

# Europees wetsvoorstel AI

AI Kennissessie CoE-DSC/VNO 18  
juni 2024



**Table 1: Overview of EU Legislations in the Digital Sector**

												Applicable law	Published in the Official Journal of the European Union
												In regulation	Proposal by the European Commission entered the legislative process.
												Planned initiative	Mentioned by the European Commission as potential legislative initiative
Research & Innovation	Industrial Policy	Connectivity	Data & Privacy	IPR	Cybersecurity	Law Enforcement	Trust & Safety	E-commerce & Consumer Protection	Competition	Media	Finance		
Digital Europe Programme Regulation, (EU) 2021/694	Recovery and Resilience Facility Regulation, (EU) 2021/241	Frequency Bands Directive, (EEC) 1987/7372	European Statistics, (EC) 2009/223, 2023/0287(COD)	Database Directive, (EC) 1996/9	Regulation for a Cybersecurity Act, (EU) 2019/831, 2023/0103(COD)	Law Enforcement Directive, (EU) 2016/680	Product Liability Directive (PLD), (EEC) 1985/374, 2022/0392(COD)	Unfair Contract Terms Directive (UCTD), (EC) 1993/13	EC Merger regulation, (EC) 2004/258, update_500n	Satellite and Cable I Directives, (EEC) 1993/83	Common VAT system, (EC) 2006/112, 2022/0407(CNS)		
Horizon Europe Regulation, (EU) 2021/695, (EU) 2021/764	InvestEU Programme Regulation, (EU) 2021/623	Radio Spectrum Decision, (EC) 2002/676	General Data Protection Regulation (GDPR), (EU) 2016/679	Community Design Directive, (EC) 2002/6, 2022/0391(COD)	Regulation to establish a European Cybersecurity Competence Centre, (EU) 2021/887	Directive on combating fraud and counterfeiting of non-cash means of payment, (EU) 2019/713	Toys Regulation, (EC) 2009/48, 2023/0290(COD)	Price Indication Directive, (EC) 1999/6	Technology Transfer Block Exemption, (EC) 2014/316	Information Society Directive, (EC) 2001/29	Administrative cooperation in the field of taxation, (EU) 2011/16		
Regulation on a pilot regime distributed ledger tech. market, (EU) 2022/888	Connecting Europe Facility Regulation, (EU) 2021/1163	Broadband Cost Reduction Directive, (EU) 2014/611, 2023/0046(COD)	Regulation to protect personal data processed by EU institutions, bodies, offices and agencies, (EU) 2018/1726	Enforcement Directive (IPR), (EC) 2004/48	NIS 2 Directive, (EU) 2022/2558	Regulation on interoperability between EU information systems in the field of borders and visas, (EU) 2019/817	European Standardization Regulation, (EU) 2019/1026	E-commerce Directive, (EC) 2000/31	Company Law Directive, (EU) 2017/1132, 2023/0089(COD)	Audio-visual Media Services Directive (AVMSD), (EU) 2010/13	Payment Service Directive 2 (PSD2), (EU) 2015/2366, 2023/0209(COD)		
	Regulation on High Performance Computing Joint Undertaking, (EU) 2016/1173	Open Internet Access Regulation, (EU) 2015/2120	Regulation on the free flow of non-personal data, (EU) 2018/1807	Directive on the protection of trade secrets, (EU) 2016/943	Information Security Regulation, 2022/0083(COD)	Regulation on terrorist content online, (EU) 2021/784	eIDAS Regulation, (EU) 2014/910, 2021/0136(COD)	Unfair Commercial Practices Directive (UCPD), (EC) 2005/29	Market Surveillance Regulation, (EU) 2019/1020	Portability Regulation, (EU) 2017/1328	Digital Operational Resilience Act (DORA Regulation), (EU) 2023/2654		
	Regulation on Joint Undertakings under Horizon Europe, (EU) 2021/2086, 2022/0023(INLE)	European Electronic Communications Code Directive (EECC), (EU) 2018/1972	Open Data Directive (PSI), (EU) 2019/1024	Design Directive, 2022/0393(COD)	Cybersecurity Regulation, 2022/0086(COD)	Temporary CSAM Regulation, (EU) 2021/1222, 2022/0166(COD)	Radio Equipment Directive (RED), (EU) 2014/53	Directive on Consumer Rights (CRD), (EU) 2011/83, 2022/0117(COD)	PSB Regulation, (EU) 2019/1169	Satellite and Cable II Directive, (EU) 2019/789	Crypto-assets Regulation (MICA), (EU) 2023/1114		
	Decision on a path to the Digital Decade, (EU) 2022/2481	eu-top-level domain Regulation, (EU) 2019/617	Data Governance Act (DGA Regulation), (EU) 2022/868	Compulsory licensing of patents, 2023/0129(COD)	Cyber Resilience Act, 2022/0273(COD)	E-evidence Regulation, (EU) 2023/1533	Regulation for a Single Digital Gateway, (EU) 2018/1724	e-invoicing Directive, (EU) 2014/68	Single Market Programme, (EU) 2021/690	Copyright Directive, (EU) 2019/770	Financial Data Access Regulation, 2023/0205 (COD)		
	European Chips Act (Regulation), (EU) 2023/1781	Roaming Regulation, (EU) 2022/632	ePrivacy Regulation, 2017/0093(COD)	Standard essential patents, 2023/0133(COD)	Cyber Solidarity Act (Regulation), 2023/0109(COD)	Directive on combating violence against women, 2022/0068(COD)	General Product Safety Regulation, (EU) 2023/888	Geo-Blocking Regulation, (EU) 2018/502	Vertical Block Exemption Regulation (VBER), (EU) 2022/720	European Media Freedom Act, 2022/0277(COD)	Payment Services Regulation, 2023/0210(COD)		
	European critical raw materials act (Regulation), 2023/0079(COD)	Regulation on the Union Secure Connectivity Programme, (EU) 2023/688	European Data Act (Regulation), 2022/0047(COD)			Digitalization of travel documents	Machinery Regulation, (EU) 2023/1230	Regulation on cooperation for the enforcement of consumer protection laws, (EU) 2017/2394	Digital Market Act (DMA Regulation), (EU) 2022/1926	Remuneration of musicians from third countries for recorded music played in the EU	Digital euro, 2023/0212 (COD)		
	Net Zero Industry Act, 2023/0061(COD)	New radio spectrum policy programme (RSPF 2.0)	European Health Data Space Regulation, 2022/0140(COD)				AI Act (Regulation), 2021/0106(COD)	Digital content Directive, (EU) 2019/770	Regulation on distortive foreign subsidies, (EU) 2022/2660		Regulation on combating late payment, 2023/0323(COD)		
	Establishing the Strategic Technologies for Europe Platform (STEP), 2023/0199(COD)	Digital Networks Act	Regulation on data collection for short-term rental, 2022/0356(COD)				Eco-design Regulation, 2022/0095(COD)	Directive on certain aspects concerning contracts for the sale of goods, (EU) 2019/771	Horizontal Block Exemption Regulations (HBER), (EU) 2023/1066, (EU) 2023/1067				
	EU Space Law		Interoperable Europe Act, 2022/0375(COD)				AI Liability Directive, 2022/0303(COD)	Digital Services Act (DSA Regulation), (EU) 2022/2066	Platform Work Directive, 2021/0414(COD)				
	Initiative to open up European supercomputer capacity to AI start-ups		Harmonization of GDPR enforcement 2023/0202(COD)					Political Advertising Regulation, 2021/0381(COD)	Single Market Emergency Instrument (SMEI), 2022/0278(COD)				
			Access to vehicle data, functions and resources					Right to repair Directive, 2023/0083(COD)					
			GreenData4all					Multimodal digital mobility services (MDMS)					
								Consumer protection: strengthened enforcement cooperation					



## **The (draft) EU AI Act explained**

# AI Act

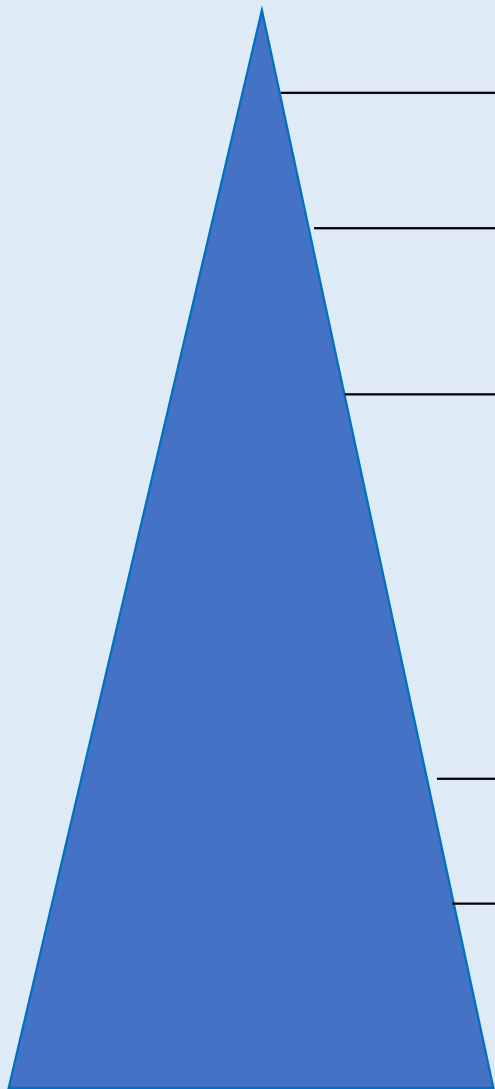
## DOELEN:

- a) bevorderen van het vertrouwen
- b) bevorderen van groei en innovatie.

## HOE?

- Productveiligheid
- Conformity before placing on market or taking into use
- Volgens een risico gebaseerde aanpak
- Verordening





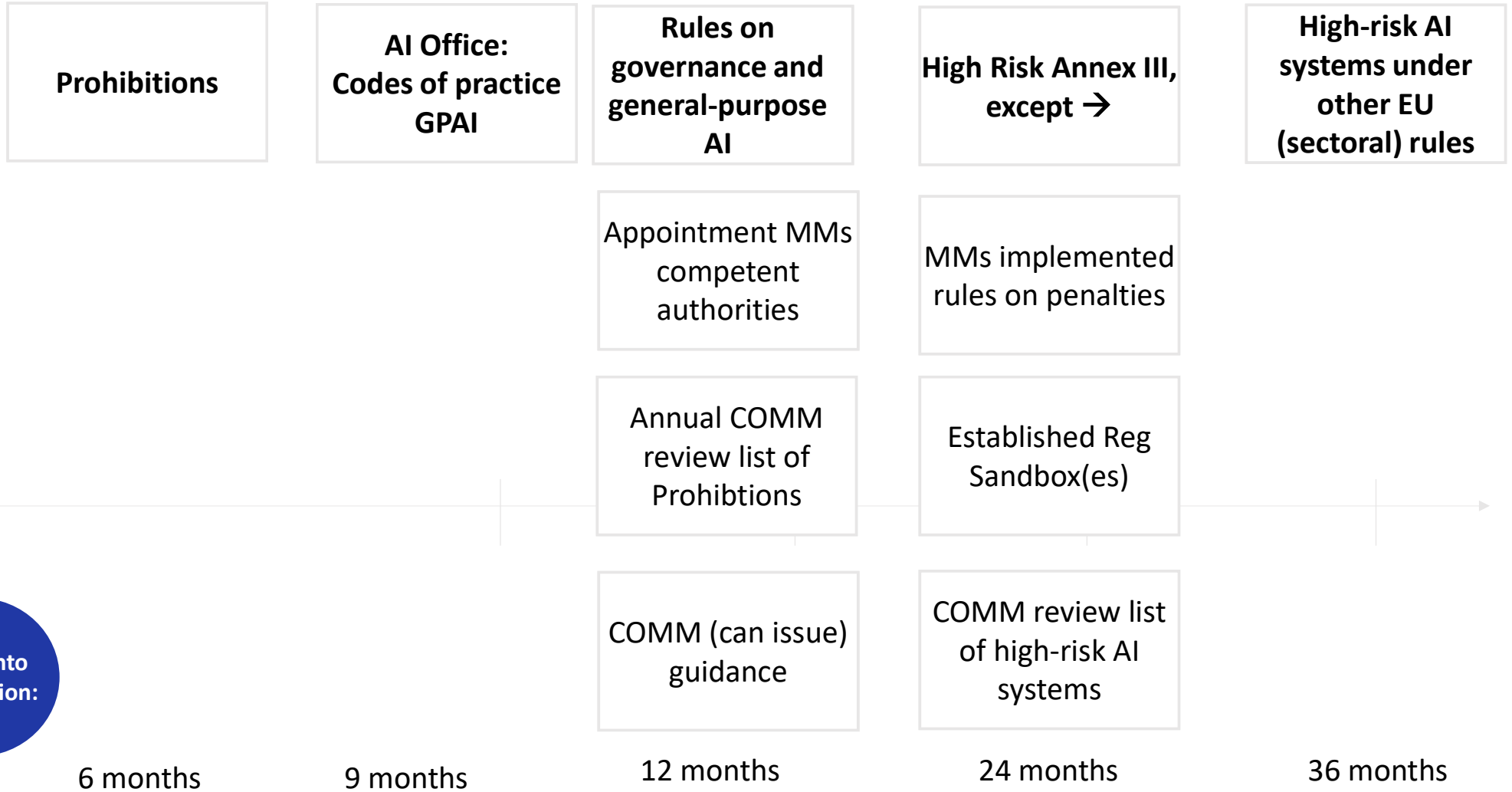
<b>Unacceptable risk (e.g. social scoring)</b>	<b>Forbidden</b>
High Risk (e.g. recruitment, medical devices) Annex I/II & III	<b>Permitted but</b> subject to compliance with AI requirements and ex-ante conformity assessment
AI with specific extra transparency obligations ('impersonation bots') (art. 52) and <i>whether qualified as high-risk or not</i>	<b>Permitted but</b> subject to information/transparency obligations  [notify humans they interact with a bot, are exposed to emotion recognition system or biometric categorization system; & apply label to deep fakes]
Rules on GPAI	<b>Permitted but</b> subject to obligations
Minimal or no risk:	<b>Permitted</b> with no restrictions [codes of conduct encouraged to foster voluntary application of requirements to low-risk AI systems]

# Process and timeline



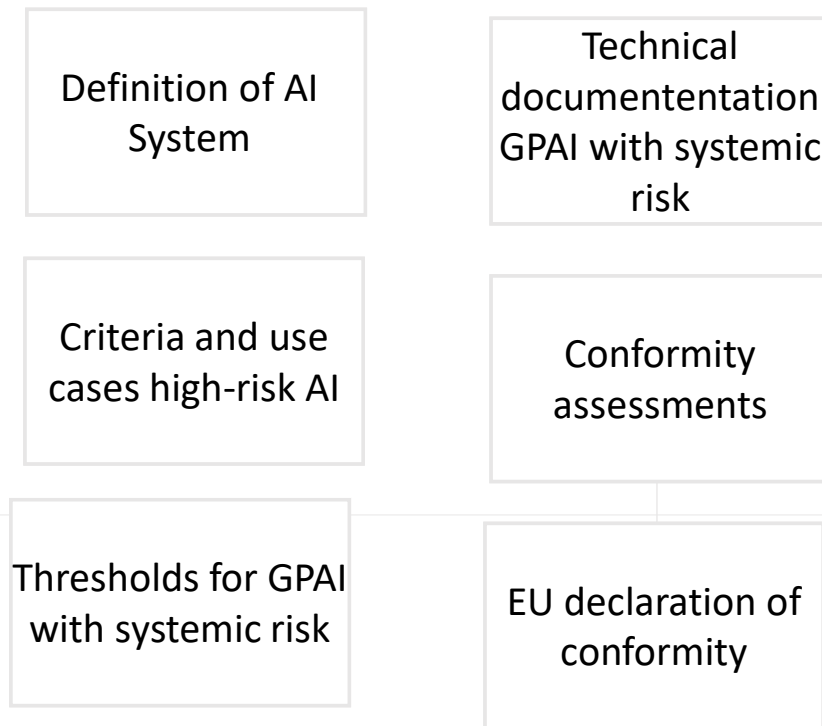
First: publication in Official Journal of EU

Adoption and entry into force

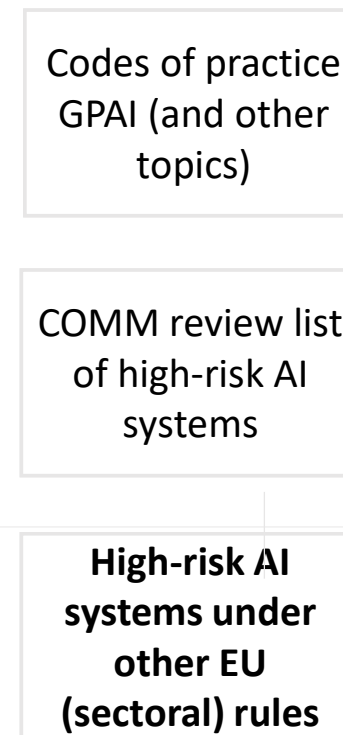


# Further rulemaking

The COMM can issue delegated acts on:



The AI Office is to draw up:



# Standards on AI

CEN CENELEC Technical Committee 21 (CEN-CLC/JTC 21)

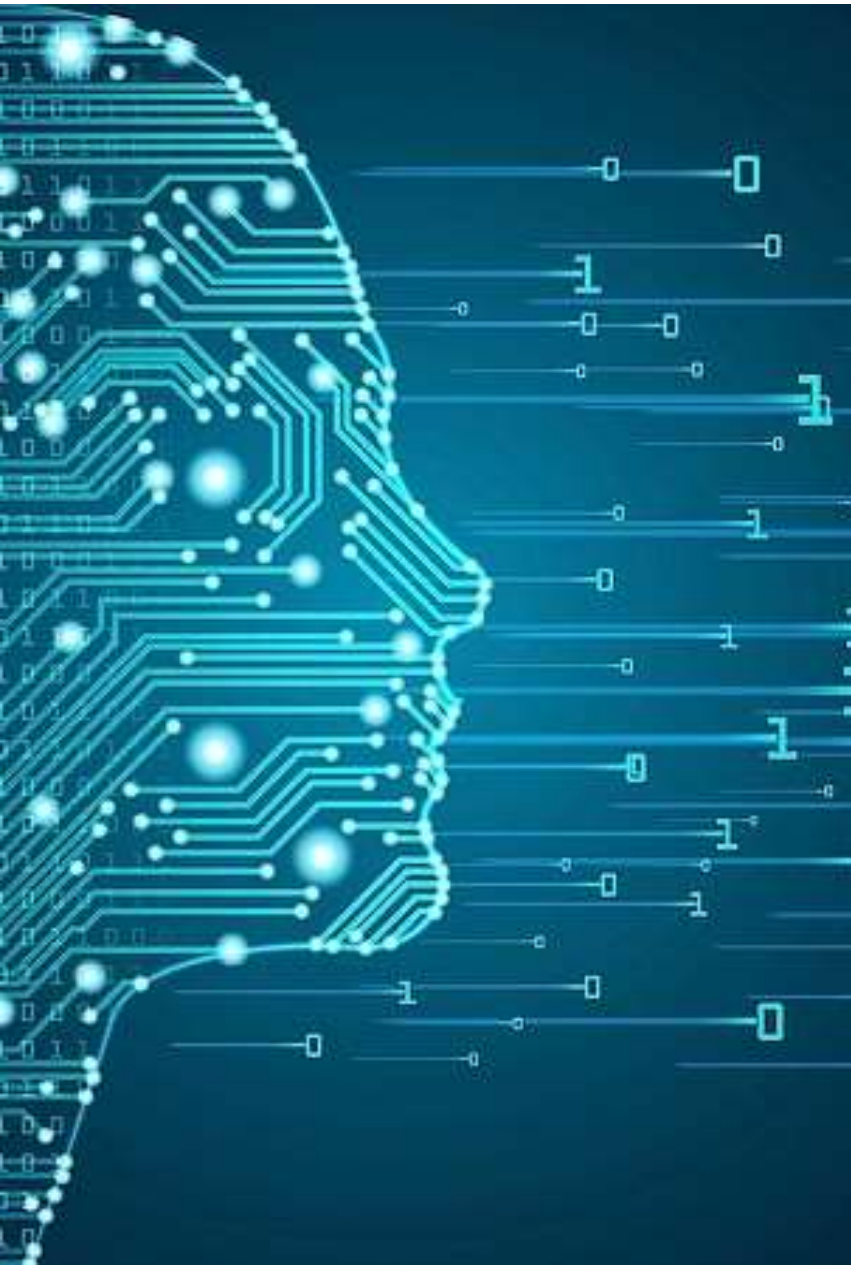
Support  
Standardisation  
requests on AI

Accountability  
Quality  
Data for AI  
Security and privacy  
Ethics  
Engineering of AI  
systems  
Safety of AI systems

See what is already  
developed in  
international context  
(ISO) and what is  
needed on top in EU  
(regarding AI Act)

ISO/IEC 38500:2015  
(accountability)  
ISO 9001 or ISO/IEC  
27001 (Quality)

Started working  
on AI-enhanced  
Nudging  
Mechanisms

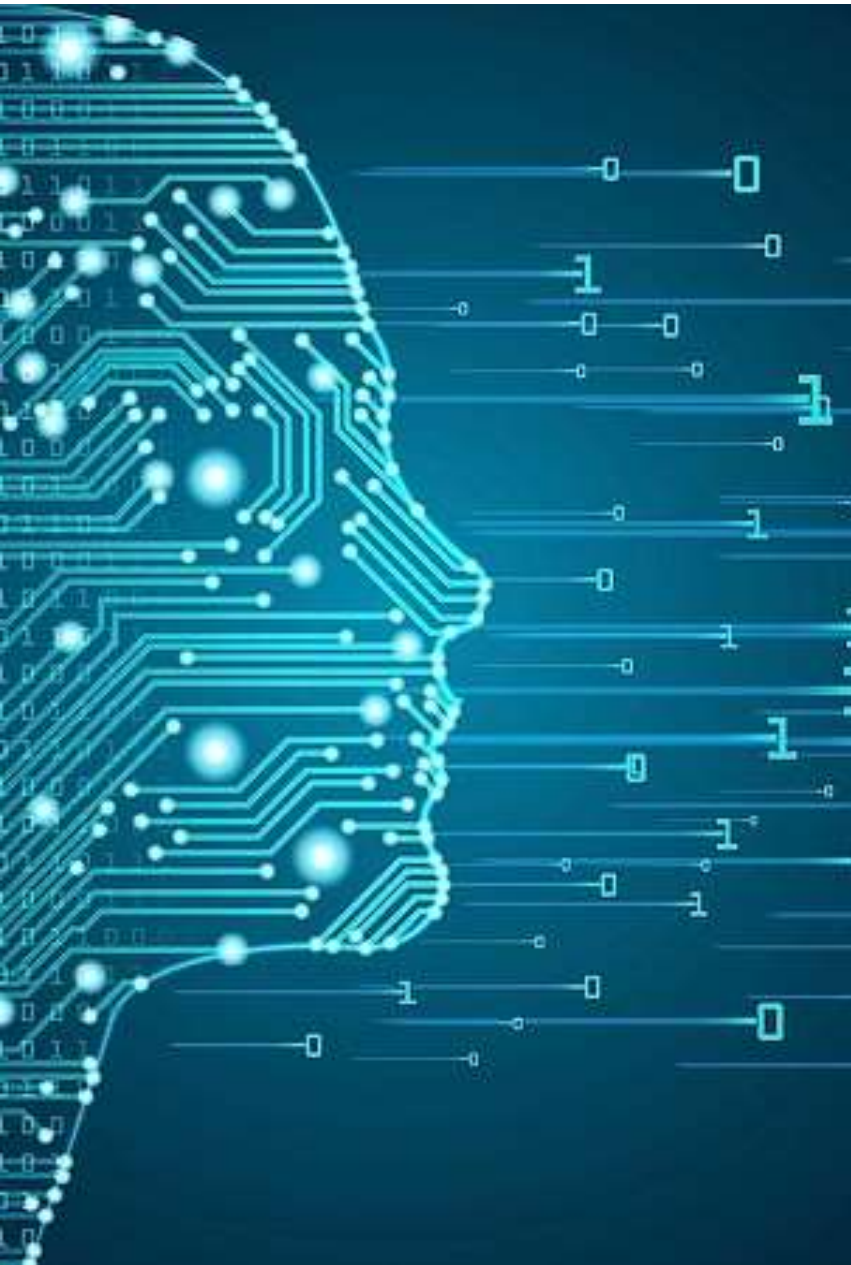


## AI system

“An AI system is a machine-based system 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.”

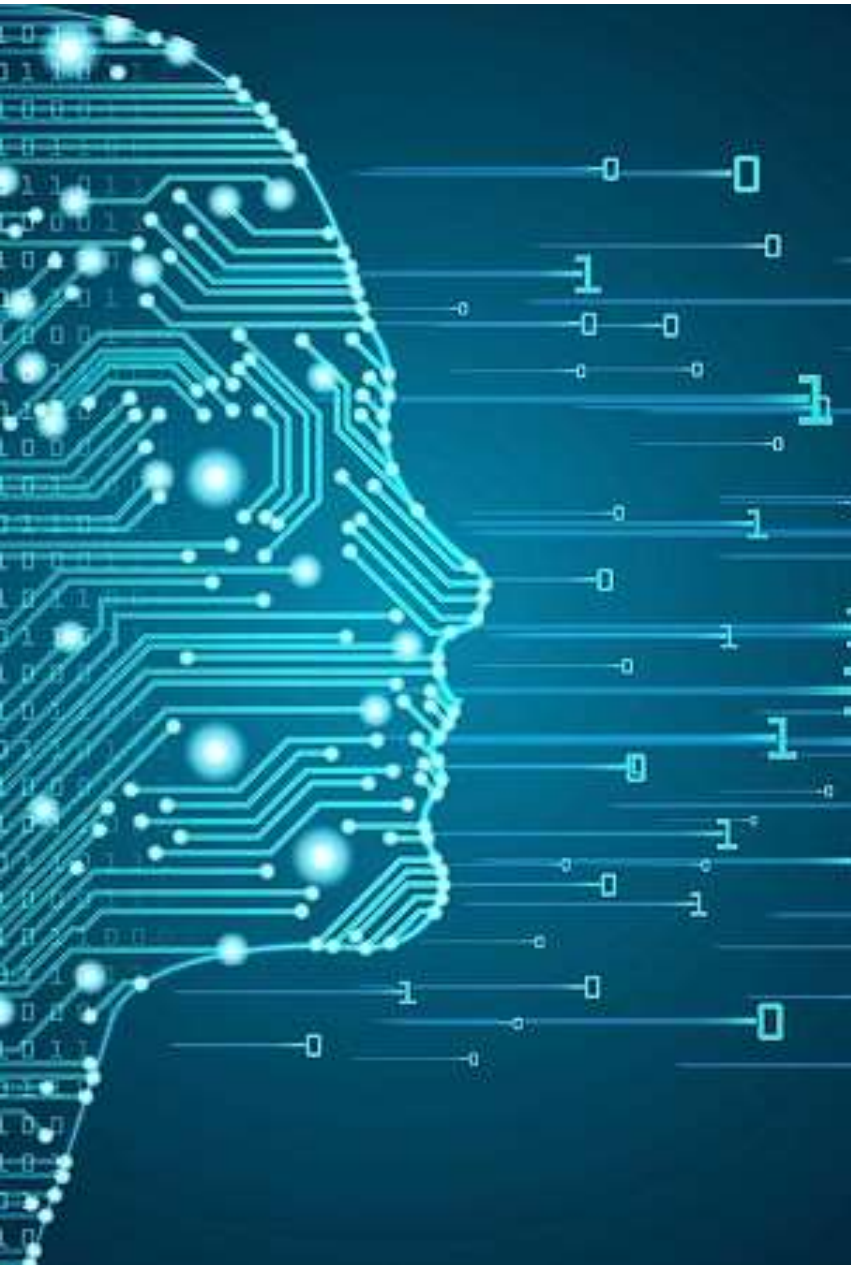
OESO (update):

“An AI system is a machine-based system that, for explicit or implicit objectives, **infers**, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment”



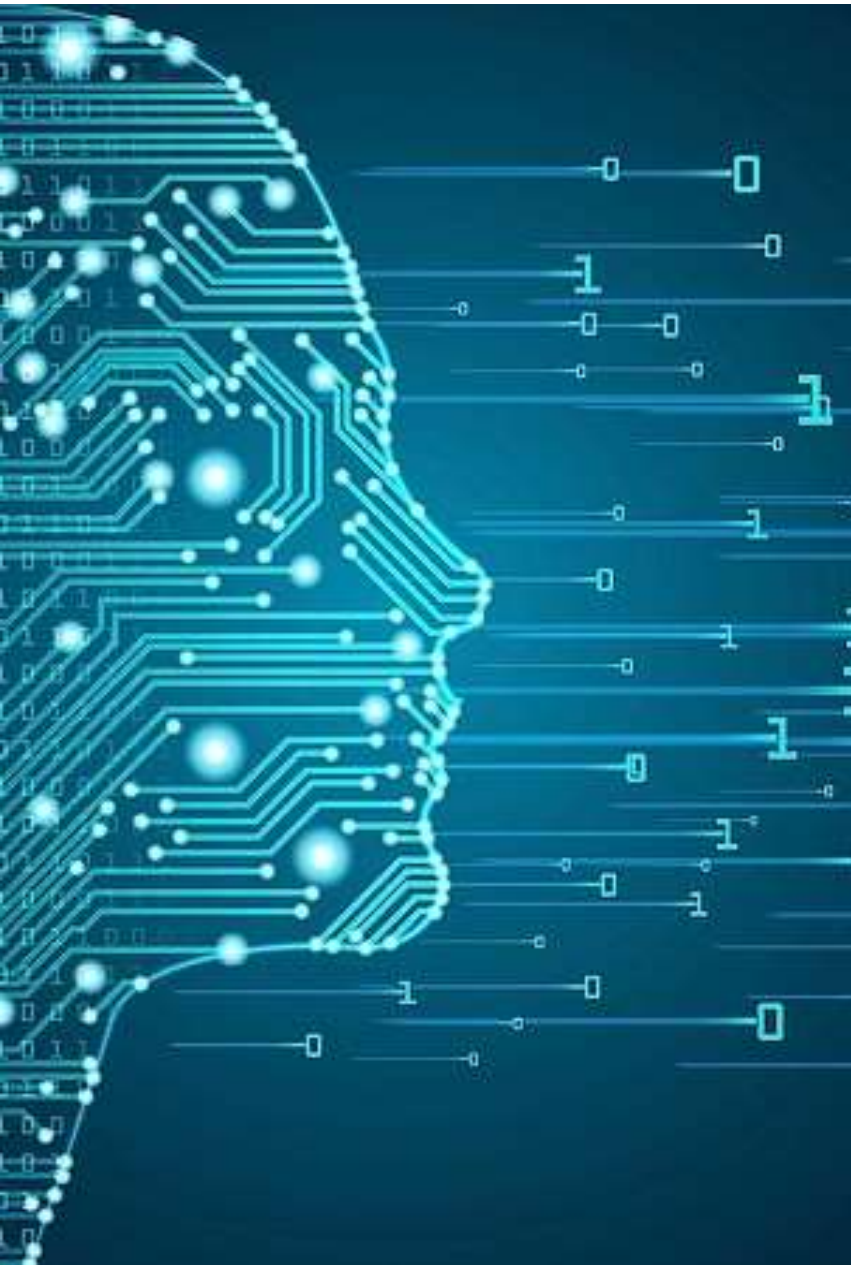
[Overweging 6]

- “Should **not** cover systems that are based on the rules defined solely by natural persons to automatically execute operations.
- A key characteristic of AI systems is their capability to **infer**: process of generating outputs and capability of AI systems to derive models and/or algorithms from inputs/data.
- The capacity of an AI system to infer goes beyond basic data processing, enable learning, reasoning or modelling.
- The techniques that enable inference while building an AI system **include** machine learning approaches that learn from data how to achieve certain objectives; and logic- and knowledge-based approaches that infer from encoded knowledge or symbolic representation of the task to be solved.



## VERBODEN AI

- Deploying **subliminal, manipulative** or **deceptive** techniques to change behaviour
- AI-systems that infer **emotions** in the workplace or educational institutes
- **Real-time remote biometric identification** in publicly accessible spaces for law enforcement purpose
- And 5 more, waaronder:



## VERBODEN AI

Biometric categorisation systems that categorise individuals based on the biometric data to deduce specific categories of personal data (bijzondere persoonsgegevens).

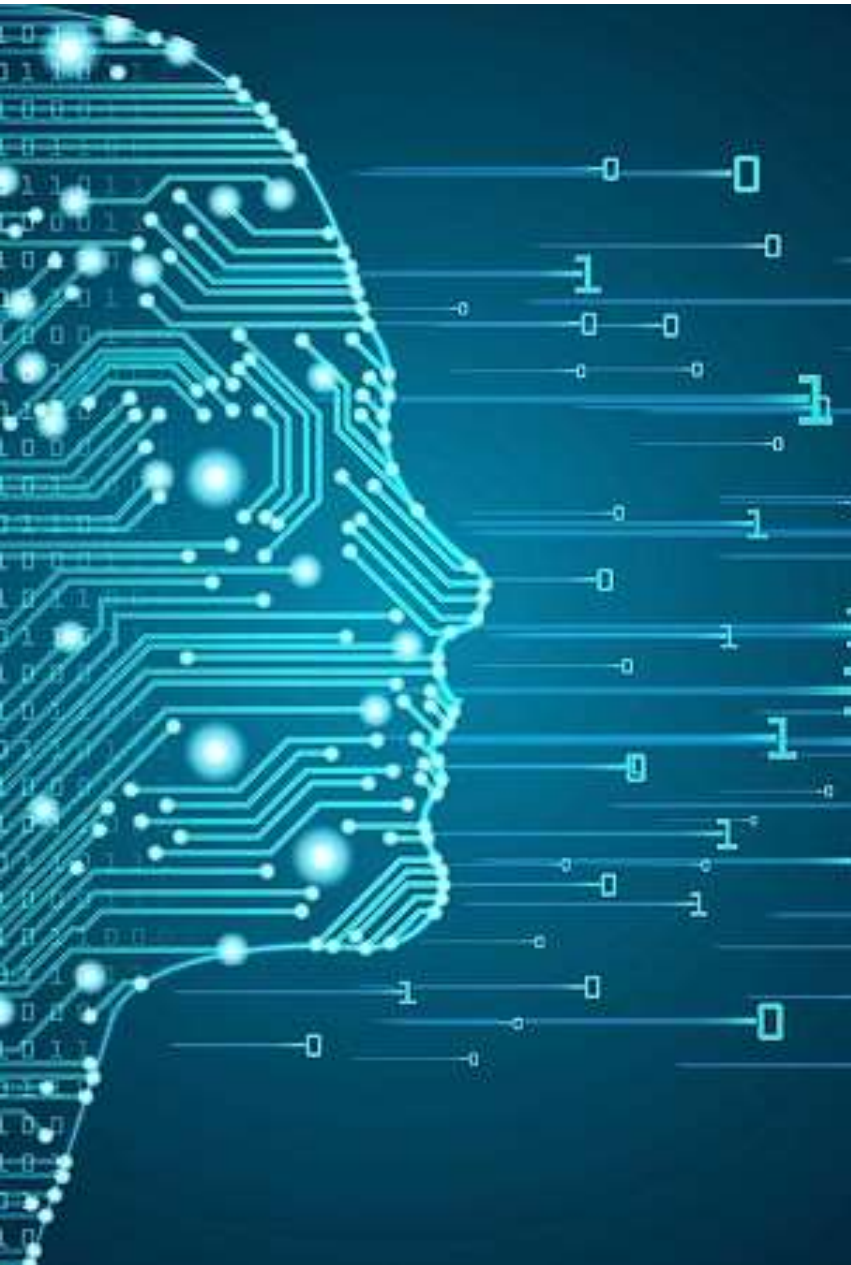
*“the placing on the market, the putting into service for this specific purpose, or the use of biometric categorisation systems that categorise individually natural persons based on their biometric data to deduce or infer their race, political opinions, trade union membership, religious or philosophical beliefs, sex life or sexual orientation; this prohibition does not cover any labelling or filtering of lawfully acquired biometric datasets, such as images, based on biometric data or categorizing of biometric data in the area of law enforcement;”*

# Dark Patterns

AI Act	DSA	AVG	OHP	Data Act
<p>Deploying <b>subliminal</b> techniques or purposefully <b>manipulative or deceptive</b> techniques, with objective or effect of materially <b>distorting</b> behaviour by appreciably <b>impairing</b> to make informed decision, that causes or reasonably likely to <b>cause significant harm</b> (dark patterns)</p>	<p>Providers of online platforms: not design, organise or operate their online interfaces: <b>deceives</b> or <b>manipulates</b> or <b>otherwise materially distorts or impairs</b> the ability to make free and informed decisions</p>	<p>Not to be subject to a decision based solely on automated processing, including profiling, which <b>produces legal effects</b> concerning him or her <b>or similarly significantly affects</b> him or her.            Uitzonderingen:  <ul style="list-style-type: none"> <li>• Noodzakelijk contract</li> <li>• Wettelijke basis</li> <li>• Toestemming</li> </ul>           Niet gebaseerd op bijz per geg tenzij art. 9.2 (a),(g) AVG</p>	<p>Commercial practice which <b>materially distorts</b> or is likely to materially distort the economic behaviour with regard to the product [...]</p> <p>materially distort = appreciably <b>impair</b> decision, that would not have taken otherwise.</p>	<p>Not make the exercise of choices or rights <b>unduly difficult</b>, including [...] by <b>subverting or impairing</b> the autonomy, decision-making or choices of the user via the structure, design, function or manner of operation of a user digital interface or part thereof</p>
<p>Artikel 5.1(a); overweging 29</p>	<p>Artikel 25 Overweging 67</p>	<p>Artikel 22 Overweging 71</p>	<p>Artikel 2 en 5</p>	<p>Artikel 4.4 en 6.2 Overweging 38</p>

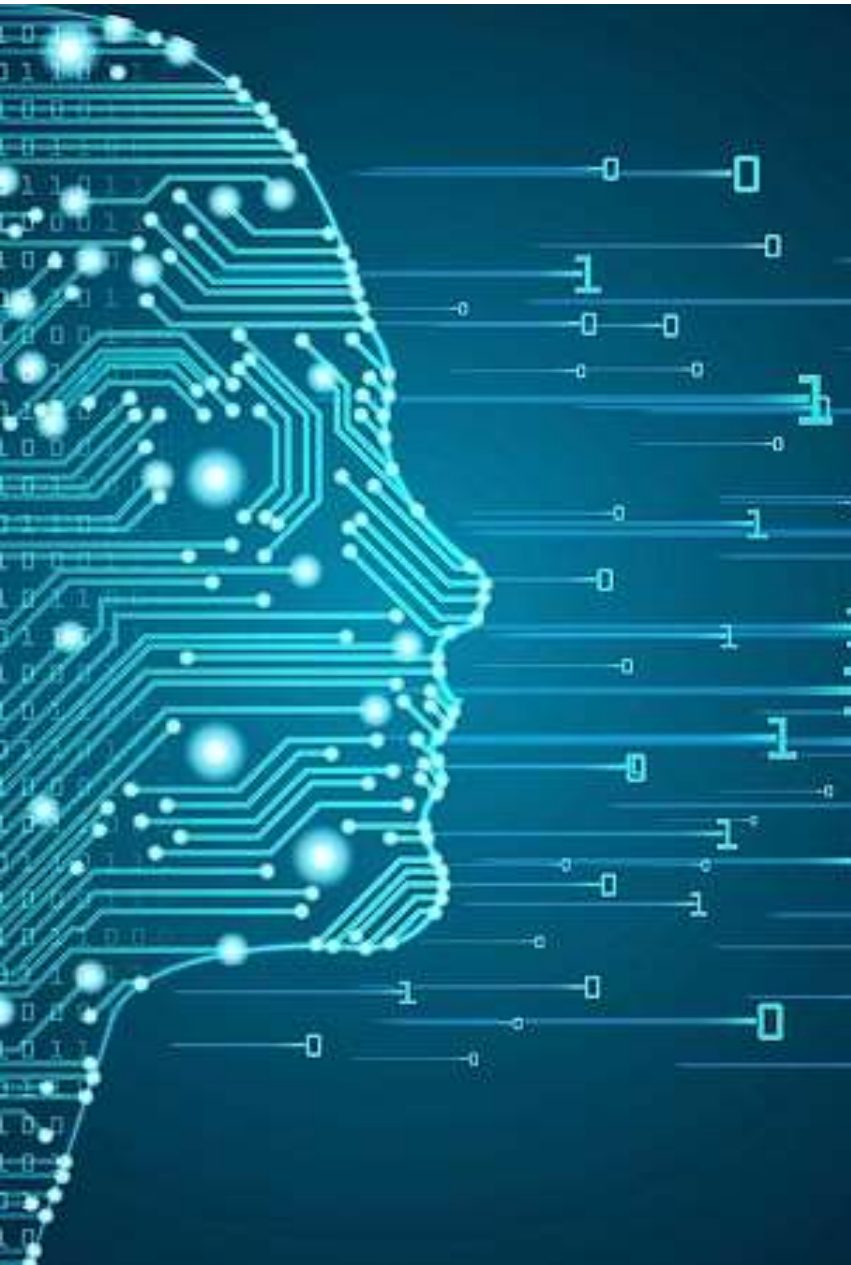
Niet: legitieme reclamepraktijken

AI Act	DSA		AVG	Data Act	DMA
<b>Verbod</b> op AI system <b>to infer emotions of a natural person in the areas of workplace and education institutions (except medical &amp; safety reasons)</b>	<b>Verbod</b> op gerichte advertenties gebaseerd op profielen opgebouwd met gebruik van bijzondere persoonsgegevens	<b>Verbod voor O.P.</b> advertenties gebaseerd op profielen waarvan ze redelijkerwijs met zekerheid bewust zijn dat minderjarigen gebruik maken van hun diensten	<b>Verbod</b> op verwerking bijzondere persoonsgegevens tenzij wettelijke uitzondering.	(o.a.) <b>Verbod</b> 3 <sup>rd</sup> parties to use accessed data for developing a <b>competing</b> connected product.; <b>profilieren</b> obv data tenzij noodzakelijk dienst; verbod doorgifte aan gatekeeper	<b>Verbod</b> for Gatekeepers to combine certain data without <b>freely given consent</b> ; <b>verbod</b> op gebruik data vanuit duale rol Gatekeeper. <b>(bieden van gelijkwaardig alternatief (afsluiten van dienst niet toegestaan).</b>
Artikel 5 (f)	Artikel 26	Artikel 28	Artikel 9	Artikel 6.2(e); Artikel 11.3 (b) Overweging 32	Artikel 1.8 (f) Artikel 5.2
Placing on market, putting into service or use of AI system		Lid 3: geen verplichting aanvullende persoonsgegevens		protects data holders' innovation efforts	data andere 'core platform services'/andere diensten GK; of van diensten van derden



Hoog-Risico Annex I - sectorale wetgeving met 3<sup>rd</sup> party assessment:

- Toys
- Machinery
- Lifts
- Radio equipment
- Medical devices
- Drones
- Vehicles
- Tractors



## Hoog-Risico Annex III - Use cases

### **Biometrics**

Remote biometric identification systems

Biometric categorisation

Emotion recognition

### **Safety in the operation of critical infrastructure**

Digital infrastructure, road traffic, supply of gas, water, heating and electricity

### **Education and vocational training**

E.g. determining admission, evaluating learning outcomes

### **Employment**

E.g. recruitment and selection of natural persons, promotion and termination

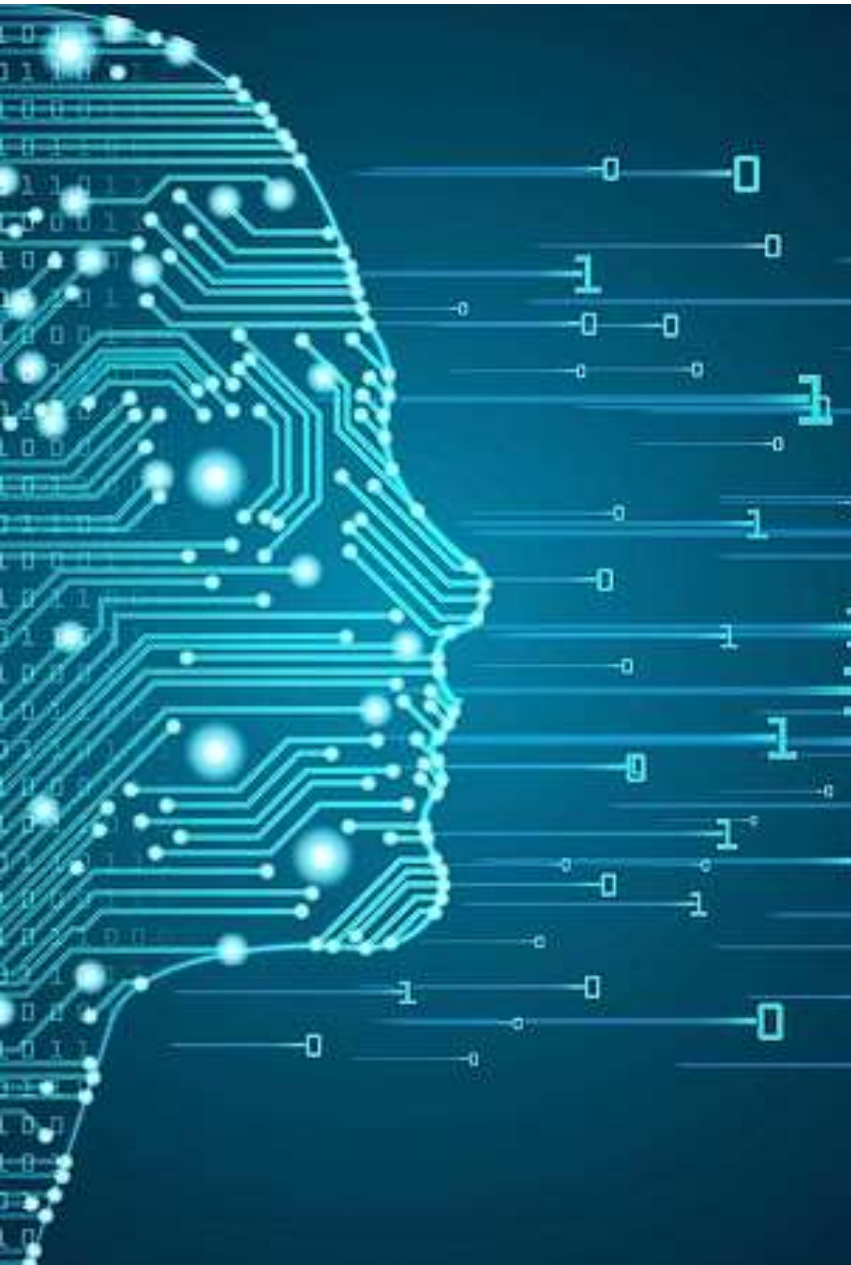
### **Access to essential private and public services and benefits**

Evaluation of eligibility of natural persons

Evaluation of creditworthiness

Risk assessment for pricing of life and health insurance

Evaluate and classify emergency calls



## Hoog-Risico Annex III - Use cases

### **Law enforcement**

Assessing the risk of becoming a victim

The use of polygraphs

Evaluate reliability of evidence

Assessing likelihood of reoffence or offence

Profiling for the detection, investigation or prosecution of criminal offences

### **Migration, asylum and border control management**

The use of polygraphs

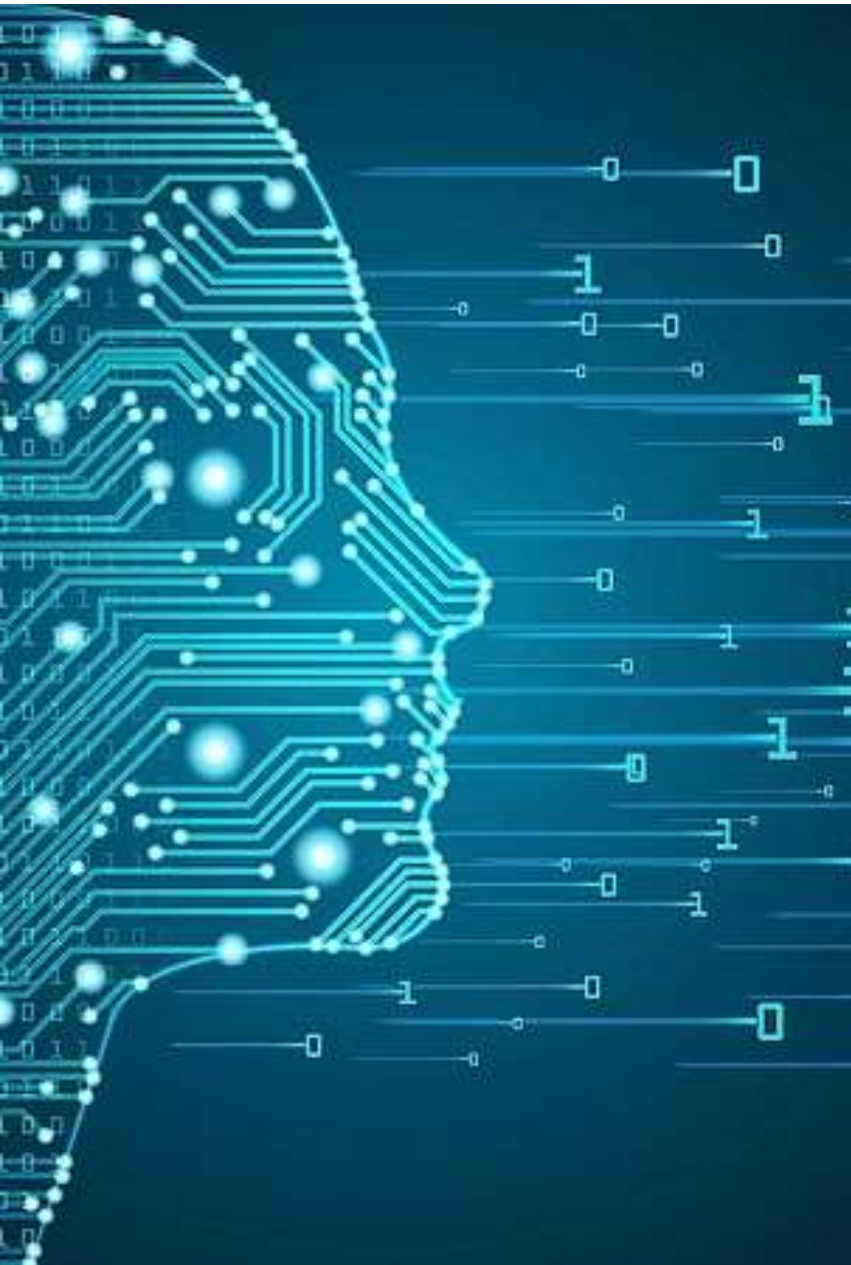
Assessing risk posed by someone entering the territory

Assisting the examination of asylum and visa applications

### **Administration of justice and democratic processes**

Assisting judicial authorities to research and interpret facts

Influencing the outcome of an election or referendum



Hoog-Risico Annex III - Use cases – extra filter:

***Extra filter*** hoog-risico classificatie Annex III  
(risico gebaseerde aanpak)

- narrow procedural tasks
- Mere preparatory tasks
- Improvement results as humanly prepared
- Decision without replacing human assessment

Hoog-Risico Annex III - Use cases; extra filter:

*By derogation from paragraph 2, an AI system referred to in Annex III shall not be considered to be high-risk where it does not pose a significant risk of harm to the health, safety or fundamental rights of natural persons, including by not materially influencing the outcome of decision making.*

*The first subparagraph shall apply where any of the following conditions is fulfilled:*

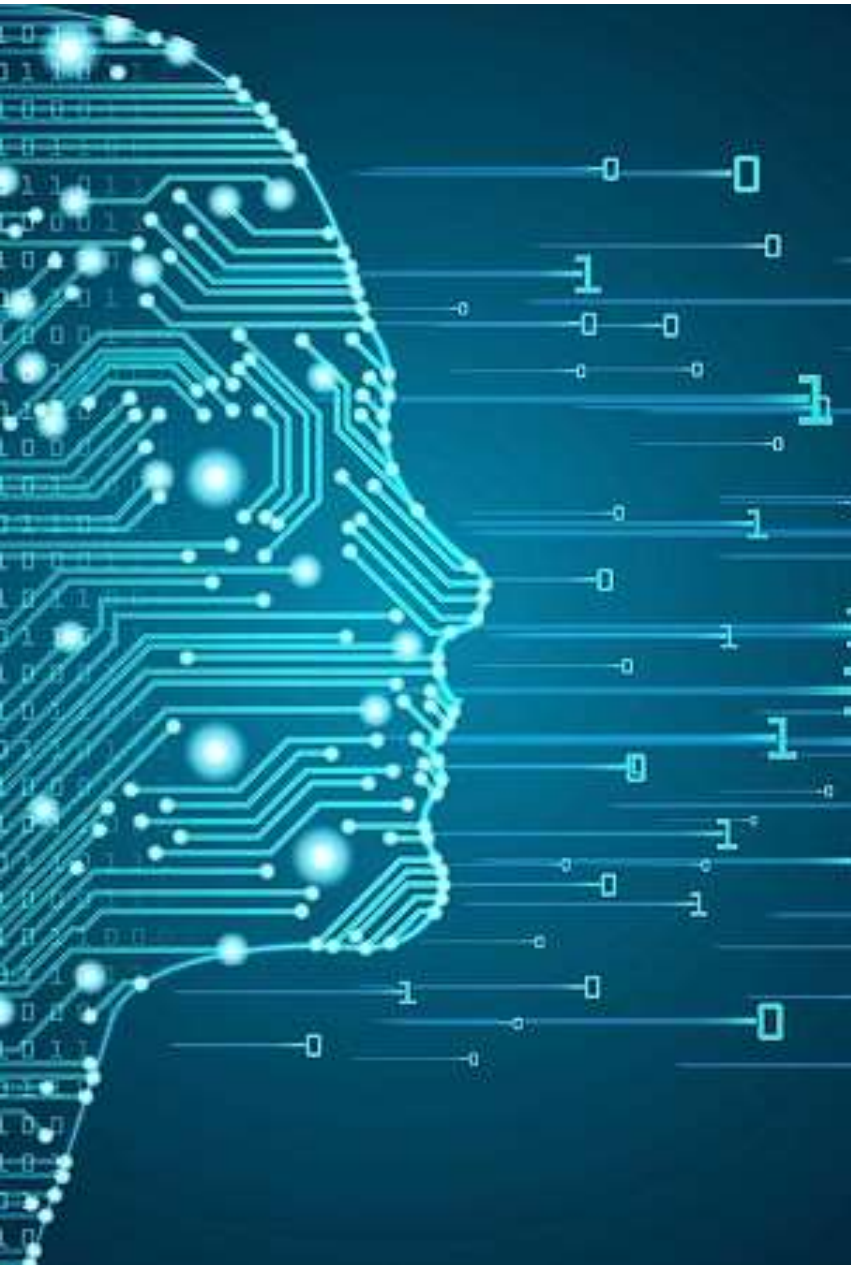
*(a) the AI system is intended to perform a narrow procedural task;*

*(b) the AI system is intended to improve the result of a previously completed human activity;*

*(c) the AI system is intended to detect decision-making patterns or deviations from prior decision-making patterns and is not meant to replace or influence the previously completed human assessment, without proper human review; or*

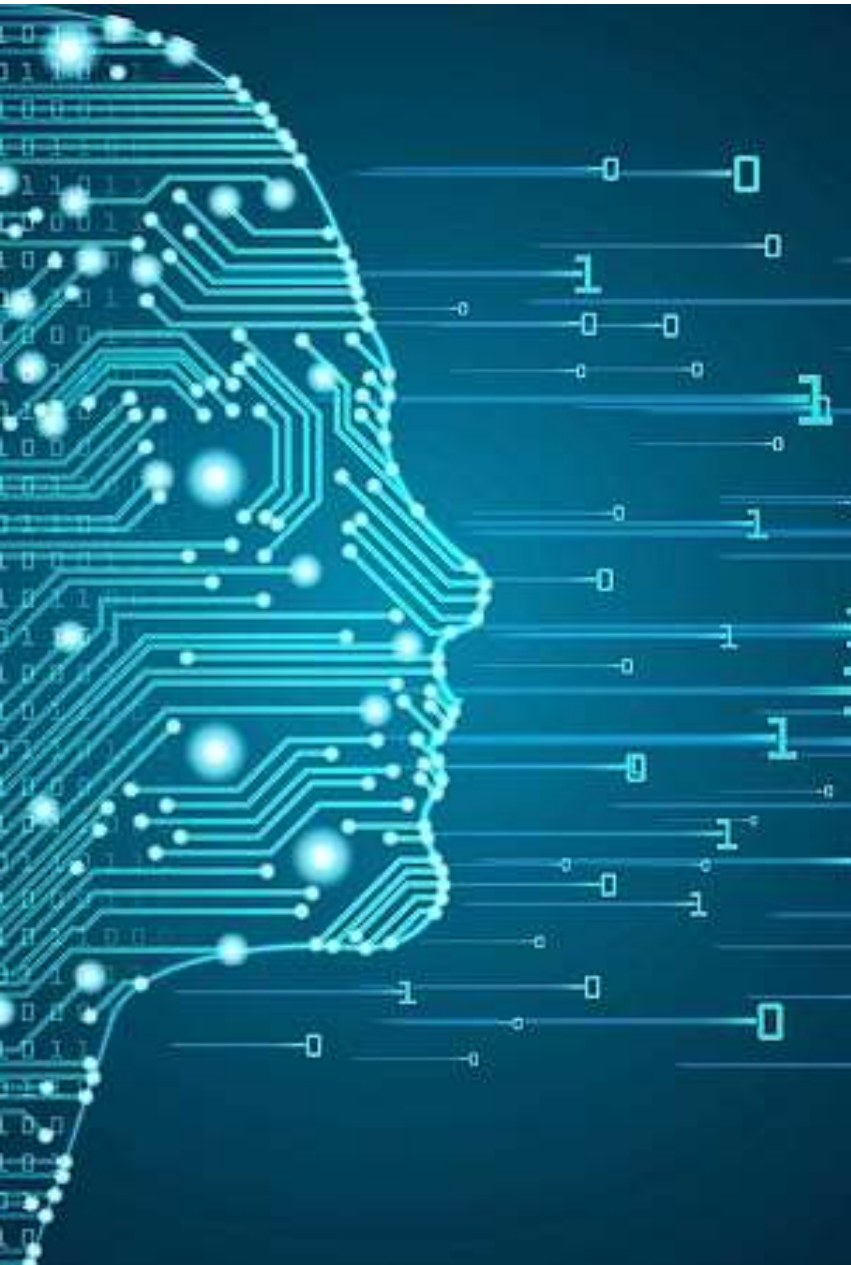
*(d) the AI system is intended to perform a preparatory task to an assessment relevant for the purposes of the use cases listed in Annex III.*

*Notwithstanding the first subparagraph, an AI system referred to in Annex III shall always be considered to be **high-risk** where the AI system performs **profiling** of natural persons.*



## Obligations of **providers high risk AI**

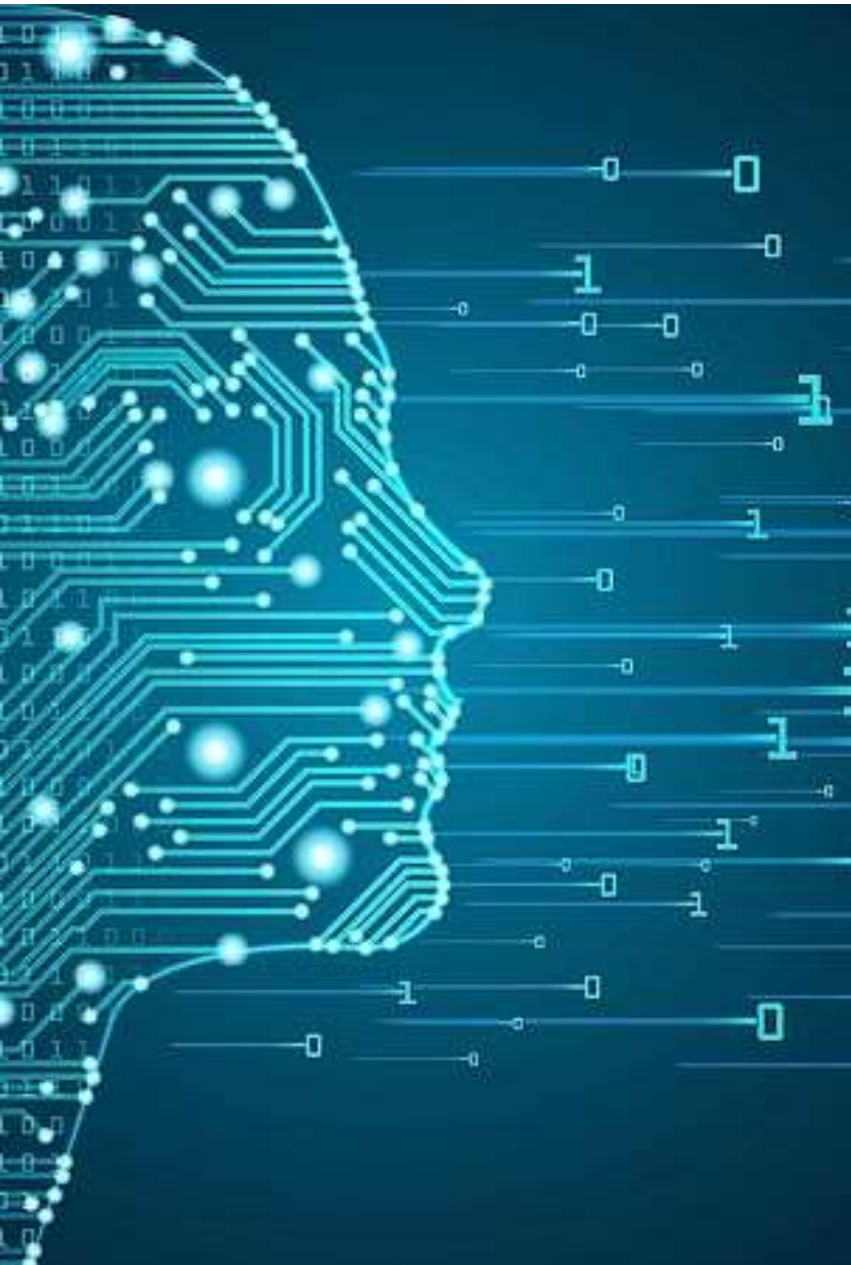
- Risk management system (art. 9)
- Quality management system (art. 17)
- Data and data governance (art. 10)
- Technical documentation (art. 11)
- Record keeping (art. 12)
- Transparency and provision info to deployers (art. 13)
- Human oversight (art. 14)
- Accuracy, robustness and cybersecurity (art. 15)
- Conformity assessment procedure (art. 43)
- Draw up an EU declaration of conformity (art. 47)
- Take the necessary corrective actions & info (art. 20)
- Affix CE marking (art. 48)
- Cooperate with competent authorities (art. 21)
- Incident reporting (art. 73)
- Providers established outside the Union shall, appoint an authorized representative (art. 22)
- Register in EU database (art.49)
- Responsibility along the value chain (art. 25)
- Post market monitoring (plan) (art. 72); **etc.**



### Obligations of importers

Before placing on the market, make sure:

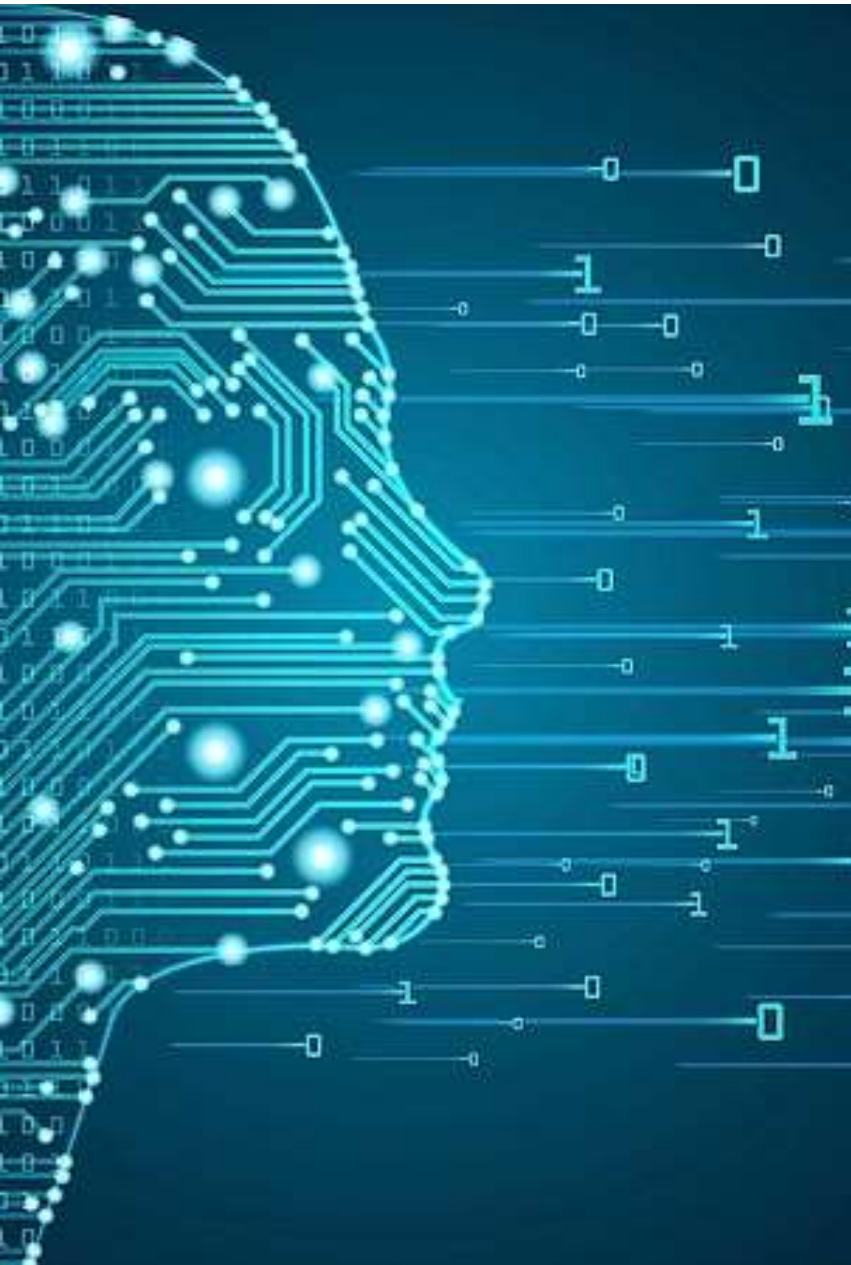
- conformity assessment procedure has been carried out by the provider
- provider has drawn up the technical documentation in accordance with Annex IV
- bears the required CE marking
- accompanied by the required documentation and user instructions
- Non-EU Provider appointed authorized representative



### Obligations of distributors

Before placing on the market, shall **verify** that:

- bears the required CE marking
- system is accompanied by the required documentation and user instructions
- that the provider and importer, as applicable, have complied with the obligations of this Regulation



Obligations of distributors, importers, deployer or any other third-party

Changes Colour (is **considered provider**) if:

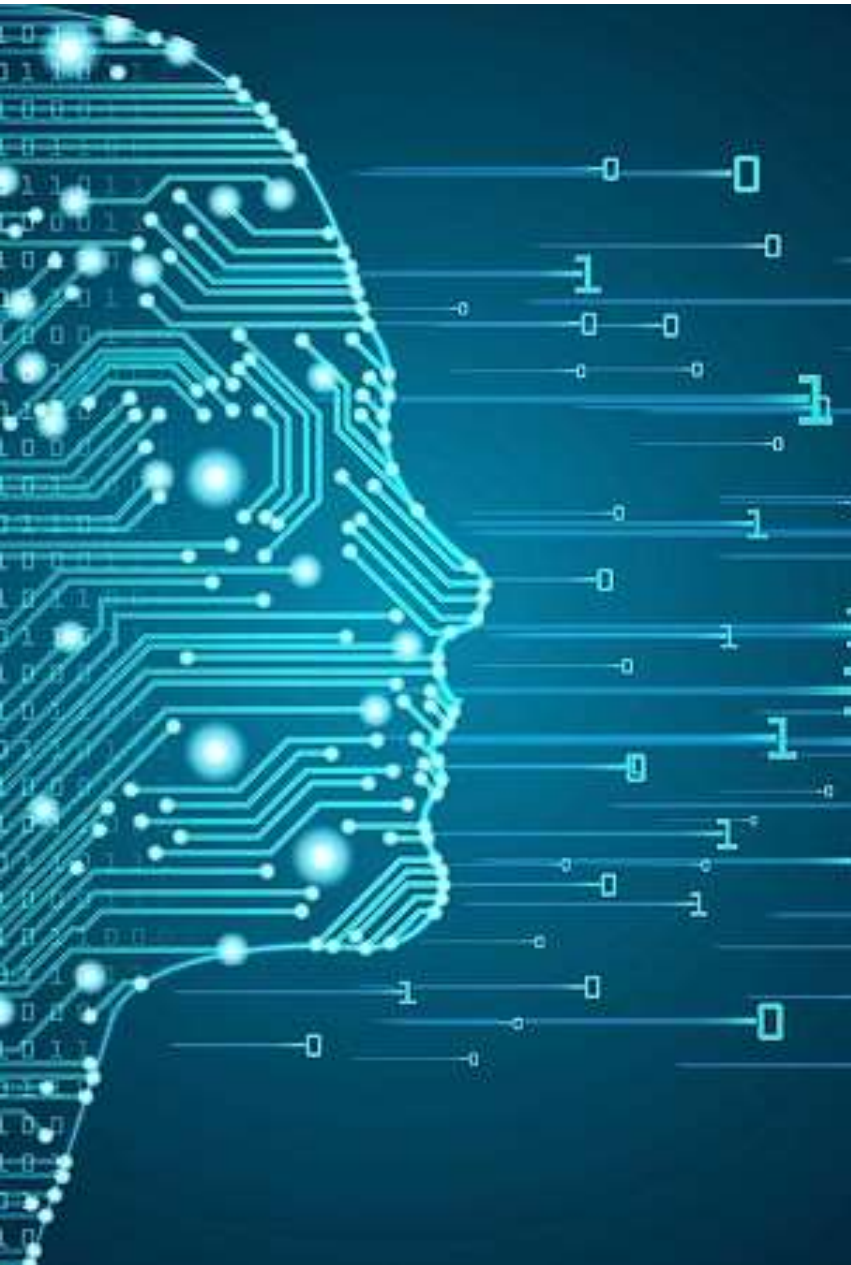
A. Place system on the market under their name of trademark

B. Make a substantial modification to the system

Ba Modify the intended purpose already placed on the market or put into services (including of GPAI).

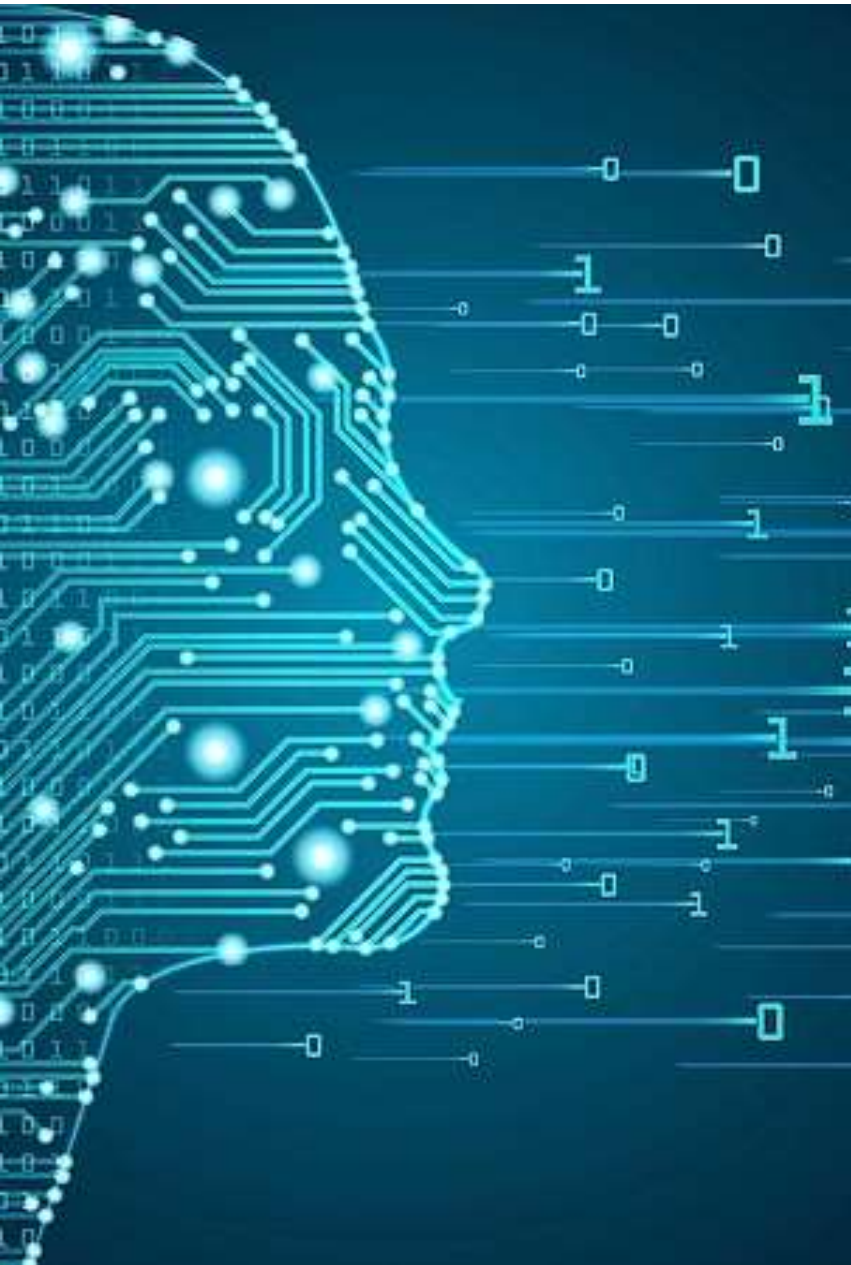
Regarding B and Ba: the original provider shall no longer be considered to be the provider (under this Regulation).

*Former provider has to cooperate and provide necessary information and provide reasonably expected technical access and other assistance required for fulfilment obligations.*



### Obligations of deployers

- Use the system in accordance with the **user instructions**
- **Assign human oversight (necessary competence, training and authority)**
- **(if) input data → to be relevant and sufficiently representative**
- **Monitor** the operation of the system (user instructions)
- **Inform the provider or the distributor**
- Keep the **automatic generated logs (under their control)**
- Use transparency info to carry out a **DPIA under GDPR**

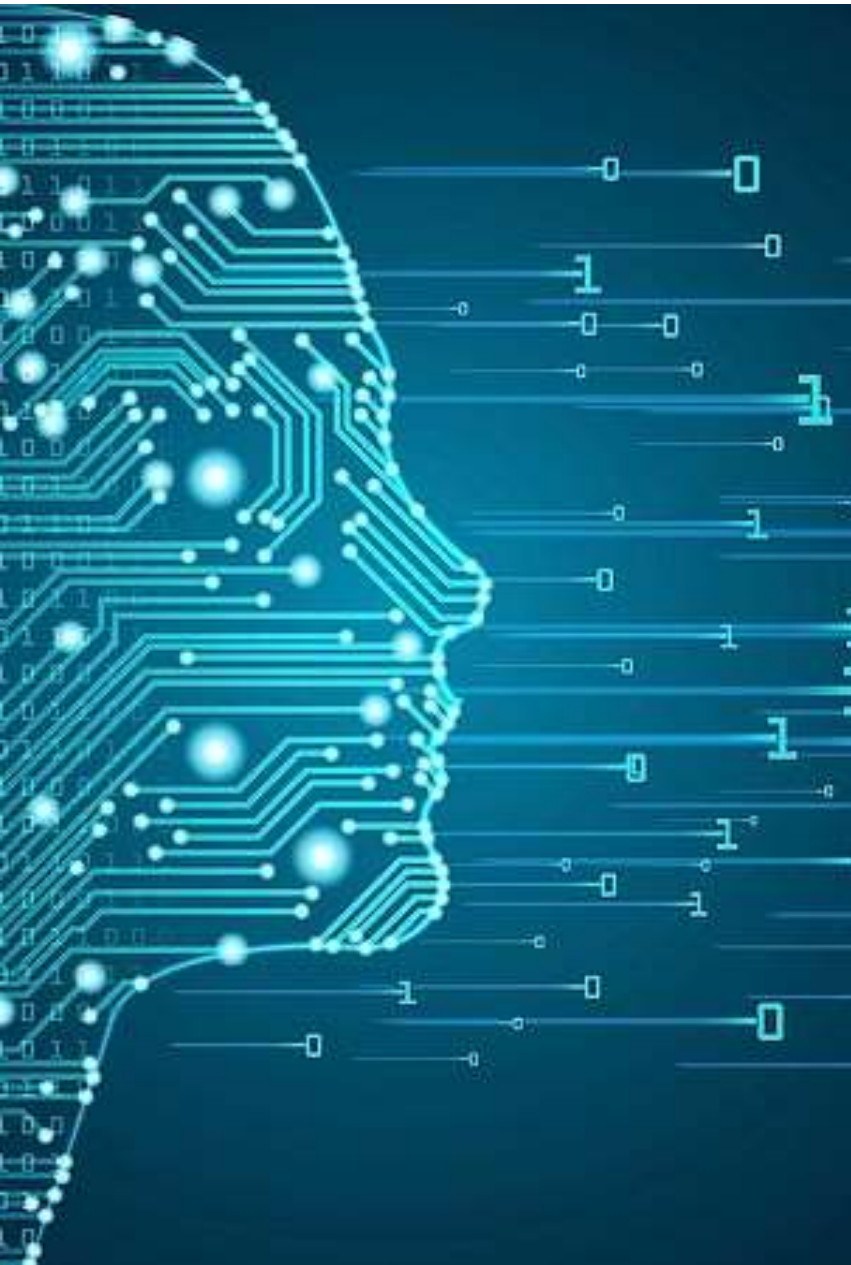


#### *Article 4 AI literacy*

*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.*

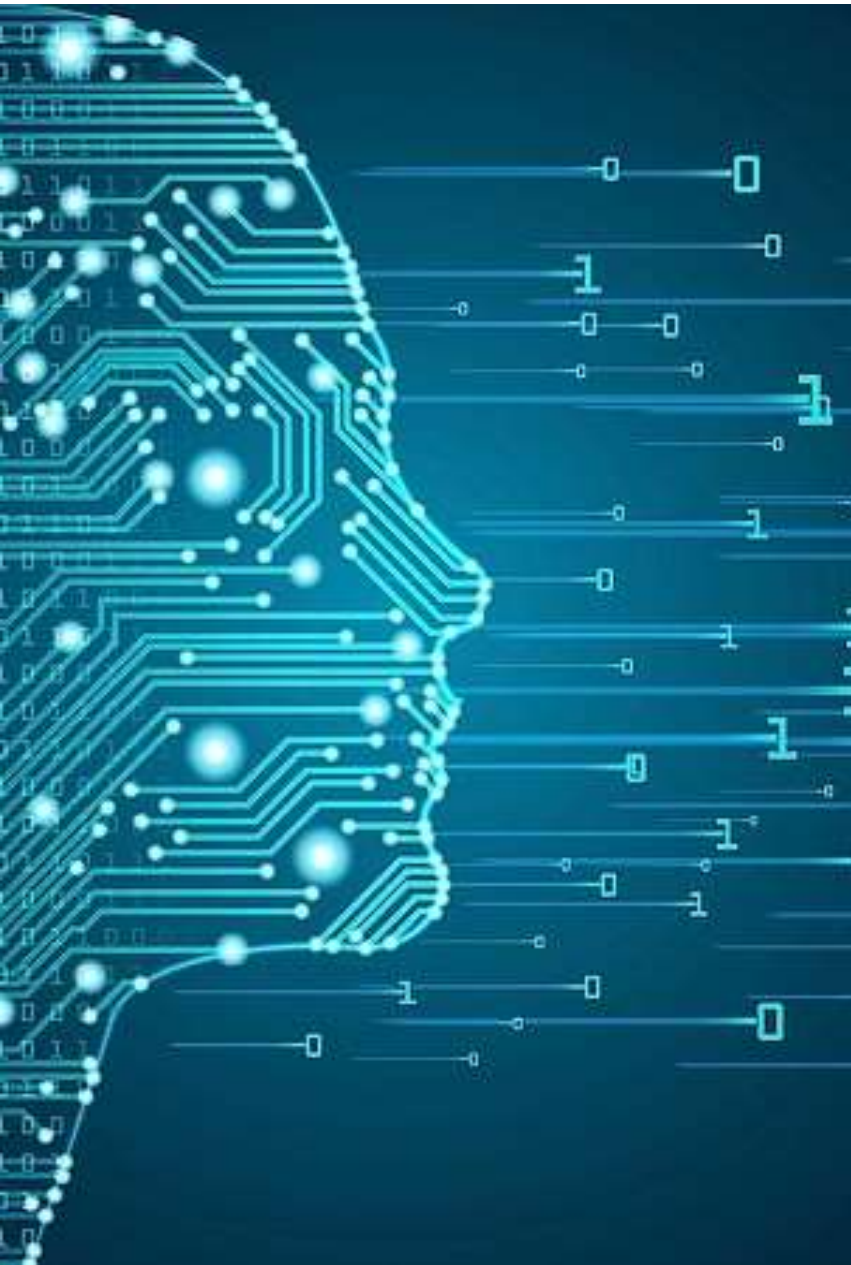
# Harmonised standards

AI Act	DSA	AVG	Data Act	DMA
<p>Standardisation should play a key role to provide technical solutions to providers to ensure compliance with Regulations, in line with the state of the art, to promote innovation as well as competitiveness and growth in the single market. Compliance with harmonised standards should be a means for providers to demonstrate conformity with the requirements of this Regulation.</p>				
<p>However, in the absence of relevant references to harmonised standards, the Commission should be able to establish, via implementing acts, and after consultation of the advisory forum, common specifications for certain requirements under this Regulation.</p>				



## SMEs

- The implementation of the risk management system/quality management system shall be **proportionate to the size** of the provider's organization
- conformity assessments “taking due **account of the size** of an undertaking”
- **Measures** for small-scale providers and users (priority sandboxes; awareness; dedicated **communication channel**)
- Small-scale providers and start-ups regarding **codes of conduct**
- Member States – **proportionality** penalties

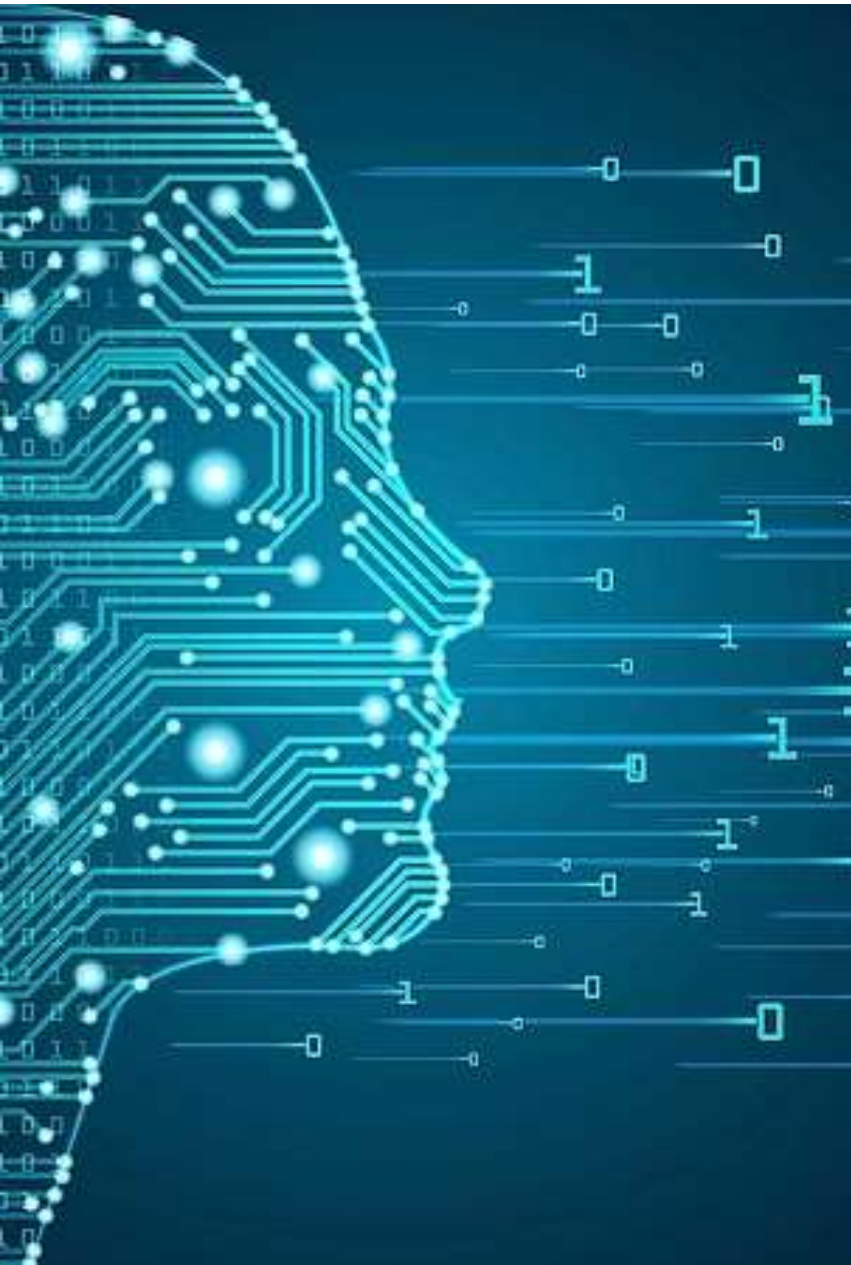


## **GPAI**

Onderscheid GPAI en GPAI met systeem risico's (systemic risk).

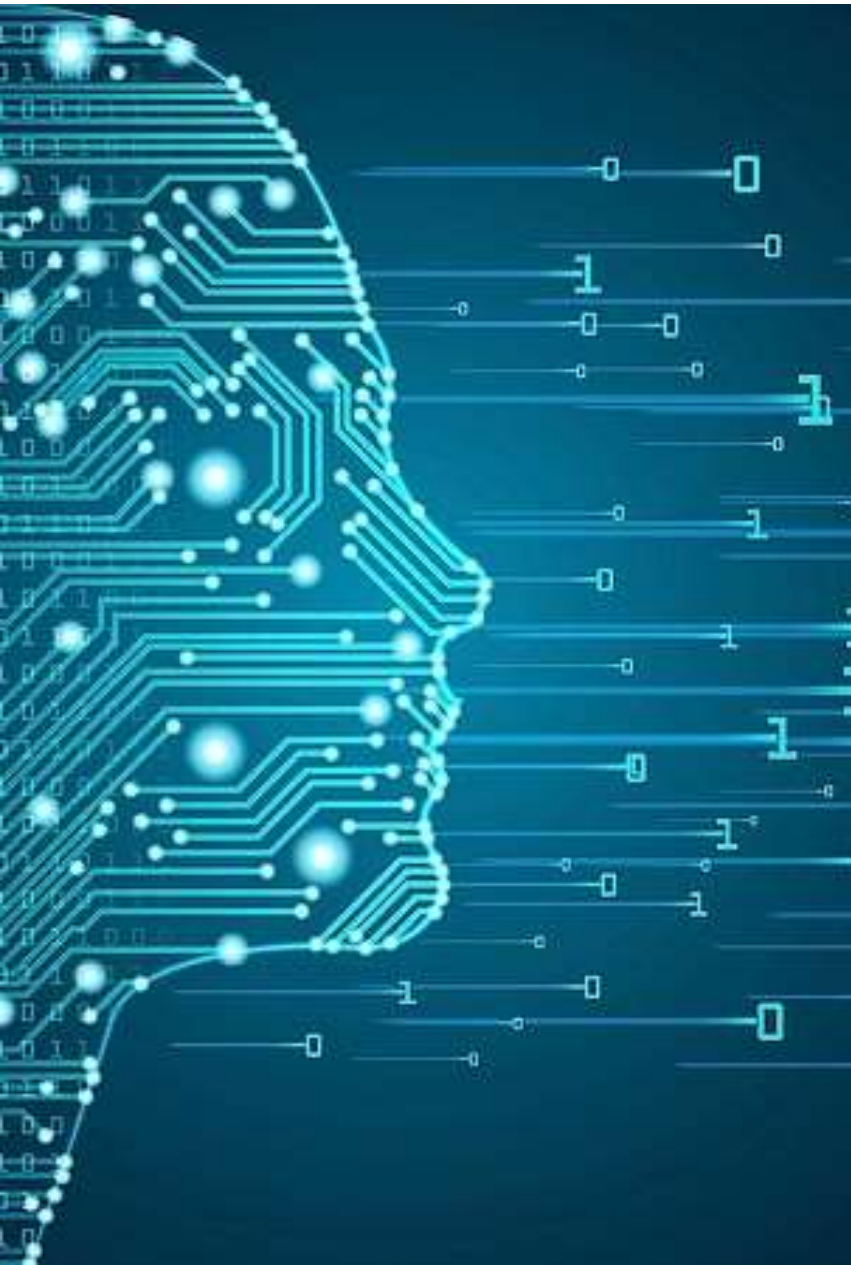
Classificatie GPAI met systeem risico's, aan de hand van criteria: training compute power  $10^{25}$  FLOPs (floating point operations).

Moet binnen 2 weken gemeld worden aan EC (moment dat je aan criteria voldoet of dat bekend is dat aan de criteria zal worden voldaan). Nu alleen GPT-4 (misschien Gemini), rest valt hier niet binnen.



## Verplichtingen alle GPAI:

- a) Technische documentatie (beschikbaar houden voor AI Office en nationale competente autoriteit)
- b) Documentatie en info: downstream providers in staat stellen aan hun verplichtingen onder de AI Act te voldoen:
  - a) capaciteiten en beperkingen (Annex minimale elementen technische documentatie);
- c) Auteursrecht beleid: hoe reservering van auteursrechten te identificeren en te respecteren.
- d) Samenvatting inhoud gebruikt voor training (AI Office template)



## Verplichtingen GPAI met systemic risk:

- a) Verplichtingen die voor alle GPAI providers gelden
- b) Model evaluatie
- c) Beoordelen en mitigeren mogelijke systeem risico's
- d) Rapporteren serieuze risico's (aan AI Office en nationale bevoegde autoriteit)
- e) Adequaat niveau cybersecurity beveiliging

Om compliance aan te tonen, kan gebruik worden gemaakt van Code of practice. Deze code moet binnen 9 maanden gerealiseerd zijn, AI Office taak om aan te jagen en faciliteren).

# Governance and enforcement

## Rules for AI systems

National authorities following the market surveillance system

## Rules for general-purpose AI models

EU level: AI Office within Commission



### AI Board

with Member States to coordinate at EU level



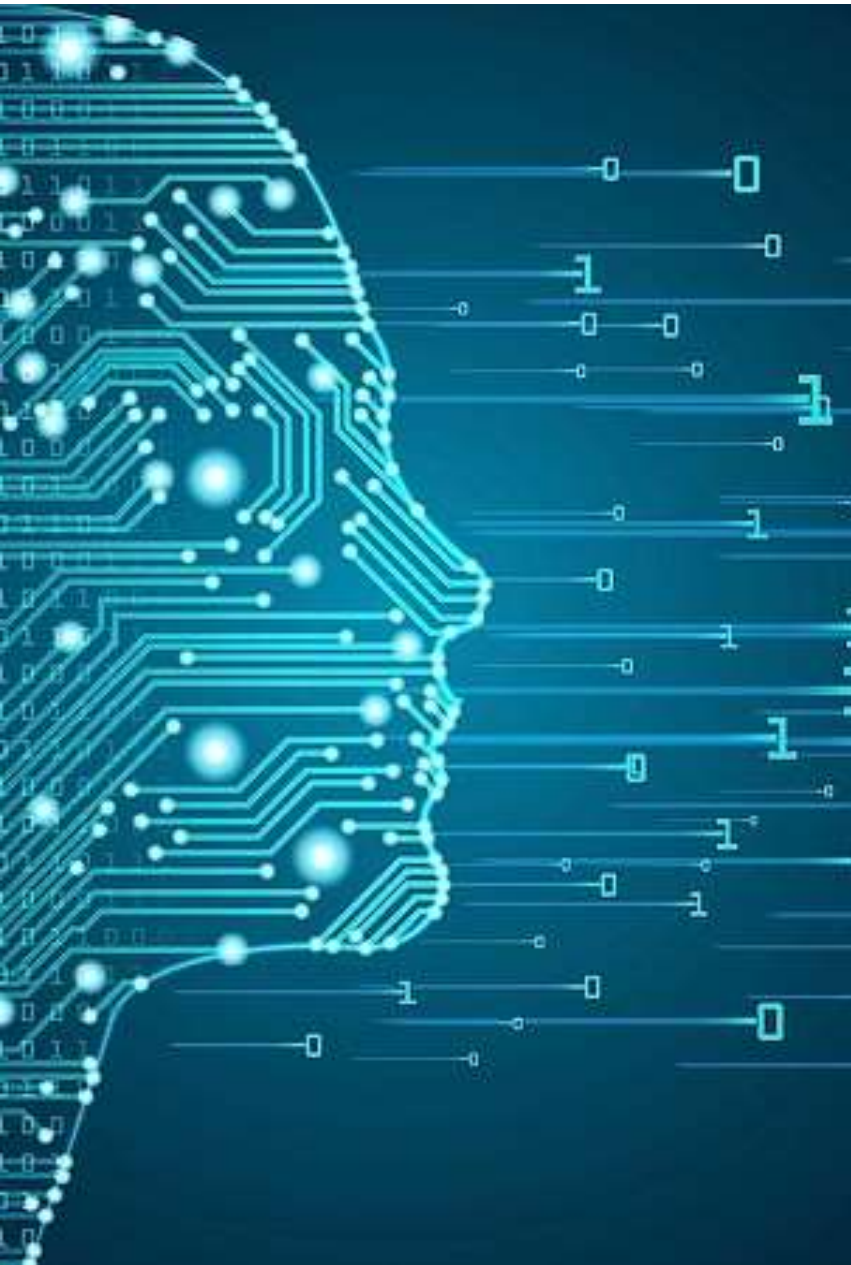
### Scientific Panel

supports with technical advice



### Advisory Forum

supports with input from stakeholders



## Toezicht op AI

AI Act establishes

- European AI Office (@ Commission)

- European AI Board for harmonised enforcement

AI Office

- Supervision over and enforcement of requirements GPAI models

- Support implementation of AI Act and support innovation

Market surveillance authorities

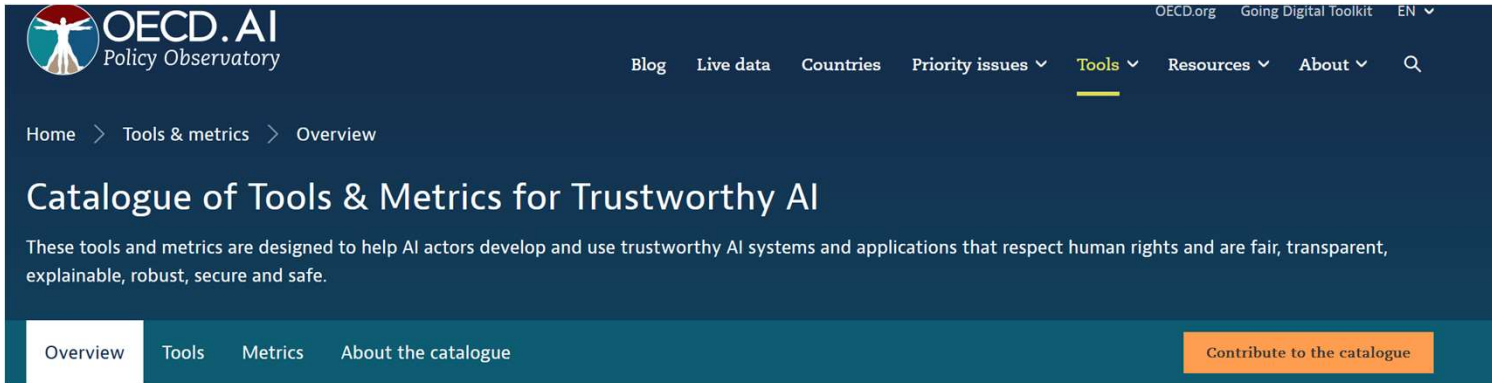
- Competences to perform market surveillance and sanction non-compliance

- Supervision over forbidden AI practices, high-risk AI systems and transparency requirements

- Represented in AI Board

- Coordination and collaboration key for effective oversight

# OECD AI Observatory:



The screenshot shows the OECD AI Observatory website. The header includes the OECD AI Policy Observatory logo, navigation links for Blog, Live data, Countries, Priority issues, Tools (highlighted), Resources, and About, and a search icon. The breadcrumb trail is Home > Tools & metrics > Overview. The main heading is 'Catalogue of Tools & Metrics for Trustworthy AI'. Below it, a paragraph states: 'These tools and metrics are designed to help AI actors develop and use trustworthy AI systems and applications that respect human rights and are fair, transparent, explainable, robust, secure and safe.' A navigation bar at the bottom of the page includes 'Overview' (selected), 'Tools', 'Metrics', and 'About the catalogue', along with a 'Contribute to the catalogue' button.

<https://oecd.ai/en/catalogue/overview>

## Why we need a catalogue of tools and metrics for trustworthy AI

There are tools and metrics out there that help AI actors to build and deploy AI systems that are trustworthy. However, these tools and metrics are often hard to find and absent from the ongoing AI policy discussions. This catalogue makes it easier to find tools and metrics by providing a one-stop-shop for helpful approaches, mechanisms and practices for trustworthy AI.



### Tools

Find a tool that fits your specific needs

> [See all tools and related use cases](#)



### Metrics

Explore metrics to evaluate how AI systems align with trustworthy AI Principles

> [See all metrics and related uses cases](#)

## Popular technical searches

- > [Technical tools to remove bias](#)
- > [Technical tools for robust and secure data collection and processing](#)
- > [Metrics to measure model performance](#)
- > [Metrics to measure privacy](#)
- > [Technical tools to audit AI systems](#)
- > [Technical tools for reskilling or upskilling](#)
- > [Metrics to measure fairness](#)

VRAGEN?

