Article

AI Act: Decoding the new dawn in artificial intelligence regulation

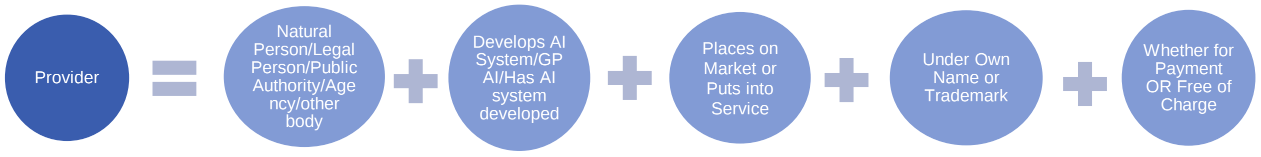
The implementation of the AI Act heralds a new era in the regulation of artificial intelligence (***AI***). This article serves as a comprehensive guide to understanding its impact, focussing on the scope of its application, prohibited AI practices, key enforcement considerations, and its institutional setting. Delving into the intricacies of the Act, in this article, we provide an overview of the boundaries of permissible AI innovation to help organisations navigate the new regulatory landscape effectively.

Brief overview

- The AI Act sets a common framework for the use and supply of AI systems in the EU, making it the first binding worldwide horizontal regulation on AI.
- The AI Act aims to ensure that AI systems used in the EU are safe, transparent, traceable, non-discriminatory, and environmentally friendly. Oversight by humans is emphasised to prevent harmful outcomes, and obligations for providers and users are established based on the level of risk posed by AI systems.
- It offers a classification for AI systems with different requirements and obligations tailored to a 'risk-based approach'. AI systems presenting 'unacceptable' risks are prohibited[1], while 'high-risk' AI systems are subject to requirements to access the EU market, including conformity assessment before deployment.
- Specific rules are provided for General Purpose AI (***GPAI***) models, with more stringent requirements for GPAI models with 'high-impact capabilities' that could pose systemic risks.
- The Act establishes a governance structure at both European and national levels to oversee AI deployment and ensure compliance with regulations.

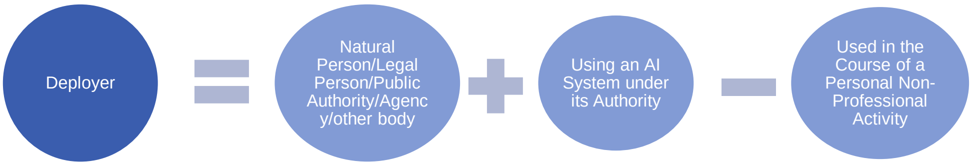
Roles

'**Provider**' means 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.

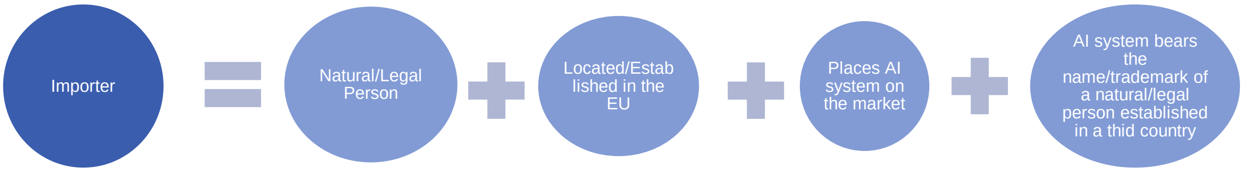

Provider
=
Natural Person/Legal Person/Public Authority/Agency/other body
+
Develops AI System/GPAI/Has AI system developed
+
Places on Market or Puts into Service
+
Under Own Name or Trademark
+
Whether for Payment OR Free of Charge

[1] Exemptions exist for uses related to military, defence, national security, scientific research, personal non-professional activities, and open-source AI, among others (see exemptions listed under the 'Scope' section below).

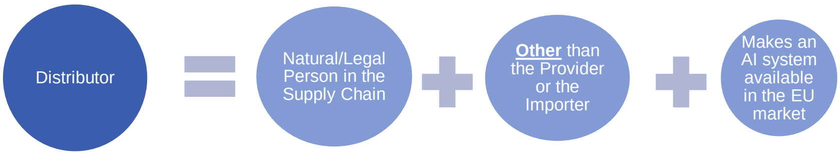
‘**Deployer**’ means a natural or legal person, public authority, agency or other body using an AI system under its authority except where the AI system is used in the course of a personal non-professional activity.


Deployer
=
Natural Person/Legal Person/Public Authority/Agency/other body
+
Using an AI System under its Authority
−
Used in the Course of a Personal Non-Professional Activity

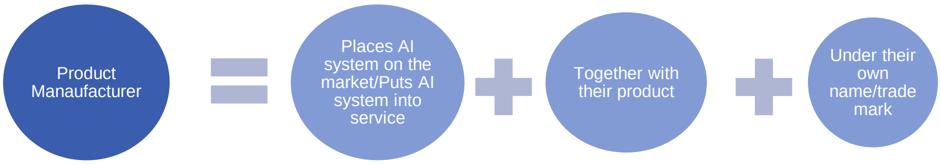
‘**Importer**’ means a natural or legal person located or established in the European Union (the ***Union***) that places on the market an AI system that bears the name or trademark of a natural or legal person established in a third country.


Importer
=
Natural/Legal Person
+
Located/Established in the EU
+
Places AI system on the market
+
AI system bears the name/trademark of a natural/legal person established in a thid country

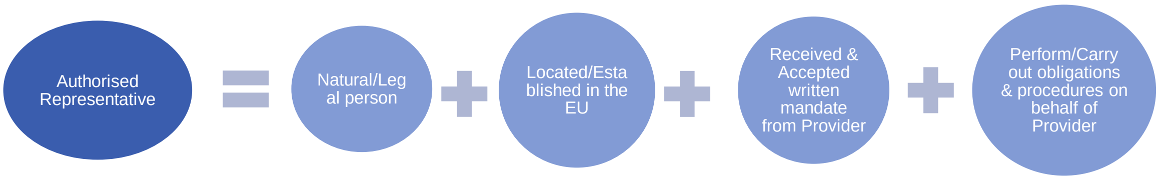
‘**Distributor’** means a natural or legal person in the supply chain, other than the provider or the importer, that makes an AI system available on the Union market.


Distributor
=
Natural/Legal Person in the Supply Chain
+
Other than the Provider or the Importer
+
Makes an AI system available in the EU market

‘**Product Manufacturer**’ means a manufacturer placing on the market or putting into service an AI system together with their product and under their own name or trademark.


Product Manaufacturer
=
Places AI system on the market/Puts AI system into service
+
Together with their product
+
Under their own name/trademark

‘**Authorised Representative**’ means a natural or legal person located or established in the Union who has received and accepted a written mandate from a provider of an AI system or a general-purpose AI model to, respectively, perform and carry out on its behalf the obligations and procedures established by this Regulation.


Authorised Representative
=
Natural/Legal person
+
Located/Established in the EU
+
Received & Accepted written mandate from Provider
+
Perform/Carry out obligations & procedures on behalf of Provider

‘**Operator**’ means a provider, product manufacturer, deployer, authorised representative, importer or distributor.

Scope

Understanding the scope of the AI Act and its application across different entities and scenarios.

The AI Act applies to:

- **Providers** placing on the market or putting into service AI systems or placing on the market GPAI models in the EU, irrespective of whether those providers are established or located within the EU;
- **Deployers** of AI systems that have their place of establishment or are located within the EU;
- **Providers and Deployers** of AI systems that have their place of establishment or are located in a third country, where the **output** produced by the AI system is used in the EU;
- **Product manufacturers** placing on the market or putting into service an AI system together with their product and under their own name or trademark;
- **Importers and Distributors** of AI systems;
- **Authorised representatives of providers**, which are not established in the EU; and
- **Affected persons** that are located in the EU.

Please refer to the decoded scope for providers, deployers, and product manufacturers in **Annex 1** below.

Exemptions

- **National security**: The regulation does not apply to AI systems used exclusively for military, defence, or national security purposes, whether inside or outside the EU.
- **International cooperation**: AI systems used by third-country public authorities or international organisations collaborating with the EU are exempt, provided they ensure fundamental rights protection.
- **Scientific research**: AI systems developed solely for scientific research purposes are exempt.
- **Exemption for pre-market activities**: Research, testing, or development of AI systems before market release are exempt, subject to applicable laws.
- **Personal use exclusion**: Individuals using AI systems for personal, non-professional purposes are exempt.
- **Open-source license exclusion**: AI systems under free and open-source licenses are exempt unless they meet specific criteria.
- This regulation does not affect laws regarding:
    - **Intermediary service provider liability**: The regulation does not affect laws regarding intermediary service provider liability.
    - **Data protection laws**: EU laws on data protection and privacy apply.
    - **Consumer protection and product safety**: Other EU laws on consumer protection and product safety still apply.
    - **Workers' rights protection**: Member States can enforce laws more protective of workers' rights regarding AI system use.

A risk-based approach

The AI Act introduces a comprehensive risk-based approach to AI regulation, categorising AI systems into four main categories based on their potential impact and level of risk:

1 **Unacceptable risk:** AI systems violating EU fundamental rights and societal values, like those involved in cognitive behavioural manipulation, social scoring, or real-time biometric identification, are prohibited, except where exemptions apply as noted above.

2 **High risk:** Systems posing significant risks to safety or fundamental rights, such as those used in critical infrastructure management, legal interpretation, or law enforcement, must undergo rigorous conformity assessment and post-market monitoring.

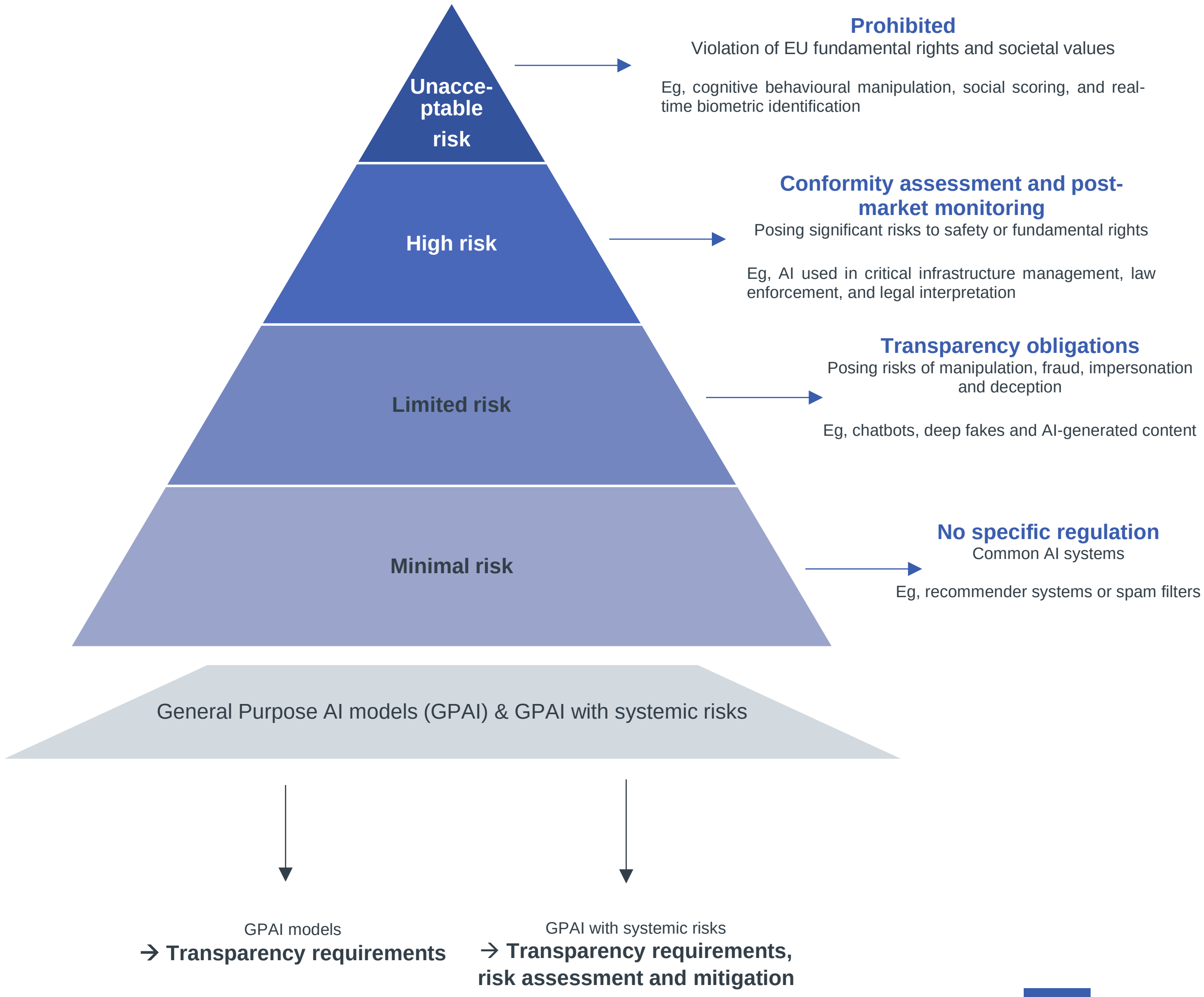
3 **Limited risk:** AI systems which pose risks of misinformation and manipulation, fraud, impersonation, and consumer deception, like chatbots, deep fakes and fakes and AI systems which generate or manipulate image, audio, or video content, are subject to transparency obligations.

4 **Minimal risk:** The majority of AI systems fall into this category, like recommender systems or spam filters, exempting them from specific obligations, though voluntary commitment to additional codes of conduct is permitted.

Specific Rules for GPAI: General Purpose AI (***GPAI***) models have specific regulations, with more stringent requirements for models with 'high-impact capabilities' that could pose systemic risks. A few examples of the most impactful GPAI models include GPT-3, GPT-4, AlphaStar, Chinchilla, Codex, DALL•E 2, Gopher, MuZero, PaLM and Wu Dao 2.0.

For a detailed guide on navigating the risk-based classification, please refer to the Pyramid of Risk below.

The Pyramid of Risk



Unacce-ptable risk

Prohibited
Violation of EU fundamental rights and societal values

Eg, cognitive behavioural manipulation, social scoring, and real-time biometric identification

High risk

Conformity assessment and post-market monitoring
Posing significant risks to safety or fundamental rights

Eg, AI used in critical infrastructure management, law enforcement, and legal interpretation

Limited risk

Transparency obligations
Posing risks of manipulation, fraud, impersonation and deception

Eg, chatbots, deep fakes and AI-generated content

Minimal risk

No specific regulation
Common AI systems

Eg, recommender systems or spam filters

General Purpose AI models (GPAI) & GPAI with systemic risks

GPAI models
→ **Transparency requirements**

GPAI with systemic risks
→ **Transparency requirements, risk assessment and mitigation**

Which AI practices are prohibited?

The AI Act prohibits the following AI practices that pose unacceptable risks:

- Placing on the market, putting into service, or using AI systems employing subliminal techniques or purposefully manipulative or deceptive techniques to materially distort behaviour, causing significant harm to individuals' decision-making abilities.

- Employing AI systems exploiting vulnerabilities of individuals due to age, disability, or specific social or economic situations to materially distort behaviour, causing significant harm.

- Using AI systems for social behaviour evaluation or classification based on sensitive characteristics, leading to unjustified or disproportionate treatment of individuals or groups.

- Employing AI systems for risk assessments of individuals regarding criminal offenses based solely on profiling or personality traits, excluding those supporting human assessment based on objective and verifiable facts.

- Creating or expanding facial recognition databases through untargeted scraping of facial images.

- Inferring emotions of individuals in workplace and education institutions, except for medical or safety reasons.

- Utilising biometric categorisation systems to infer sensitive personal characteristics.

- Employing 'real-time' remote biometric identification systems in publicly accessible spaces for law enforcement purposes, unless strictly necessary for specific objectives like search for missing persons or prevention of imminent threats, subject to strict safeguards and prior authorisation.

Enforcement and institutional setting

The implementation of the AI Act will be overseen by national authorities, supported by the AI Office within the European Commission. Member states have 12 months to nominate oversight agencies responsible for enforcing the regulations.

This responsibility extends to establishing or designating at least one market surveillance authority and at least one notifying authority to ensure the application and implementation of the act. Non-compliant entities will face heavy fines. Additionally, the implementation will be supported by various EU level actors, including the European Commission, the AI Board, the AI Office, the EU standardisation bodies (CEN and CENELEC) and an advisory forum and scientific panel of independent experts. Further details on the key national and EU-level actors are outlined below.

EU Level

The AI Office: The AI Office was established to be the centre of AI expertise and to provide advice on the implementation of the new rules, in particular as regards GPAI models and to develop codes of practice to support the proper application of the AI act. The AI Office is tasked with several actions, including:

- Providing standardised templates, as requested by the AI Board, for areas covered by the AI Act;
- Developing and maintaining a single information platform to offer accessible information about the AI Act for all operators across the EU;
- Organising communication campaigns to increase awareness about the obligations arising from the AI Act; and
- Evaluating and promoting the convergence of best practices in public procurement procedures related to AI systems.

The AI Board:

- The AI Board will be advising and assisting the European Commission and the Member States in order to facilitate the consistent and effective application of the Regulation.
- The AI Board will be composed of one representative per Member State, with the European Data Protection Supervisor participating as an observer. The AI Office will also attend meetings without taking part in the votes.
- Other national and EU authorities, bodies, or experts may be invited to meetings by the AI Board on a case-by-case

basis, where the issues discussed will be of relevance to them.

- Each representative will be designated by their Member State for a period of three years, renewable once.

Member State Level

Notifying authorities: Each Member State shall designate or establish at least one notifying authority responsible for setting up and carrying out the necessary procedures for the assessment, designation and notification of conformity assessment bodies and for their monitoring.

Market surveillance authorities:

- Each Member State must establish or designate at least one national competent authority as a market surveillance authority, which will be responsible with overseeing the compliance of AI systems and ensuring that appropriate restrictive measures are taken in respect of the product or the AI system concerned, such as withdrawal of the product or the AI system from their market, without undue delay.
- The market surveillance authorities also have reporting obligations, including annual reports to the European Commission and relevant national competition authorities regarding information discovered during market surveillance activities that may be relevant for the application of Union competition rules.
- They must also annually report to the Commission on any prohibited practices used during the year and the measures taken to address them.

Timeline

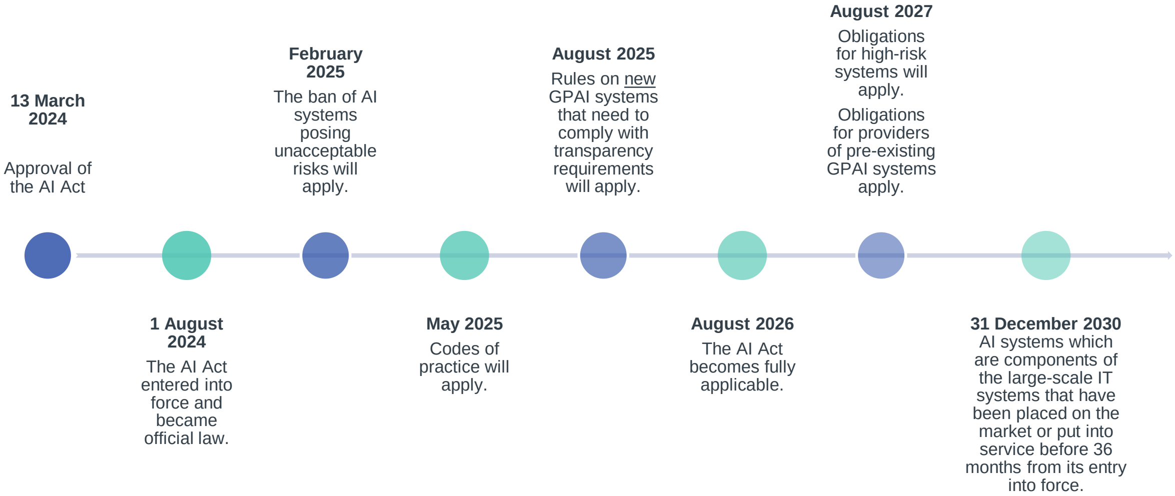
On 21 May 2024, the Council of the EU adopted the AI Act, which entered into force on 1 August 2024, 20 days after its publication in the Official Journal of the EU, marking a significant milestone in AI governance. The approved text of the AI Act will become fully enforceable 24 months after its entry into force, with certain aspects taking effect earlier or later:

Earlier

- The prohibition of AI systems posing unacceptable risks will be enforced six months after its entry into force.
- Codes of practice will come into effect 9 months after its entry into force.
- Rule on new general-purpose AI systems, which must adhere to transparency requirements, will be implemented 12 months after its entry into force.

Later

- High-risk systems will be granted additional time to ensure compliance, with their obligations becoming enforceable 36 months after its entry into force.
- Providers of GPAI models that have been placed on the market before 12 months from the date of AI Act’s entry into force shall be brought into compliance by 36 months from the date of the AI Act’s entry into force.
- AI systems which are components of the large-scale IT systems established by the legal acts listed in Annex X of the AI Act that have been placed on the market or put into service before 36 months its entry into force shall be brought into compliance by 31 December 2030.



13 March 2024

Approval of the AI Act

1 August 2024

The AI Act entered into force and became official law.

February 2025

The ban of AI systems posing unacceptable risks will apply.

May 2025

Codes of practice will apply.

August 2025

Rules on new GPAI systems that need to comply with transparency requirements will apply.

August 2026

The AI Act becomes fully applicable.

August 2027

Obligations for high-risk systems will apply.

Obligations for providers of pre-existing GPAI systems apply.

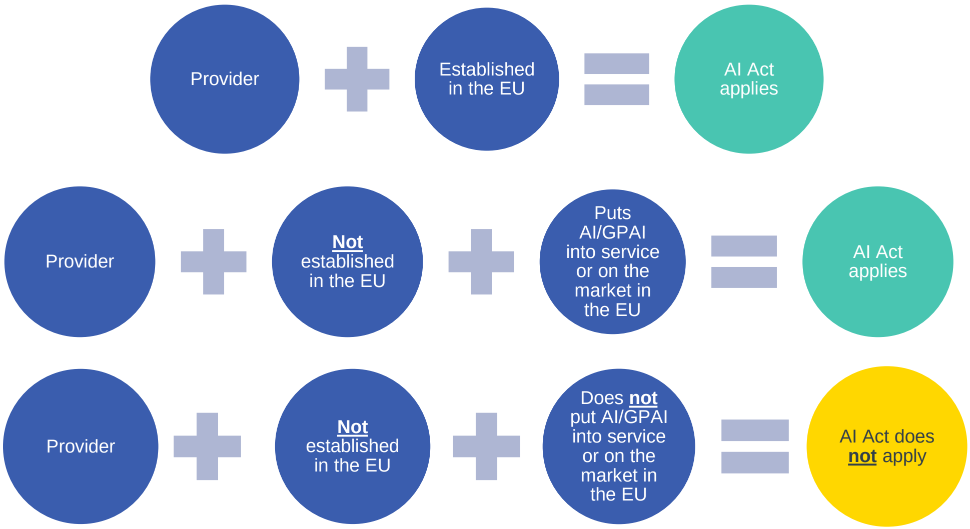
31 December 2030

AI systems which are components of the large-scale IT systems that have been placed on the market or put into service before 36 months from its entry into force.

If you or your business is impacted by the AI Act and require more guidance, please contact the authors or your usual Harneys contact to discuss further.

Annex 1 – Scope of AI Act

Provider

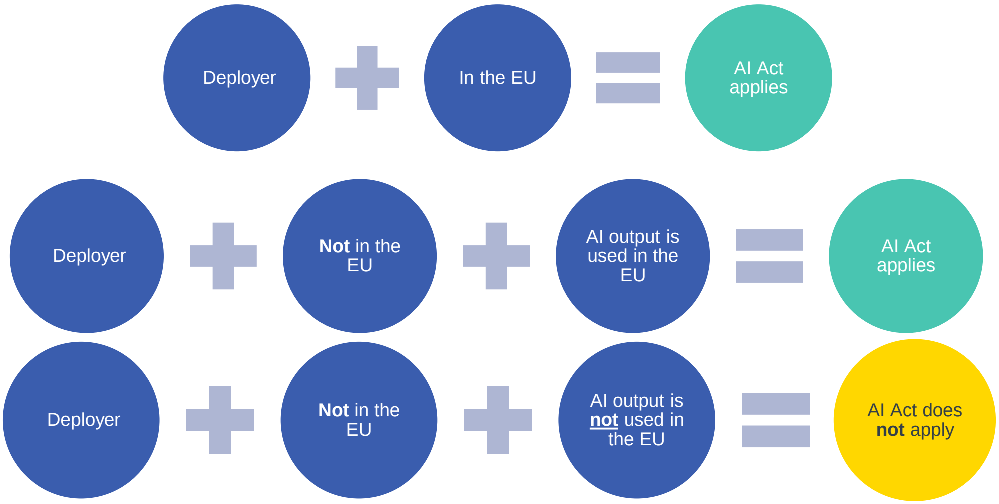


Provider + Established in the EU = AI Act applies

Provider + **Not** established in the EU + Puts AI/GPAI into service or on the market in the EU = AI Act applies

Provider + **Not** established in the EU + Does **not** put AI/GPAI into service or on the market in the EU = AI Act does **not** apply

Deployer

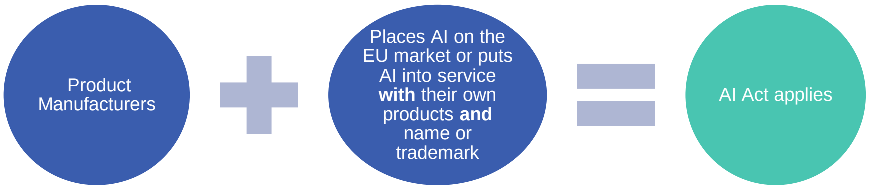


Deployer + In the EU = AI Act applies

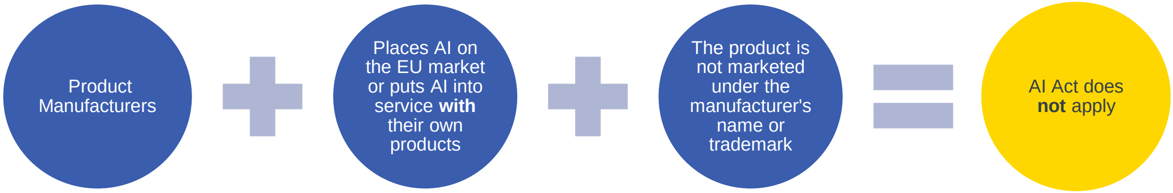
Deployer + **Not** in the EU + AI output is used in the EU = AI Act applies

Deployer + **Not** in the EU + AI output is **not** used in the EU = AI Act does **not** apply

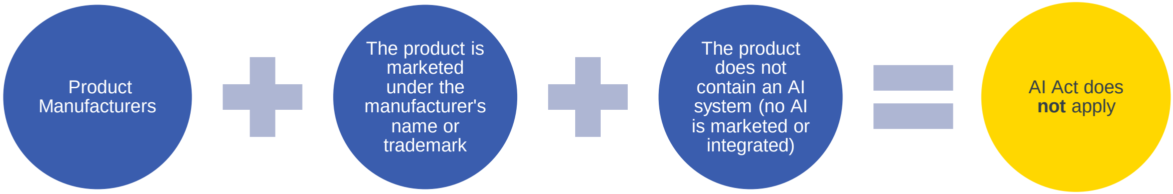
Product Manufacturer



Product Manufacturers + Places AI on the EU market or puts AI into service **with** their own products **and** name or trademark = AI Act applies



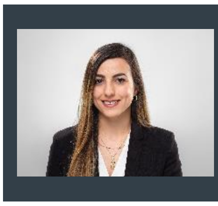
Product Manufacturers + Places AI on the EU market or puts AI into service **with** their own products + The product is not marketed under the manufacturer's name or trademark = AI Act does **not** apply



Product Manufacturers + The product is marketed under the manufacturer's name or trademark + The product does not contain an AI system (no AI is marketed or integrated) = AI Act does **not** apply

Authors

Juan Pablo Urrutia
Partner | Cayman Islands
Funds & Regulatory
+1 345 949 8599
juanpablo.urrutia@harneys.com



Marilena Papachristodoulou
Associate | Cyprus
Banking & Corporate
+357 96 101091
marilena.papachristodoulou@harneys.com

Harneys is a leading international offshore law firm. From locations around the globe, Harneys advises the world’s top law firms, financial institutions and corporations on the laws of British Virgin Islands, Cayman Islands, Cyprus, Luxembourg, Bermuda, Anguilla, and Jersey. Jersey legal services are provided through a referral arrangement with Harneys (Jersey) which is an independently owned and controlled Jersey law firm. For more information about Harneys please visit harneys.com or contact us at marketing@harneys.com.

The foregoing is for general information only and not intended to be relied upon for legal advice in any specific or individual situation.