

# Procedure file

Basic information	
<p>COD - Ordinary legislative procedure (ex-codecision procedure) Regulation</p> <p>2021/0106(COD)</p>	Awaiting Council's 1st reading position
<p>Artificial Intelligence Act</p> <p>Subject 3.30.06 Information and communication technologies, digital technologies 3.40.06 Electronics, electrotechnical industries, ICT, robotics</p> <p>Legislative priorities <a href="#">Joint Declaration 2023-24</a> <a href="#">Joint Declaration 2022</a> <a href="#">Joint Declaration 2021</a></p>	

Key players			
European Parliament	Joint Committee Responsible	Rapporteur	Appointed
	 <a href="#">Internal Market and Consumer Protection</a>		01/12/2021
	<a href="#">Civil Liberties, Justice and Home Affairs</a>	 <a href="#">BENIFEI Brando</a>	01/12/2021
		 <a href="#">TUDORACHE Dragos</a>	
		Shadow rapporteur	
		 <a href="#">CLUNE Deirdre</a>	
		 <a href="#">VOSS Axel</a>	
		 <a href="#">VITANOV Petar</a>	
		 <a href="#">HAHN Svenja</a>	
		 <a href="#">LAGODINSKY Sergey</a>	
		 <a href="#">VAN SPARRENTAK Kim</a>	
		 <a href="#">LACAPELLE Jean-Lin</a>	
		 <a href="#">MADISON Jaak</a>	
		 <a href="#">ROOKEN Rob</a>	
	 <a href="#">ZŁOTOWSKI Kosma</a>		
	 <a href="#">ERNST Cornelia</a>		



KONEČNÁ Kateřina

LIBE [Internal Market and Consumer Protection](#)[Civil Liberties, Justice and Home Affairs](#)

Committee for opinion

Rapporteur for opinion

Appointed

ENVI [Environment, Public Health and Food Safety](#)

15/09/2021

[SOLÍS PÉREZ Susana](#)ITRE [Industry, Research and Energy](#)

(Associated committee)

11/01/2022

[MAYDELL Eva](#)TRAN [Transport and Tourism](#)

04/11/2021

[CUTAJAR Josianne](#)CULT [Culture and Education](#)

(Associated committee)

13/07/2021

[KOLAJA Marcel](#)JURI [Legal Affairs](#)

(Associated committee)

10/01/2022

[VOSS Axel](#)Council of the European Union  
European Commission

Commission DG

Commissioner

[Communications Networks, Content and Technology](#)

BRETON Thierry

European Economic and  
Social Committee

## Key events

21/04/2021	Legislative proposal published	<a href="#">COM(2021)0206</a>	Summary
07/06/2021	Committee referral announced in Parliament, 1st reading		
16/12/2021	Referral to associated committees announced in Parliament		
16/12/2021	Referral to joint committee announced in Parliament		
11/05/2023	Vote in committee, 1st reading		
22/05/2023	Committee report tabled for plenary, 1st reading	<a href="#">A9-0188/2023</a>	Summary
13/06/2023	Debate in Parliament		
14/06/2023	Results of vote in Parliament		
14/06/2023	Decision by Parliament, 1st reading	<a href="#">T9-0236/2023</a>	Summary

14/06/2023	Matter referred back to the committee responsible		
13/02/2024	Approval in committee of the text agreed at 1st reading interinstitutional negotiations	<a href="#">PE758.862</a> GEDA/A/(2024)000753	
12/03/2024	Debate in Parliament		
13/03/2024	Decision by Parliament, 1st reading	<a href="#">T9-0138/2024</a>	Summary

Technical information	
Procedure reference	2021/0106(COD)
Procedure type	COD - Ordinary legislative procedure (ex-codecision procedure)
Procedure subtype	Legislation
Legislative instrument	Regulation
Legal basis	Treaty on the Functioning of the EU TFEU 016-p2; Rules of Procedure EP 57; Treaty on the Functioning of the EU TFEU 114; Rules of Procedure EP 58
Mandatory consultation of other institutions	<a href="#">European Economic and Social Committee</a>
Stage reached in procedure	Awaiting Council's 1st reading position
Committee dossier	CJ40/9/07994

Documentation gateway					
Legislative proposal		<a href="#">COM(2021)0206</a>	21/04/2021	EC	Summary
Document attached to the procedure		SEC(2021)0167	22/04/2021	EC	
Document attached to the procedure		SWD(2021)0084	22/04/2021	EC	
Document attached to the procedure		SWD(2021)0085	22/04/2021	EC	
European Central Bank: opinion, guideline, report		<a href="#">CON/2021/0040</a> <a href="#">OJ C 115 29.12.2021, p. 0005</a>	29/12/2021	ECB	
Committee draft report		<a href="#">PE731.563</a>	20/04/2022	EP	
Committee opinion	ENVI	<a href="#">PE699.056</a>	22/04/2022	EP	
Amendments tabled in committee		<a href="#">PE732.802</a>	10/06/2022	EP	
Amendments tabled in committee		<a href="#">PE732.836</a>	10/06/2022	EP	
Amendments tabled in committee		<a href="#">PE732.837</a>	10/06/2022	EP	
Amendments tabled in committee		<a href="#">PE732.838</a>	10/06/2022	EP	
Amendments tabled in committee		<a href="#">PE732.839</a>	10/06/2022	EP	
Amendments tabled in committee		<a href="#">PE732.840</a>	10/06/2022	EP	
Amendments tabled in committee		<a href="#">PE732.841</a>	10/06/2022	EP	
Amendments tabled in committee		<a href="#">PE732.843</a>	10/06/2022	EP	
Amendments tabled in committee		<a href="#">PE732.844</a>	10/06/2022	EP	
Committee opinion	ITRE	<a href="#">PE719.801</a>	14/06/2022	EP	

Committee opinion	<b>CULT</b>	<a href="#">PE719.637</a>	16/06/2022	EP	
Committee opinion	<b>TRAN</b>	<a href="#">PE730.085</a>	12/07/2022	EP	
Committee opinion	<b>JURI</b>	<a href="#">PE719.827</a>	12/09/2022	EP	
Committee report tabled for plenary, 1st reading/single reading		<a href="#">A9-0188/2023</a>	22/05/2023	EP	Summary
Text adopted by Parliament, partial vote at 1st reading/single reading		<a href="#">T9-0236/2023</a>	14/06/2023	EP	Summary
Coreper letter confirming interinstitutional agreement		GEDA/A/(2024)000753	02/02/2024	CSL	
Text agreed during interinstitutional negotiations		<a href="#">PE758.862</a>	02/02/2024	EP	
Text adopted by Parliament, 1st reading/single reading		<a href="#">T9-0138/2024</a>	13/03/2024	EP	Summary

### Additional information

Research document	<a href="#">Briefing</a>	17/11/2021
-------------------	--------------------------	------------

## Artificial Intelligence Act

**PURPOSE:** to lay down a uniform legal framework in particular for the development, marketing and use of artificial intelligence in conformity with EU values (Artificial Intelligence Act).

**PROPOSED ACT:** Regulation of the European Parliament and of the Council.

**ROLE OF THE EUROPEAN PARLIAMENT:** the European Parliament decides in accordance with the ordinary legislative procedure and on an equal footing with the Council.

**BACKGROUND:** faced with the rapid technological development of AI and a global policy context where more and more countries are investing heavily in AI, the EU must act as one to address challenges of AI. It is in the EU's interest to be a world leader in the development of human-centred, sustainable, safe, ethical and trustworthy artificial intelligence.

Some Member States have already explored the adoption of national rules to ensure that artificial intelligence is safe and is developed and used in compliance with fundamental rights obligations. Differing national rules may lead to fragmentation of the internal market and decrease legal certainty for operators that develop or use AI systems. A consistent and high level of protection throughout the EU should therefore be ensured.

Following on from the [White Paper on AI](#) - "A European Approach to Excellence and Trust", the legislative proposal aims to ensure a high and consistent level of protection across the EU.

The European Parliament [resolution](#) on a framework for ethical aspects of artificial intelligence, robotics and related technologies specifically recommends that the Commission propose legislative measures to exploit the opportunities and benefits of AI, but also to ensure the protection of ethical principles.

**CONTENT:** against this background, the Commission presents the proposed regulatory framework on Artificial Intelligence with the following specific objectives:

- ensure that AI systems placed on the Union market and used are safe and respect existing law on fundamental rights and Union values;
- ensure legal certainty to facilitate investment and innovation in AI;
- enhance governance and effective enforcement of existing law on fundamental rights and safety requirements applicable to AI systems;
- facilitate the development of a single market for lawful, safe and trustworthy AI applications and prevent market fragmentation.

In order to achieve these objectives, the proposal lays down the following:

#### Harmonised risk-based approach

The proposal sets harmonised rules for the development, placement on the market and use of AI systems in the Union following a proportionate risk-based approach. It proposes a single future-proof definition of AI.

The risk-based approach differentiates between uses of AI that create:

#### Unacceptable risk

AI systems considered a clear threat to the safety, livelihoods and rights of people will be banned. This includes AI systems or applications that manipulate human behaviour to circumvent users' free will (e.g. toys using voice assistance encouraging dangerous behaviour of minors) and systems that allow social scoring' by governments.

Specific restrictions and safeguards are proposed in relation to certain uses of remote biometric identification systems for the purpose of law enforcement.

#### High-risk

AI systems identified as high-risk include AI technology used in, inter alia:

- critical infrastructures (e.g. transport), that could put the life and health of citizens at risk;
- educational or vocational training, that may determine the access to education and professional course of someone's life (e.g. scoring of exams);
- safety components of products (e.g. AI application in robot-assisted surgery);
- law enforcement that may interfere with people's fundamental rights (e.g. evaluation of the reliability of evidence);
- migration, asylum and border control management (e.g. verification of authenticity of travel documents).

The proposal sets out the legal requirements for high-risk AI systems in relation to data and data governance, documentation and recording keeping, transparency and provision of information to users, human oversight, robustness, accuracy and security.

#### Low-risk

This proposal allows the free use of applications such as AI-enabled video games or spam filters. The vast majority of AI systems fall into this category. The draft Regulation does not intervene here, as these AI systems represent only minimal or no risk for citizens' rights or safety.

#### Governance

The Commission proposes that national competent market surveillance authorities supervise the new rules, while the creation of a European Artificial Intelligence Board will facilitate their implementation, as well as drive the development of standards for AI. In addition, voluntary codes of conduct are proposed for non-high-risk AI, as well as regulatory sandboxes to facilitate responsible innovation.

#### Market monitoring and surveillance

The Commission will be in charge of monitoring the effects of the proposal. It will establish a system for registering stand-alone high-risk AI applications in a public EU-wide database. This registration will also enable competent authorities, users and other interested people to verify if the high-risk AI system complies with the requirements laid down in the proposal and to exercise enhanced oversight over those AI systems posing high risks to fundamental rights.

Moreover, AI providers will be obliged to inform national competent authorities about serious incidents or malfunctioning that constitute a breach of fundamental rights obligations as soon as they become aware of them, as well as any recalls or withdrawals of AI systems from the market.

The Commission will publish a report evaluating and reviewing the proposed AI framework five years following the date on which it becomes applicable.

#### Budgetary implications

Member States will have to designate supervisory authorities in charge of implementing the legislative requirements. Their supervisory function could build on existing arrangements, for example regarding conformity assessment bodies or market surveillance, but would require sufficient technological expertise and human and financial resources.

## Artificial Intelligence Act

---

The Committee on the Internal Market and Consumer Protection and the Committee on Civil Liberties, Justice and Home Affairs adopted the joint report by Brando BENIFEI (S&D, IT) and Drago TUDORACHE (Renew, RO) on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts.

Given the major impact that artificial intelligence can have on society and the need to build trust, it is vital for artificial intelligence and its regulatory framework to be developed according to Union values enshrined in Article 2 TEU, the fundamental rights and freedoms enshrined in the Treaties, the Charter, and international human rights law.

#### Purpose

The purpose of the proposed regulation is to promote the uptake of human centric and trustworthy artificial intelligence and to ensure a high level of protection of health, safety, fundamental rights, democracy and rule of law and the environment from harmful effects of artificial intelligence systems in the Union. It lays down a uniform legal framework in particular for the development, the placing on the market, the putting into service and the use of artificial intelligence in conformity with Union values and ensures the free movement of AI-based goods and services cross-border, thus preventing Member States from imposing restrictions on the development, marketing and use of Artificial Intelligence systems (AI) systems, unless explicitly authorised by this Regulation. Certain AI systems can also have an impact on democracy and rule of law and the environment. These concerns are specifically addressed in the critical sectors and use cases listed in the annexes to this Regulation.

The amended text stipulates that the regulation should preserve the values of the Union facilitating the distribution of artificial intelligence benefits across society, protecting individuals, companies, democracy and rule of law and the environment from risks while boosting innovation and employment and making the Union a leader in the field.

#### General principles applicable to all AI systems

All operators covered by the Regulation should make every effort to develop and use AI or general purpose AI systems in accordance with the following general principles: (i) human agency and oversight; (ii) technical robustness and safety; (iii) privacy and data governance; (iv)

transparency; (v) diversity, non-discrimination and fairness; and (vi) social and environmental well-being.

### Scope

To support research and innovation, the regulation should not undermine research and development activity and respect freedom of scientific research. It is therefore necessary to exclude from its scope AI systems specifically developed for the sole purpose of scientific research and development and to ensure that the regulation does not otherwise affect scientific research and development activity on AI systems.

Members also added exemptions for research activities and AI components provided under open-source licenses. The new law promotes regulatory sandboxes, or controlled environments, established by public authorities to test AI before its deployment.

### AI literacy

Members stressed that when implementing the proposed regulation, the Union and the Member States should promote measures for the development of a sufficient level of AI literacy, across sectors and taking into account the different needs of groups of providers, deployers and affected persons concerned, including through education and training, skilling and reskilling programmes and while ensuring proper gender and age balance, in view of allowing a democratic control of AI systems.

### High-risk AI

Members expanded the classification of high-risk areas to include harm to peoples health, safety, fundamental rights or the environment. They also added AI systems to influence voters in political campaigns and in recommender systems used by social media platforms (with more than 45 million users under the Digital Services Act) to the high-risk list.

Members also added the following bans such as:

- real-time remote biometric identification systems in publicly accessible spaces;
- post remote biometric identification systems, with the only exception of law enforcement for the prosecution of serious crimes and only after judicial authorisation;
- biometric categorisation systems using sensitive characteristics (e.g. gender, race, ethnicity, citizenship status, religion, political orientation);
- predictive policing systems (based on profiling, location or past criminal behaviour);
- emotion recognition systems in law enforcement, border management, workplace, and educational institutions; and
- indiscriminate scraping of biometric data from social media or CCTV footage to create facial recognition databases (violating human rights and right to privacy).

### The European Artificial Intelligence Office

The proposal establishes the European Artificial Intelligence Office which should be an independent body of the Union. It is proposed that its seat be in Brussels.

It should carry out, inter alia, the following tasks:

- support, advise, and cooperate with Member States, national supervisory authorities, the Commission and other Union institutions, bodies, offices and agencies with regard to the implementation of this Regulation;
- promote public awareness and understanding of the benefits, risks, safeguards and rights and obligations in relation to the use of AI systems;
- facilitate the development of common criteria and a shared understanding among market operators and competent authorities of the relevant concepts provided for in this Regulation;
- provide monitoring of foundation models and to organise a regular dialogue with the developers of foundation models with regard to their compliance as well as AI systems that make use of such AI models.

The AI Office should be accountable to the European Parliament and to the Council; act independently and ensure a high level of transparency.

### EU database for high-risk AI systems

The amended text stressed that the Commission should, in collaboration with the Member States, set up and maintain a public EU database containing information concerning high-risk AI systems. Information contained in the EU database should be freely available to the public.

## Artificial Intelligence Act

---

The European Parliament adopted, by 499 votes to 28 with 93 abstentions, amendments to the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain Union legislative acts.

The matter was referred back to the committee responsible for inter-institutional negotiations.

### Purpose

The regulation lays down a uniform legal framework in particular for the development, the placing on the market, the putting into service and the use of artificial intelligence in conformity with Union values. Its aim is to promote the uptake of human centric and trustworthy artificial intelligence and to ensure a high level of protection of health, safety, fundamental rights, democracy and rule of law and the environment from harmful effects of artificial intelligence systems in the Union.

### Supporting innovation

To boost AI innovation and support SMEs, Members added exemptions for research activities and AI components provided under open-source

licenses. The new law promotes so-called regulatory sandboxes, or real-life environments, established by public authorities to test AI before it is deployed.

#### General principles applicable to all AI systems

All operators covered by the Regulation should make every effort to develop and use AI or general purpose AI systems in accordance with the following general principles: (i) human agency and oversight; (ii) technical robustness and safety; (iii) privacy and data governance; (iv) transparency; (v) diversity, non-discrimination and fairness; and (vi) social and environmental well-being.

#### AI literacy

When implementing the regulation, the Union and the Member States should promote measures for the development of a sufficient level of AI literacy, across sectors and taking into account the different needs of groups of providers, deployers and affected persons concerned, including through education and training, skilling and reskilling programmes and while ensuring proper gender and age balance, in view of allowing a democratic control of AI systems.

#### Prohibition of AI practices

AI systems posing an unacceptable level of risk to personal safety will be prohibited. Members expanded the list to include bans on intrusive and discriminatory uses of AI, such as:

- systems that use subliminal techniques or deliberately manipulative or deceptive techniques, with the aim of substantially distorting a persons or a group of persons behaviour by appreciably impairing the persons ability to make an informed decision, thereby causing the person to take a decision that that person would not have otherwise taken in a manner that causes or is likely to cause that person, another person or group of persons significant harm;
- systems which exploit the possible vulnerabilities of a given person or group of persons, in particular known or predictable personality traits or the social or economic situation, age, physical or mental capacity of that person or group of persons, with the aim or effect of substantially altering that person's behaviour;
- placing on the market, putting into service or use of biometric categorisation systems that categorise natural persons according to sensitive or protected attributes (e.g. gender, race, ethnic origin, citizenship status, religion, political orientation), or characteristics or based on the inference of those attributes or characteristics;
- systems used for social rating (classifying people according to their social behaviour or personality characteristics);
- the use of real-time remote biometric identification systems in publicly accessible areas;
- predictive policing systems (based on profiling, location or past criminal behaviour);
- emotion recognition systems in law enforcement, border management, the workplace, and educational institutions; and
- untargeted scraping of facial images from the internet or CCTV footage to create facial recognition databases (violating human rights and right to privacy).
- emotion recognition systems used in law enforcement, border management, the workplace and educational establishments;
- post remote biometric identification systems, with the only exception of law enforcement for the prosecution of serious crimes and only after judicial authorisation.

The following have been added to the list of high-risk systems:

- systems intended to be used as security components in the management and operation of the supply of water, gas, heating, electricity and critical digital infrastructures;
- systems intended to be used to assess the appropriate level of education of an individual and which substantially influence the level of education and vocational training from which that individual will benefit or to which he or she will have access;
- systems intended to be used to monitor and detect prohibited behaviour in students during tests in the context of, or within, education and training institutions;
- systems intended to be used to make or substantially influence decisions on the eligibility of natural persons for health and life insurance;
- systems intended to evaluate and classify emergency calls from individuals;
- AI systems intended to be used by public authorities in the management of migration, asylum and border controls to process, control and verify data for the purpose of detecting, recognising and identifying natural persons;
- systems intended to be used to influence the outcome of an election or referendum or the voting behaviour of individuals in the exercise of their vote in elections or referendums;
- AI systems used in recommender systems operated by major social media platforms.

#### Obligations for general purpose AI

Generative AI systems based on such models, like ChatGPT, would have to comply with transparency requirements (disclosing that the content was AI-generated, also helping distinguish so-called deep-fake images from real ones) and ensure safeguards against generating illegal content. Detailed summaries of the copyrighted data used for their training would also have to be made publicly available.

#### AI Office

The proposal establishes the AI Office, which should be an independent body of the Union. It is proposed that it should be based in Brussels. Its tasks should include the following:

- support, advise and cooperate with Member States, national supervisory authorities, the Commission and other Union institutions, bodies, offices or agencies on the implementation of this Regulation;

- monitor and ensure the effective and consistent application of the Regulation;
- contribute to the coordination between the national supervisory authorities responsible for the application of the Regulation;
- mediate in discussions on serious disagreements which may arise between competent authorities concerning the application of the Regulation;
- coordinate joint investigations.

The IA office should be accountable to the European Parliament and the Council, act independently and ensure a high level of transparency.

Right to lodge a complaint with a national supervisory authority

Every natural persons or groups of natural persons will have the right to lodge a complaint with a national supervisory authority if they consider that the AI system relating to him or her infringes this Regulation. Lastly, Members want to boost citizens right to file complaints about AI systems and receive explanations of decisions based on high-risk AI systems that significantly impact their fundamental rights and socio-economic well-being.

## Artificial Intelligence Act

---

The European Parliament adopted by 523 votes to 46, with 49 abstentions, a legislative resolution on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts.

The European Parliament's position adopted at first reading under the ordinary legislative procedure amends the proposal as follows:

Subject matter

The purpose of this Regulation is to improve the functioning of the internal market and promote the uptake of human-centric and trustworthy artificial intelligence (AI), while ensuring a high level of protection of health, safety, fundamental rights enshrined in the Charter of Fundamental Rights, including democracy, the rule of law and environmental protection, against the harmful effects of artificial intelligence systems (AI systems) in the Union, and to support innovation.

This Regulation does not apply to AI systems or AI models, including their output, specifically developed and put into service for the sole purpose of scientific research and development.

Regulatory sandboxes and real-world testing will have to be established at the national level, and made accessible to SMEs and start-ups, to develop and train innovative AI before its placement on the market.

This Regulation applies to AI systems released under free and open source licences, unless they are placed on the market or put into service as high-risk AI systems.

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.

Prohibited AI Practices

The new rules prohibit the following AI practices:

- AI system that deploys subliminal techniques beyond a persons consciousness or purposefully manipulative or deceptive techniques, with the objective, or the effect of, materially distorting the behaviour of a person or a group of persons by appreciably impairing their ability to make an informed decision, thereby causing a person to take a decision that that person would not have otherwise taken;
- AI system that exploits any of the vulnerabilities of a person or a specific group of persons due to their age, disability or a specific social or economic situation, with the objective, or the effect, of materially distorting the behaviour of that person;
- AI systems with social scores (classification of natural persons based on their social behaviour or known, inferred or predicted personal or personality characteristics);
- AI system for making risk assessments of natural persons in order to assess or predict the likelihood of a natural person committing a criminal offence, based solely on the profiling of a natural person or on assessing their personality traits and characteristics;
- AI systems that create or expand facial recognition databases through the untargeted scraping of facial images from the internet or CCTV footage;
- AI systems to infer emotions of a natural person in the areas of workplace and education institutions, except where the use of the AI system is intended to be put in place or into the market for medical or safety reasons;
- 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;
- real-time remote biometric identification systems in publicly accessible spaces for the purposes of law enforcement, unless and in so far as such use is strictly necessary for one of the following objectives: (i) the targeted search for specific victims of abduction, trafficking in human beings or sexual exploitation of human beings, as well as searching for missing persons; (ii) the prevention of a genuine threat of a terrorist attack; (iii) the identification of a person suspected of having committed a criminal offence, for the purpose of conducting a criminal investigation, prosecution or executing a criminal penalty for offences punishable by a custodial sentence of a maximum duration of at least four years.

The use of the real-time remote biometric identification system in publicly accessible spaces should be authorised only if the relevant law enforcement authority has completed a fundamental rights impact assessment. In addition, their use remains limited to what is strictly necessary concerning the period of time as well as the geographic and personal scope. In any case, no decision producing an adverse legal effect on a person should be taken based solely on the output of the remote biometric identification system.

#### Obligations for high-risk systems

The Regulation lays down clear obligations are also foreseen for other high-risk AI systems (due to their significant potential harm to health, safety, fundamental rights, environment, democracy and the rule of law).

The following have been added to the list of high-risk systems, in particular, systems intended to be used:

- as safety components in the management and operation of critical digital infrastructure, road traffic and the supply of water, gas, heating and electricity;
- to determine the access, admission or assignment of individuals to educational and vocational training establishments, at all levels;
- for the recruitment or selection of natural persons, in particular for publishing targeted job offers, analysing and filtering applications and evaluating candidates;
- to assess the eligibility of individuals for essential social security benefits and services, including healthcare services;
- for risk assessment and pricing of life and health insurance for individuals;
- in the context of migration, asylum and border control management, for the purposes of detecting, recognising or identifying natural persons;
- to influence the outcome of an election or referendum or the electoral behaviour of natural persons in the exercise of their vote.

Such systems must assess and reduce risks, maintain use logs, be transparent and accurate, and ensure human oversight. Citizens will have a right to submit complaints about AI systems and receive explanations about decisions based on high-risk AI systems that affect their rights.

#### General-purpose AI (GPAI)

General-purpose AI systems, and the GPAI models such as ChatGPT they are based on, must meet certain transparency requirements including compliance with EU copyright law and publishing detailed summaries of the content used for training. The more powerful GPAI models that could pose systemic risks will face additional requirements, including performing model evaluations, assessing and mitigating systemic risks, and reporting on incidents.

Additionally, artificial or manipulated images, audio or video content (deepfakes) need to be clearly labelled as such.

Transparency					
MAYDELL Eva	Rapporteur		IMCO	09/04/2024	BSA   The Software Alliance
BENIFEI Brando	Rapporteur		IMCO	20/03/2024	Bain Consultants
BENIFEI Brando	Rapporteur		IMCO	20/03/2024	Onfido
BENIFEI Brando	Rapporteur		IMCO	13/03/2024	ALLAI Netherlands
BENIFEI Brando	Rapporteur		IMCO	13/03/2024	Future of Life Institute
MAYDELL Eva	Rapporteur		IMCO	07/03/2024	Giesecke+Devrient GmbH
TUDORACHE Drago?	Rapporteur		LIBE	06/03/2024	Mexico Special Envoy for Emerging Technologies
TUDORACHE Drago?	Rapporteur		LIBE	05/03/2024	Alibaba
TUDORACHE Drago?	Rapporteur		LIBE	05/03/2024	Friedrich Naumann Foundation
MAYDELL Eva	Rapporteur		IMCO	05/03/2024	OpenAI OpCo, LLC
REPASI René	Member	15/03/2024	JEF Karlsruhe ASTA KIT		
KOKALARI	Member	06/03/2024	AI Sweden		

Arba			
GARCÍA DEL BLANCO Ibán	Member	20/02/2024	Confederación Sindical de Comisiones Obreras
GARCÍA DEL BLANCO Ibán	Member	15/02/2024	European Studies and Human Rights (Pontifical University of Salamanca, Spain)
DIDIER Geoffroy	Member	06/02/2024	IFPI Representing recording industry worldwide
GARCÍA DEL BLANCO Ibán	Member	13/12/2023	DG FORTA TV
GARCÍA DEL BLANCO Ibán	Member	08/12/2023	German Marshall Fund
WÖLKEN Tiemo	Member	28/11/2023	Bundesverband Musikindustrie e.V.
GUSMÃO José	Member	28/11/2023	Audiogest - Associação para a Gestão e Distribuição de Direitos Associação Fonográfica Portuguesa
FERBER Markus	Member	28/11/2023	Bundesverband Musikindustrie e.V. (BVMI)