

The European Union Artificial Intelligence Act

07/11/2024

The world is how we shape it*

sopra  steria

*Le monde est tel que nous le façonnons

Agenda

1. AI Act presentation: Key points
2. Use cases
3. Q&A

01

AI Act Presentation

01



One step further following numerous regulations governing data and digital services



RGPD :

Some similarities and complementarity, even if the purpose is different. GDPR compliance is for instance a prerequisite in a declaration of conformity for high-risk AI system and some approaches are comparable (e.g. in terms of transparency obligations)



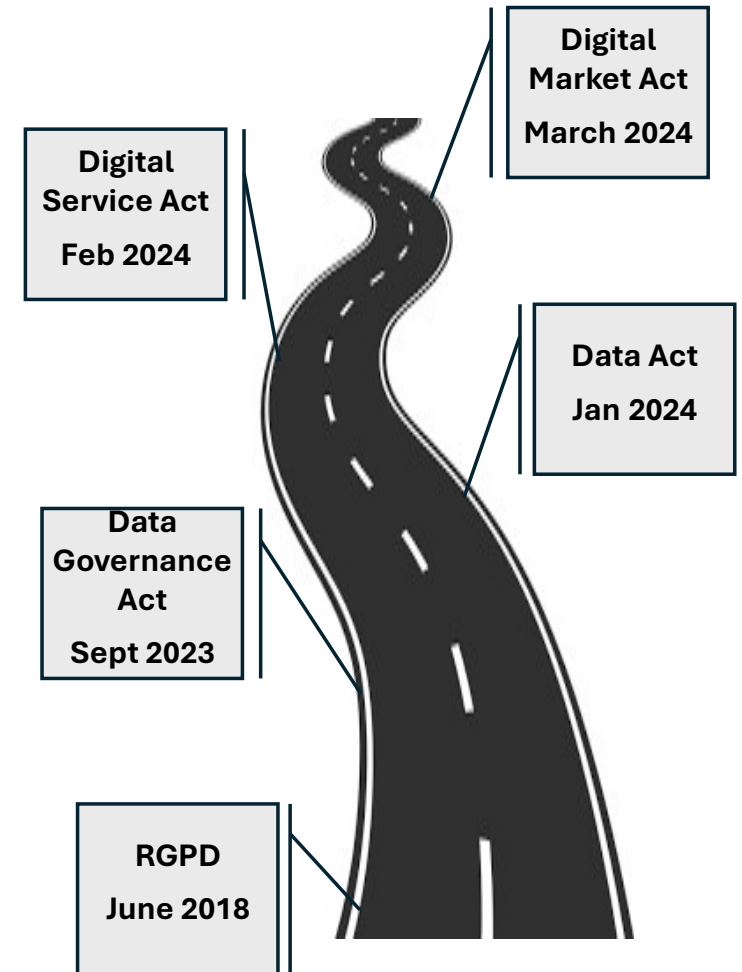
Digital Service Act :

It applies to online platforms and search engines for transparency reporting on their internal complaints handling systems and content moderation activities. But also to guarantee a high level of protection for the privacy, safety and security of minors.



Data act :

DA specifies who can create value from data, and under what conditions regulate data sharing between companies and consumers, and prohibit unfair data access terms



The banking sector is strongly impacted by this regulatory tightening

Digital transformation: a key regulatory challenge for the ECB

Priority 1: Strengthen resilience to immediate macro-financial and geopolitical shocks

Shortcomings in **credit risk** and **counterparty credit risk management frameworks**



Credit risk

Shortcomings in **asset and liability management frameworks**



Liquidity and funding risk; IRRBB

Priority 2: Accelerate the effective remediation of shortcomings in governance and the management of climate-related and environmental risks

Deficiencies in **management bodies' functioning** and steering capabilities



Governance

Deficiencies in **risk data aggregation and reporting**

Material exposures to **physical and transition risk drivers of climate change**



Climate-related and environmental risks

Further progress in digital transformation and building robust operational resilience frameworks

Deficiencies in **digital transformation strategies**




Business model

Deficiencies in **operational resilience frameworks**, namely IT outsourcing and IT security/cyber risks




Operational risk

ECB Banking Supervision: SSM supervisory priorities 2024 - 2026



DORA regulation aims to ensure the operational resilience of financial entities against digital risks. As financial services become increasingly dependent on information and communication technologies (ICT), DORA addresses the growing need to protect critical infrastructures from cyber threats and other disruptions.



On the other side, *Guidance on Loans origination and Monitoring* opened a thin way by allowing institutions and creditors to adopt methods which may include models, depending on the risk level, size and type of loan

Main objectives of the AI Act

The collage features three news articles: a Reuters article from October 2018 about Amazon scrapping a biased recruiting tool; a dark-themed article titled 'Predictive policing algorithms are racist. They need to be dismantled.' from July 2020; a BBC article from October 2020 about a UK passport photo checker showing bias against dark-skinned women; and a New York Times article from February 2018 titled 'Facial Recognition Is Accurate, if You're a White Guy'.

Protect EU citizens from the potential risks of AI

Prevent market fragmentation

Ensure legal certainty
And a single EU market

Facilitate investment and innovation in AI

What is the AI Act ?



EU regulation – directly applicable



Horizontal legislation (basis for sectoral ones)

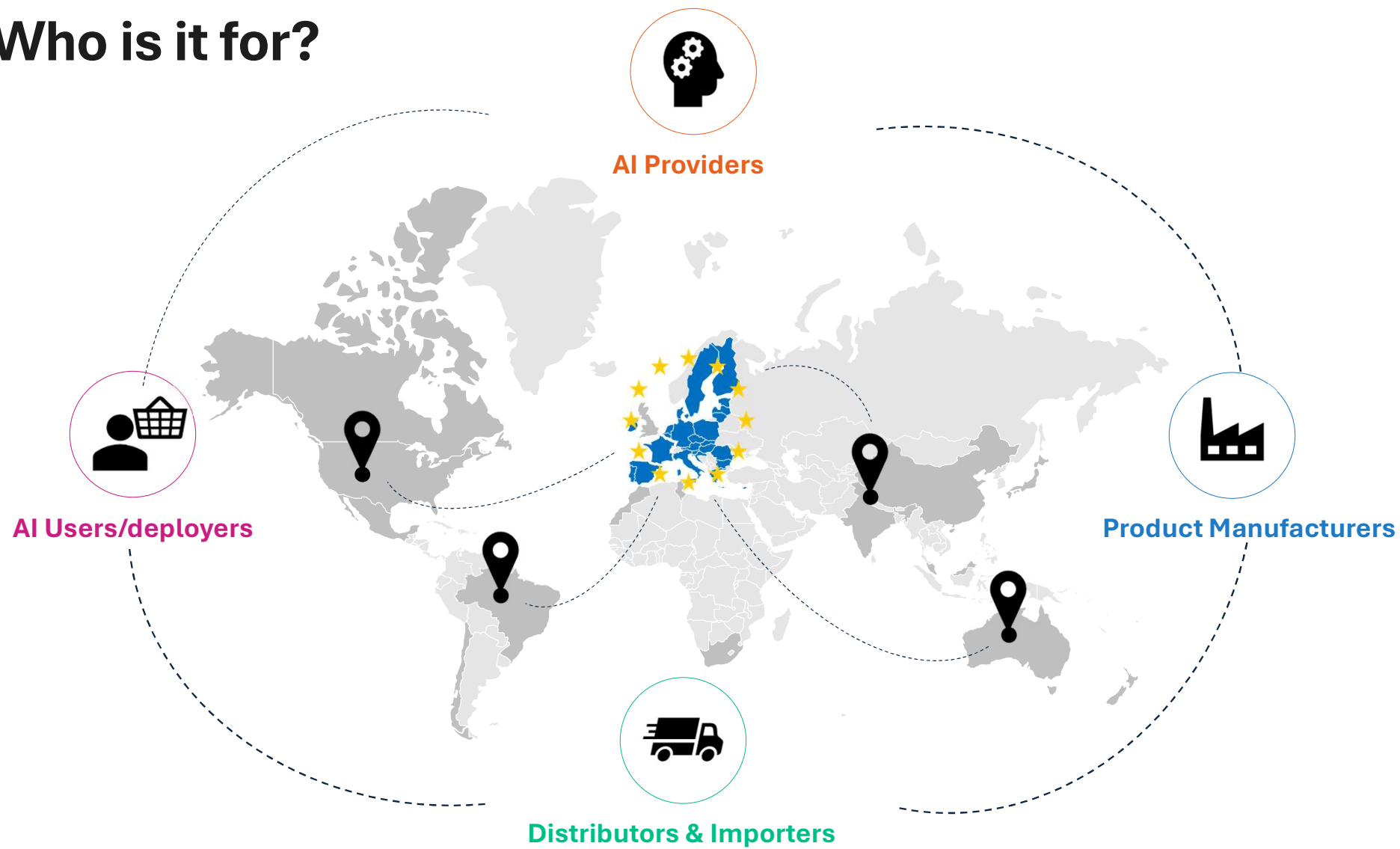


Regulating the use of AI systems not the technology



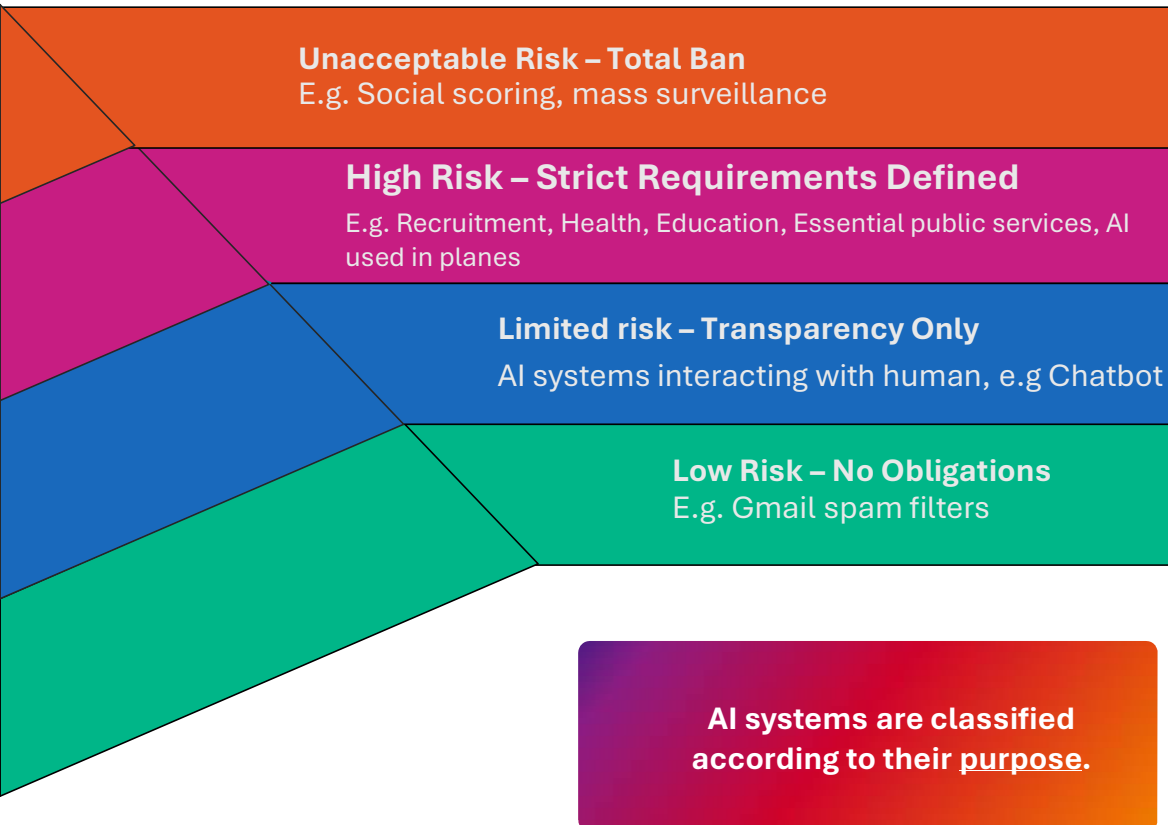
Exemptions: AI systems developed or used exclusively for military or national security purposes
R&D, AI systems released under free and open source licences (partial)

Who is it for?



A risk-based approach

*: General Purpose Artificial Intelligence



Generative AI: specificities under the AI Act:

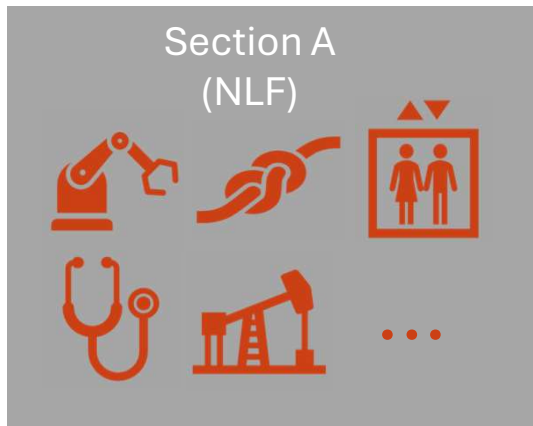


/! Risk levels and requirements are not mutually exclusive

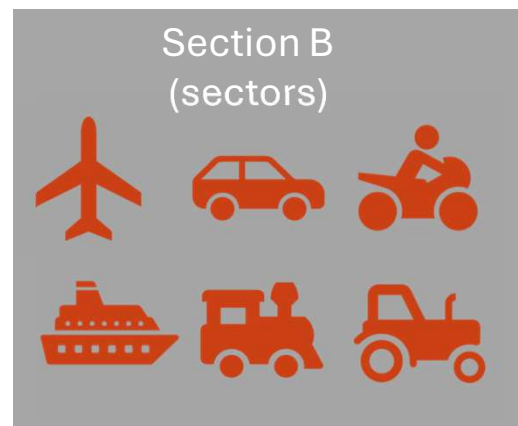
High-risk AI systems

Two categories of high-risk AI systems

AI systems intended to be used as a safety component in regulated framework (Annex I)



High-risk AI system requirements apply



Sector legislation applies
Implementation via delegated & implementing acts

AI systems operating in the areas listed in Annex III where fundamental rights issues arise



High-risk AI system requirements apply

Requirements and obligations for high-risk AI systems



Risk Management



Data Governance



Technical Documentation



Appropriate Level of Accuracy, Robustness and Cybersecurity



Automatic Event Recording



Transparency



Human Oversight



Additional obligations depending on the role in AI value chain

Underpinned by technical standards (CEN-CENELEC)

Meeting standards gives presumption of conformity

AI Act – Standardization Request

CEN-CENELEC JTC21

AI Act standardization request (SR) for horizontal harmonized standards (high-risk AI systems only):

1. **Risk management system** for AI systems (SR1)
2. Governance and quality of datasets used to build AI systems (SR2)
3. Record keeping – built-in logging capabilities in AI systems (SR3)
4. Transparency and information to the users of AI systems (SR4)
5. Human oversight of AI systems (SR5)
6. Accuracy specifications for AI systems (SR6)
7. Robustness specifications for AI systems (SR7)
8. Cybersecurity specifications for AI systems (SR8)
9. **Quality management system** for providers of AI system (SR9)
10. **Conformity assessment** for AI systems (SR10)

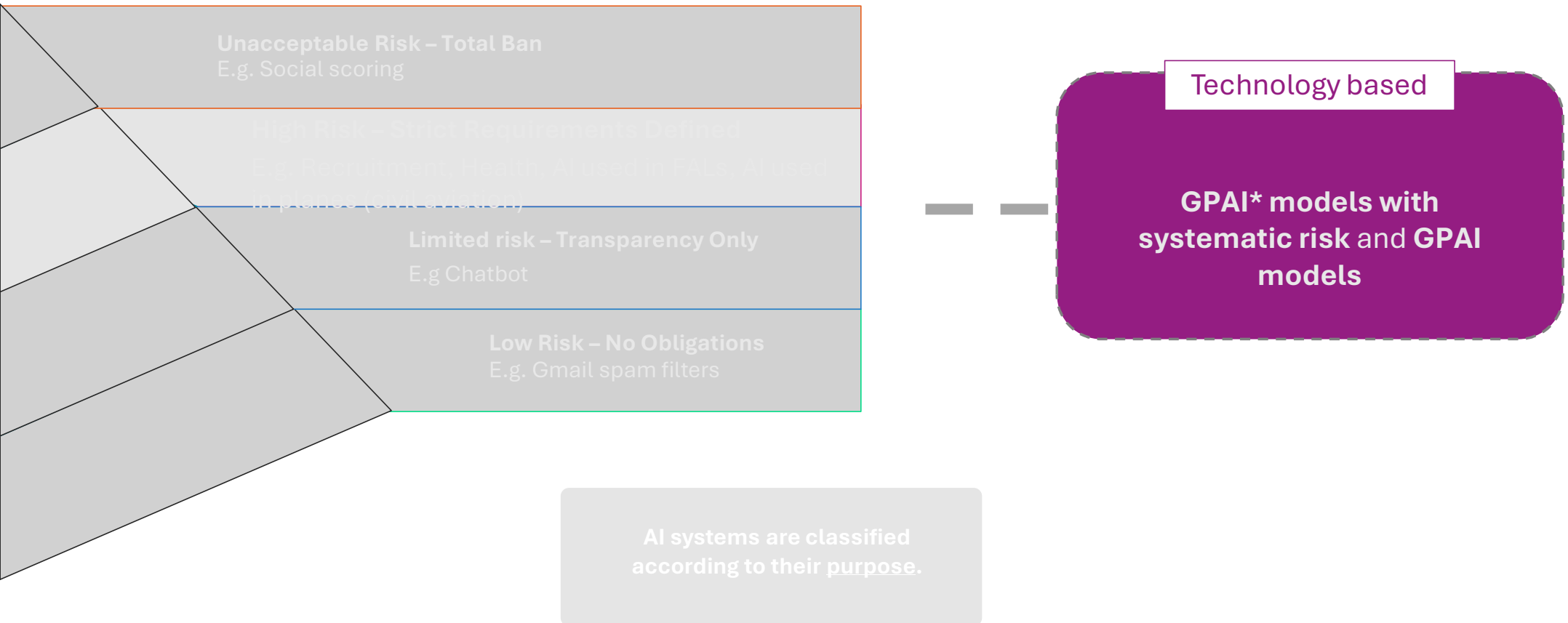


General Purpose AI:

Reliance on codes of practices until harmonised standards are developed

*: General Purpose Artificial Intelligence

Generative AI: specificities under the AI Act



For providers:

GPAI models

Technical documentation

Documentation of energy consumption

Info-sharing for future integration by deployers

Copyright provisions

Public summary of training data



GPAI models w/ systemic risks

Threshold:
high impact + FLOPS > 10^{25}

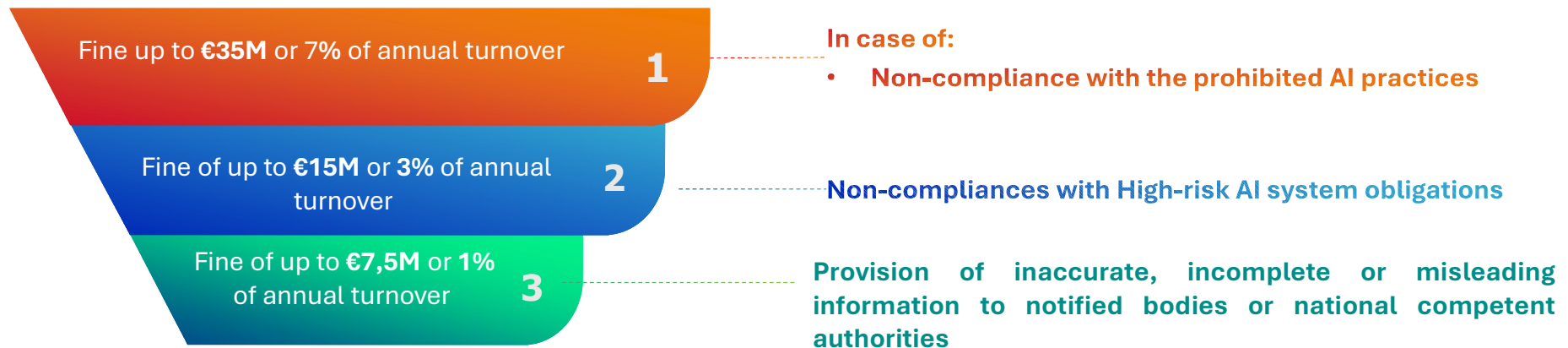
Model evaluation

Risk assessment and mitigation

Cybersecurity for model and physical infrastructure

Reliance on codes of practices until harmonised standards are developed

Sanctions under the AI Act



Supervision and enforcement

European Artificial Intelligence Office

European level

- Supporting the AI Act and enforcing general-purpose AI rules
- Contributing to the coherent application of the AI Act across the Member States
- Strengthening the development and use of trustworthy AI
- Fostering international cooperation and governance on AI
- Collaboration with a diverse range of institutions, experts and stakeholders

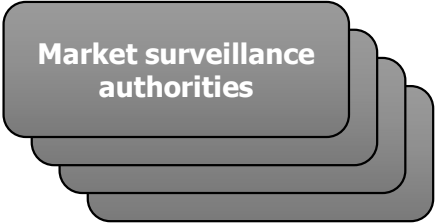
06



National competent authorities and single points of contact



“Setting up and carrying out the necessary procedures for the assessment, designation and notification of conformity assessment bodies and for their monitoring”



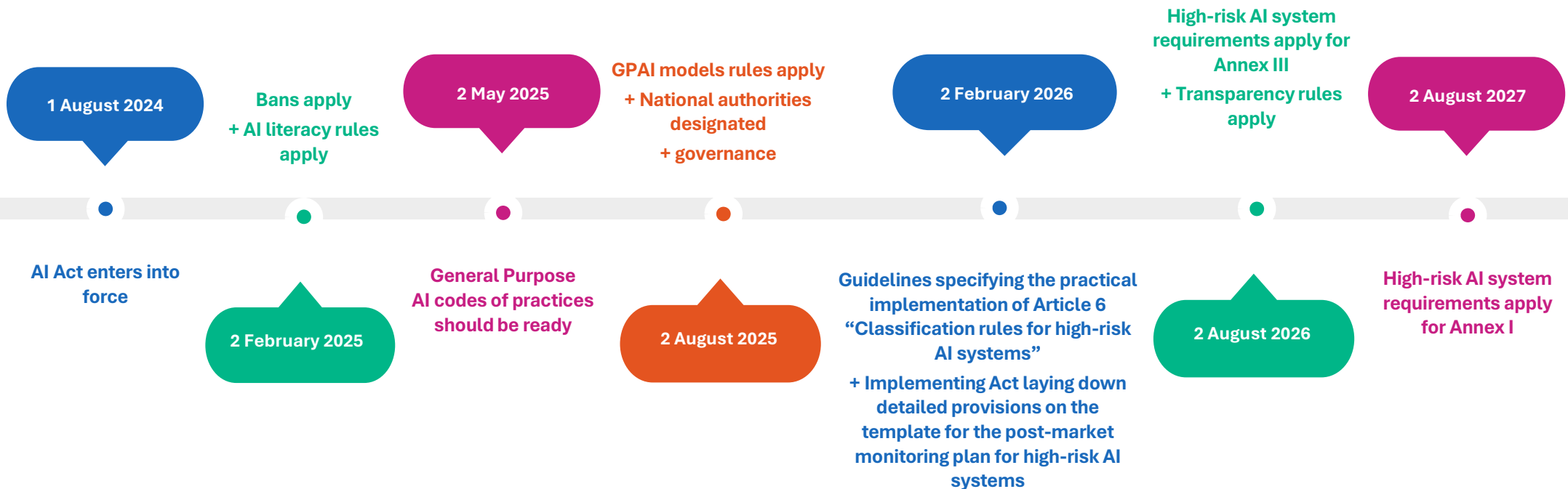
“Authority carrying out the activities and taking the measures pursuant to Regulation ”



Member States shall designate a market surveillance authority to act as the single point of contact for this Regulation, and shall notify the Commission of the identity of the single point of contact

AI Act Implementation Timeline

As of **early 2025**, then **gradual application**



AI Act – Retroactive application?

AI systems in scope already on the market or into service before date of application

If substantial modification

Compliance w/ high-risk requirements

GPAI models already on the market before date of application of GPAI rules

Compliance w/ GPAI provisions by mid-2027



High-risk AI systems **already used** by **public authorities** must be compliant by **mid-2030**

The European Commission

SHALL also provide guidelines on the practical implementation of:

- The definition of an AI system
- The requirements for high-risk AI systems
- The prohibited practices
- The provisions related to substantial modification
- The transparency obligations
- The relationship of the AI Act with the other EU harmonisation legislation listed in Annex I

CAN adopt delegated acts relating to:

- The classification rules for high-risk AI systems
- To amend the high-risk AI systems list in Annex III
- To amend Annex IV related to the technical documentation requirement for high-risk AI systems
- The conformity assessment for high-risk AI systems and the EU declaration of conformity
- To amend the to amend the articles linked to the classification of GPAI models as GPAI models with systemic risk

02

Use cases



02



Use case 1

You are using a third-party AI system to assess a natural person's creditworthiness



- The AI Act applies to you
 - Your role : **Deployer**
 - **High-risk AI system**

Use case 1 – What needs to be done:



Use case 2

You are using, for internal purposes, a conversational assistant provided by a third party, for PDF documents (providing summaries, translations, and answering to questions, etc.)



- The AI Act applies to you
 - Your role : **deployers**
- **A limited-risk AI system based on a General Purpose Model = a limited-risk GPAI system**

Use case 2 – What needs to be done:

- No requirement linked to the use of the GPAI model under the AI Act
- Regarding the use of the GPAI system => Disclose that content is artificially generated or manipulated
- Nevertheless, the AI Act does not replace other regulations (i.e.: GDPR) and company internal codes of practice (i.e.: data confidentiality)

03

Q&A

Thank you for your attention

bruno.maillot@soprasterianext.com
vincent.lefevre@soprasterianext.com

The world is how we shape it*

sopra  steria

*Le monde est tel que nous le façonnons