct Risk Assessments: Measure risk based on impact and likelihood, consider risk at different stages of the lifecycle and inter-system interactions, document the assessment adequately and identify mitigation strategies.



Implement, Monitor and Adapt: Implement risk mitigation strategies identified during the risk assessment, including human agency, regularly monitor how mitigation strategies are being implemented and whether risk mitigation is being achieved. If the identified risk factors has changed, increased or increased/decreased in likelihood, adapt mitigation strategies to meet new risk.



Assign Responsibilities: Consider creating AI Governance Committee, or a dedicated team overseeing policies and ethical concerns. Update traditional governance teams with professionals with expertise in AI-related regulatory, ethical and ops experience.



Ensure Transparency and Accountability: Maintain clear documentation of AI across its lifecycle, make sure to disclose presence of AI to end-user or interacting party, provide meaningful information about any decisions made by the model. Document data usage, quality, accuracy, reliability and representativeness.



Provide Training and Awareness: Educate employees about AI usage, ethical considerations and compliance requirements. Don't forget about Art. 4 AI Act. Make sure the training is relevant to the employees' role and responsibilities.



Theme 7

Interplay between the EU AI Act and other EU regulations

AI Act and GDPR

A friendly co-existence?

- **AI models and systems** can hardly avoid processing personal data (e.g. EDPB assumes that AI models qualify as personal data typically – NB: Impact on downstream provider of LLMs – see "AI Model Opinion" from December 2024)
- **Overlaps**-i.e. for these obligations, providers and deployers should ensure consistency in their compliance approach and documentation:
 - **Human Oversight:** Avoid the strict requirements of automated decision making under GDPR and meet human oversight requirements for high-risk AI systems under the AI Act
 - **Assessments:** Use synergies between AI Act's conformity assessments, fundamental rights impact assessments and DPIAs
 - **General principles:** Fairness, transparency and accountability upheld by both laws, which also overlap to a certain extent (e.g. avoidance of bias)

AI Act and GDPR

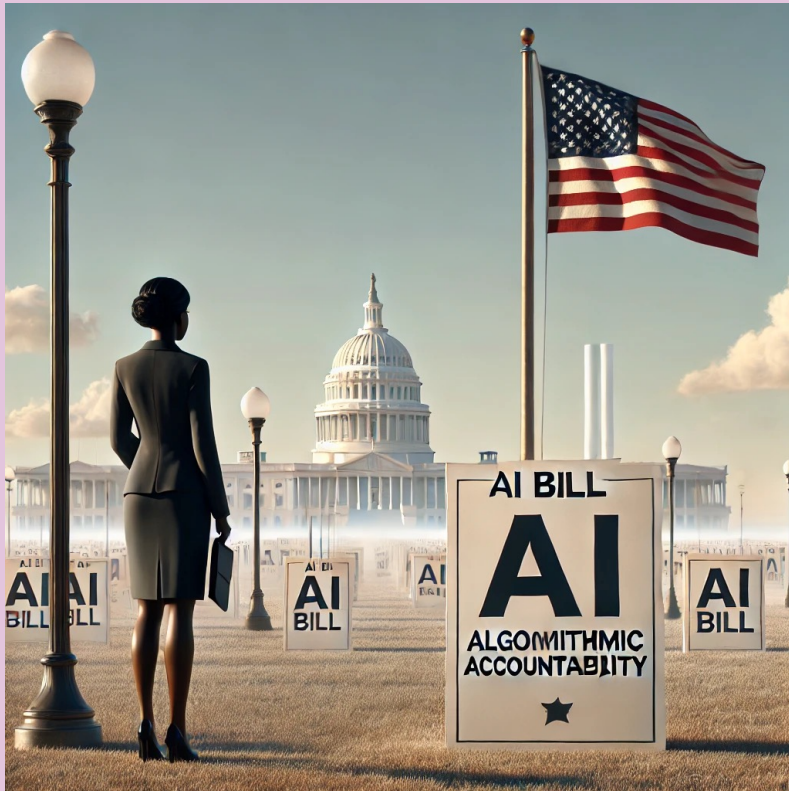
A friendly co-existence?

- **Tensions**-i.e. particular attention must be paid to the selection and processing of personal data:
 - **Data minimization** and **purpose limitation** vs **data governance** under the AI Act?
 - **Document** that the AI model is only trained with data to the extent that it is necessary for the purpose of the training and a specified purpose
- **Regulatory oversight:**
 - **Local regulators** to be appointed for high-risk, limited-risk and prohibited AI systems in most countries
 - Should this be policed by **data protection regulators**?
 - Regardless, **double enforcement** possible
 - **BUT:** Streamlining currently being discussed on EU level. Consensus seems to be that the two laws need to be interpreted and enforced coherently, and the respective authorities should cooperate closely and systematically

AI Act and GDPR

A friendly co-existence?

- If we discuss AI & GDPR compliance, the recent **EDPB report on privacy risks in LLMs** must be mentioned (issued April 2025)
- It provides **practical guidance** on privacy risk management, with concrete examples of risks and mitigations (e.g. chatbots)
- **A few highlights:**
 - Applying **privacy by design** is essential, which can be complex — and often borders on AI, security, and software engineering.
 - It offers the **FRASP framework**, which offers criteria to assess both the probability and severity of risks
 - It proposes a risk management process based on the **AI lifecycle**
 - It introduces **threat modeling** as a methodology that can be embedded into your risk management process



Theme 8

*Status of AI regulations in the US
(Danielle & Matt)*



Theme 9

AI Risk & Liability in commercial contracts



Q&A

Any question?

Use slido

Bird & Bird

Thank you!



Chris de Mauny

US Co-Head & IP Partner at Bird & Bird LLP

Chris.DeMauny@twobirds.com



Vincent Rezzouk-Hammachi

*US Co-Head & Global Head of Privacy Solutions
at Bird & Bird LLP*

Vincent.Rezzouk@twobirds.com



Maya Mancuso

*US Business Relationships Manager
at Bird & Bird LLP*

Maya.Mancuso@twobirds.com

Let's connect on **LinkedIn**



Let's connect on **LinkedIn**



Let's connect on **LinkedIn**

