Artificial Intelligence – Questions and Answers*

Brussels, 12 December 2023

Why do we need to regulate the use of Artificial Intelligence?

The potential benefits of Artificial Intelligence (AI) for our societies are manifold from improved medical care to better education. Faced with the rapid technological development of AI, the EU decided to act as one to harness these opportunities.

The EU AI Act is the world's first comprehensive AI law. It aims to address risks to health, safety and fundamental rights. The regulation also protects democracy, rule of law and the environment.

While most AI systems will pose low to no risk, certain AI systems create risks that need to be addressed to avoid undesirable outcomes.

For example, the opacity of many algorithms may create uncertainty and hamper the effective enforcement of the existing legislation on safety and fundamental rights. Responding to these challenges, legislative action was needed to ensure a well-functioning internal market for AI systems where both benefits and risks are adequately addressed.

This includes applications such as biometric identification systems or AI decisions touching on important personal interests, such as in the areas of recruitment, education, healthcare, or law enforcement.

Recent advancements in AI gave rise to ever more powerful Generative AI. So-called "general-purpose AI models" that are being integrated in numerous AI systems are becoming too important for the economy and society not to be regulated. In light of potential systemic risks, the EU puts in place effective rules and oversight.

Which risks will the new AI rules address?

The uptake of AI systems has a strong potential to bring societal benefits, economic growth and enhance EU innovation and global competitiveness. However, in certain cases, the specific characteristics of certain AI systems may create new risks related to user safety and fundamental rights. Some powerful AI models that are being widely used could even pose systemic risks.

This leads to legal uncertainty for companies and potentially slower uptake of AI technologies by businesses and citizens, due to the lack of trust. Disparate regulatory responses by national authorities would risk fragmenting the internal market.

To whom does the AI Act apply?

The legal framework will apply to both public and private actors inside and outside the EU as long as the **AI system** is placed on the Union market or its use affects people located in the EU.

It can concern both providers (e.g. a developer of a CV-screening tool) and deployers of high-risk AI systems (e.g. a bank buying this screening toolImporters of AI systems will also have to ensure that the foreign provider has already carried out the appropriate conformity assessment procedure, bears a European Conformity (CE) marking and is accompanied by the required documentation and instructions of use.

In addition, certain obligations are foreseen for providers of general-purpose AI models, including large generative AI models.

Providers of free and open-source models are exempted from most of these obligations. This exemption does not cover obligations for providers of general purpose AI models with systemic risks.

Obligations also do not apply to research, development and prototyping activities preceding the release on the market, and the regulation furthermore does not apply to AI systems that are exclusively for military, defence or national security purposes, regardless of the type of entity carrying out those activities.

What are the risk categories?

The Commission proposes a risk–based approach, with four levels of risk for AI systems, as well as an identification of risks specific to general purpose models:

- **Minimal risk**: All other AI systems can be developed and used subject to the existing legislation without additional legal obligations. The vast majority of AI systems currently used or likely to be used in the EU fall into this category. Voluntarily, providers of those systems may choose to apply the requirements for trustworthy AI and adhere to voluntary codes of conduct.
- **High-risk**: A limited number of AI systems defined in the proposal, potentially creating an adverse impact on people's safety or their fundamental rights (as protected by the EU Charter of Fundamental Rights), are considered to be high-risk. Annexed to the Act is the list of high-risk AI systems, which can be reviewed to align with the evolution of AI use cases.
- These also include safety components of products covered by sectorial Union legislation. They will always be considered high-risk when subject to third-party conformity assessment under that sectorial legislation.
- **Unacceptable risk**: A very limited set of particularly harmful uses of AI that contravene EU values because they violate fundamental rights and will therefore be banned:
  - **Social scoring** for public and private purposes;
  - **Exploitation of vulnerabilities of persons, use of subliminal techniques**;
  - **Real-time remote biometric identification in publicly accessible spaces by law enforcement**, subject to narrow exceptions (see below);
  - **Biometric categorisation** of natural persons based on biometric data to deduce or infer their race, political opinions, trade union membership, religious or philosophical beliefs or sexual orientation. Filtering of datasets based on biometric data in the area of law enforcement will still be possible;
  - **Individual predictive policing**;
  - **Emotion recognition in the workplace and education institutions,** unless for medical or safety reasons (i.e. monitoring the tiredness levels of a pilot);
  - **Untargeted scraping** of internet or CCTV for facial images to build-up or expand databases.
- **Specific Transparency risk**: For certain AI systems specific transparency requirements are imposed, for example where there is a clear risk of manipulation (e.g. via the use of chatbots). Users should be aware that they are interacting with a machine.

In addition, the AI Act considers **systemic risks** which could arise from **general-purpose AI models,** including **large generative AI models**. These can be used for a variety of tasks and are becoming the basis for many AI systems in the EU. Some of these models could carry systemic risks if they are very capable or widely used. For example, powerful models could cause serious accidents or be misused for far-reaching cyberattacks. Many individuals could be affected if a model propagates harmful biases across many applications.

How do I know whether an AI system is high-risk?

Together with a clear definition of 'high-risk', the Act sets out a solid methodology that helps identifying high-risk AI systems within the legal framework. This aims to provide legal certainty for businesses and other operators.

The risk classification is based on the intended purpose of the AI system, in line with the existing EU product safety legislation. It means that the classification of the risk depends on the function performed by the AI system and on the specific purpose and modalities for which the system is used.

Annexed to the Act is a list of use cases which are considered to be high-risk. The Commission will ensure that this list is kept up to date and relevant. Systems on the high-risk list, that perform narrow procedural tasks, improve the result of previous human activities, do not influence human decisions or do purely preparatory tasks are not considered high-risk. However, an AI system shall always be considered high-risk if it performs profiling of natural persons.

What are the obligations for providers of high-risk AI systems?

Before **placing a high-risk AI system on the EU market** or otherwise putting it into service, providers must subject it to a **conformity assessment**. This will allow them to demonstrate that

their system complies with the mandatory requirements for trustworthy AI (e.g. data quality, documentation and traceability, transparency, human oversight, accuracy, cybersecurity and robustness). This assessment has to be repeated if the system or its purpose are substantially modified.

AI systems being safety components of products covered by sectorial Union legislation will always be deemed high-risk when subject to third-party conformity assessment under that sectorial legislation. Also, for biometric systems a third-party conformity assessment is always required.

Providers of high-risk AI systems will also have to **implement quality and risk management systems** to ensure their compliance with the new requirements and minimise risks for users and affected persons, even after a product is placed on the market.

High-risk AI systems that are deployed by public authorities or entities acting on their behalf will have to be **registered in a public EU database**, unless those systems are used for law enforcement and migration. The latter will have to be registered in a non-public part of the database that will be only accessible to relevant supervisory authorities.

Market surveillance authorities will support post-market monitoring through audits and by offering providers the possibility to report on serious incidents or breaches of fundamental rights obligations of which they have become aware. Any market surveillance authority may authorise placing on the market of specific high-risk AI for exceptional reasons.

In case of a breach, the requirements will allow national authorities to have access to the information needed to investigate whether the use of the AI system complied with the law.

What are examples for high-risk use cases as defined in Annex III?

- Certain critical infrastructures for instance in the fields of road traffic and the supply of water, gas, heating and electricity;
- **Education and vocational training,** e.g. to evaluate learning outcomes and steer the learning process and monitoring of cheating;
- **Employment, workers management** and access to self-employment, e.g. to place targeted job advertisements, to analyse and filter job applications, and to evaluate candidates;
- **Access to essential private and public services** and benefits (e.g. healthcare), **creditworthiness evaluation** of natural persons, and risk assessment and pricing in relation to life and health insurance;
- Certain systems used in the fields of **law enforcement**, **border control**, administration of **justice** and **democratic processes**;
- **Evaluation and classification of emergency calls**;
- Biometric identification, categorisation and emotion recognition systems (outside the prohibited categories);
- Recommender systems of very large online platforms are not included, as they are already covered in other legislation (DMA/DSA).

How are general-purpose AI models being regulated?

General-purpose AI models, including **large generative AI** models, can be used for a variety of tasks. Individual models may be integrated into a large number of AI systems.

It is important that a provider wishing to build upon a general-purpose AI model has all the necessary information to make sure its system is safe and compliant with the AI Act.

Therefore, the AI Act obliges providers of such models to **disclose certain information to downstream system providers.** Such **transparency** enables a better understanding of these models.

Model providers additionally need to have policies in place to ensure that that they **respect copyright law** when training their models.

In addition, some of these models could pose **systemic risks**, because they are very capable or widely used.

For now, general purpose AI models that were trained using **a total computing power of more than 10^25 FLOPs** are considered to carry systemic risks, given that models trained with larger compute tend to be more powerful. The AI Office (established within the Commission) may update this threshold in light of technological advances, and may furthermore in specific cases designate other models as such based on further criteria (e.g. number of users, or the degree of autonomy of

the model).

Providers of models with systemic risks are therefore mandated to **assess and mitigate risks**, **report serious incidents**, **conduct state-of-the-art tests and model evaluations**, ensure **cybersecurity** and provide **information on the energy consumption** of their models.

For this, they are asked to **engage with the European AI Office** to draw up Codes of Conduct as the central tool to detail out the rules in cooperation with other experts. A **scientific panel** will play a central role in overseeing general-purpose AI models.

Why is 10^25 FLOPs an appropriate threshold for GPAI with systemic risks?

This threshold captures the currently most advanced GPAI models, namely OpenAI's GPT-4 and likely Google DeepMind's Gemini.

The capabilities of the models above this threshold are not yet well enough understood. They could pose systemic risks, and therefore it is reasonable to subject their providers to the additional set of obligations.

FLOP is a first proxy for model capabilities, and the exact FLOP threshold can be updated upwards or downwards by the European AI Office, e.g. in the light of progress in objectively measuring model capabilities and of developments in the computing power needed for a given performance level.

The AI Act can be amended to update the FLOP threshold (by means of a delegated act).

Is the AI Act future-proof?

The Regulation introduces different level of risks and provides clear definitions, including for GPAI.

The legislation sets result-oriented requirements for high-risk AI systems but leaves the concrete technical solutions and operationalisation primarily to industry-driven standards that will ensure that the legal framework is flexible to be adapted to different use cases and to enable new technological solutions.

In addition, the AI Act can be amended by delegated and implementing acts, including to update the FLOP threshold (delegated act), to add criteria for classifying the GPAI models as presenting systemic risks (delegated act), to amend modalities to establish regulatory sandboxes and elements of the real-world testing plan (implementing acts).

How does the AI Act regulate biometric identification?

The use of **real-time remote biometric identification in publicly accessible spaces** (i.e. facial recognition using CCTV) for law enforcement purposes is prohibited, unless used in one of the following cases:

- Law enforcement activities related to 16 specified crimes;
- Targeted search for specific victims, abduction, trafficking and sexual exploitation of human beings, and missing persons; or
- The prevention of threat to the life or physical safety of persons or response to the present or foreseeable threat of a terror attack.

The list of the 16 crimes contains:

- Terrorism;
- Trafficking in human beings;
- Sexual exploitation of children and child sexual abuse material;
- Illicit trafficking in narcotic drugs and psychotropic substances;
- Illicit trafficking in weapons, munitions and explosives;
- Murder;
- Grievous bodily injury;
- Illicit trade in human organs and tissue;
- Illicit trafficking in nuclear or radioactive materials;
- Kidnapping, illegal restraint and hostage-taking;
- Crimes within the jurisdiction of the International Criminal Court;
- Unlawful seizure of aircraft/ships;

- Rape;
- Environmental crime;
- Organised or armed robbery;
- Sabotage, participation in a criminal organisation involved in one or more crimes listed above.

Real-time remote biometric identification by law enforcement authorities would be subject to **prior authorisation by a judicial or independent administrative authority** whose decision is binding. In case of urgency, authorisation can be done within 24 hours; if the authorisation is rejected all data and output needs to be deleted.

It would need to be preceded by **prior fundamental rights impact assessment** and should be **notified to the relevant market surveillance authority and the data protection authority**. In case of urgency, the use of the system may be commenced without the registration.

Usage of AI systems for **post remote biometric identification** (identification of persons in previously collected video material) of persons under investigation requires prior authorisation by a judicial authority or an independent administrative authority, and notification of the data protection and market surveillance authority.

Why are particular rules needed for remote biometric identification?

Biometric identification can take different forms. It can be used for user authentication i.e. to unlock a smartphone or for verification/authentication at border crossings to check a person's identity against his/her travel documents (one-to-one matching).

Biometric identification could also be used remotely, for identifying people in a crowd, where for example an image of a person is checked against a database (one-to-many matching).

Accuracy of systems for facial recognition can vary significantly based on a wide range of factors, such as camera quality, light, distance, database, algorithm, and the subject's ethnicity, age or gender. The same applies for gait and voice recognition and other biometric systems. Highly advanced systems are continuously reducing their false acceptance rates.

While a 99% accuracy rate may sound good in general, it is considerably risky when the result leads to the suspicion of an innocent person. Even a 0.1% error rate is a lot if it concerns tens of thousands of people.

How do the rules protect fundamental rights?

There is already a strong protection for fundamental rights and for non-discrimination in place at EU and Member State level, but complexity and opacity of certain AI applications (‘black boxes') pose a problem.

A human-centric approach to AI means to ensure AI applications comply with fundamental rights legislation. Accountability and transparency requirements for the use of high-risk AI systems, combined with improved enforcement capacities, will ensure that legal compliance is factored in at the development stage.

Where breaches occur, such requirements will allow national authorities to have access to the information needed to investigate whether the use of AI complied with EU law.

Moreover, the AI Act requires that deployers that are bodies governed by public law or private operators providing public services and operators providing high-risk systems to conduct a fundamental rights impact assessment.

What is a fundamental rights impact assessment? Who has to conduct such an assessment, and when?

The use of a high-risk AI system may produce an impact on fundamental rights. Therefore, deployers that are bodies governed by public law or private operators providing public services, and operators providing high-risk systems shall perform an assessment of the impact on fundamental rights and notify the national authority of the results.

The assessment shall consist of a description of the deployer's processes in which the high-risk AI system will be used, of the period of time and frequency in which the high-risk AI system is intended to be used, of the categories of natural persons and groups likely to be affected by its use in the specific context, of the specific risks of harm likely to impact the affected categories of persons or group of persons, a description of the implementation of human oversight measures and of measures to be taken in case of the materialization of the risks.

If the provider already met this obligation through the data protection impact assessment, the fundamental rights impact assessment shall be conducted in conjunction with that data protection impact assessment.

How does this regulation address racial and gender bias in AI?

It is very important that AI systems **do not create or reproduce bias**. Rather, when properly designed and used, **AI systems can contribute to reduce bias and existing structural discrimination**, and thus lead to more equitable and non-discriminatory decisions (e.g. in recruitment).

The **new mandatory requirements for all high-risk AI systems will serve this purpose**. AI systems must be **technically robust** to guarantee that the technology is fit for purpose and false positive/negative results are not disproportionately affecting protected groups (e.g. racial or ethnic origin, sex, age etc.).

High-risk systems will also need to be **trained and tested with sufficiently representative datasets** to **minimise the risk of unfair biases** embedded in the model and ensure that these can be addressed through appropriate bias detection, correction and other mitigating measures.

They must also be **traceable and auditable**, ensuring that appropriate **documentation is kept**, including of the data used to train the algorithm that would be key in ex post investigations.

Compliance system before and after they are placed on the market will have to ensure these systems are **regularly monitored** and **potential risks are promptly addressed**.

When will the AI Act be fully applicable?

Following its adoption by the European Parliament and the Council, the AI Act shall enter into force on the twentieth day following that of its publication in the official Journal. It will be fully applicable 24 months after entry into force, with a graduated approach as follows:

- 6 months after entry into force, Member States shall phase out prohibited systems;
- 12 months: obligations for general purpose AI governance become applicable;
- 24 months: all rules of the AI Act become applicable including obligations for high-risk systems defined in Annex III (list of high-risk use cases);
- 36 months: obligations for high-risk systems defined in Annex II (list of Union harmonisation legislation) apply.

How will the AI Act be enforced?

Member States hold a key role in the application and enforcement of this Regulation. In this respect, each Member State should designate one or more **national competent authorities** to supervise the application and implementation, as well as carry out market surveillance activities.

To increase efficiency and to set an official point of contact with the public and other counterparts, each Member State should designate one national supervisory authority, which will also represent the country in the **European Artificial Intelligence Board**.

Additional technical expertise will be provided by an **advisory forum**, representing a balanced selection of stakeholders, including industry, start-ups, SMEs, civil society and academia.

In addition, the Commission will establish a new **European AI Office**, within the Commission, which will supervise general-purpose AI models, cooperate with the European Artificial Intelligence Board and be supported by a **scientific panel** of independent experts.

Why is a European Artificial Intelligence Board needed and what will it do?

The European Artificial Intelligence Board comprises **high-level representatives of competent national supervisory authorities**, the European Data Protection Supervisor, and the Commission. Its role is to facilitate a smooth, effective and harmonised implementation of the new AI Regulation.

The Board will issue recommendations and opinions to the Commission regarding high-risk AI systems and on other aspects relevant for the effective and uniform implementation of the new rules. Finally, it will also support standardisation activities in the area.

What are the tasks of the European AI Office?

The AI Office has as its mission to **develop Union expertise and capabilities** in the field of artificial intelligence and to contribute to the implementation of Union legislation of artificial

intelligence in a centralised structure.

In particular, the AI Office shall **enforce and supervise the new rules for general purpose AI models**. This includes drawing up codes of practice to detail out rules, its role in classifying models with systemic risks and monitoring the effective implementation and compliance with the Regulation. The latter is facilitated by the powers to request documentation, conduct model evaluations, investigate upon alerts and request providers to take corrective action.

The AI Office shall ensure coordination regarding artificial intelligence policy and collaboration between involved Union institutions, bodies and agencies as well as with experts and stakeholders. In particular, it will provide a **strong link with the scientific community** to support the enforcement, serve as international reference point for independent experts and expert organisations and facilitate exchange and collaboration with similar institutions across the globe.

What is the difference between the AI Board, AI Office, Advisory Forum and Scientific Panel of independent experts?

The **AI Board** has extended tasks in advising and assisting the Commission and the Member States.

The **AI Office** is to be established within the Commission and shall work to develop Union expertise and capabilities in the field of artificial intelligence and to contribute to the implementation of Union legislation of artificial intelligence. Particularly, the AI Office shall enforce and supervise the new rules for general purpose AI models.

The **Advisory Forum** will consist of a balanced selection of stakeholders, including industry, start-ups, SMEs, civil society and academia. It shall be established to advise and provide technical expertise to the Board and the Commission, with members appointed by the Board among stakeholders.

The **Scientific Panel of independent experts** supports the implementation and enforcement of the Regulation as regards GPAI models and systems, and the Member States would have access to the pool of experts.

What are the penalties for infringement?

When AI systems are put on the market or in use that do not respect the requirements of the Regulation, **Member States will have to lay down effective, proportionate and dissuasive penalties**, including administrative fines, in relation to infringements and communicate them to the Commission.

The Regulation sets out thresholds that need to be taken into account:

- **Up to €35m or 7%** of the total worldwide annual turnover of the preceding financial year (whichever is higher) for infringements **on prohibited practices or non-compliance** related to requirements on data;
- **Up to €15m or 3%** of the total worldwide annual turnover of the preceding financial year for **non-compliance with any of the other requirements** or obligations of the Regulation, including infringement of the rules on **general-purpose AI models**;
- **Up to €7.5m or 1.5%** of the total worldwide annual turnover of the preceding financial year for the **supply of incorrect, incomplete or misleading information** to notified bodies and national competent authorities in reply to a request;
- For each category of infringement, the threshold would be the lower of the two amounts for SMEs and the higher for other companies.

In order to harmonise national rules and practices in setting administrative fines, the **Commission, counting on the advice of the Board, will draw up guidelines**.

As EU Institutions, agencies or bodies should lead by example, they will also be subject to the rules and to possible penalties; the European Data Protection Supervisor will have the power to impose fines to them.

What can individuals do that are affected by a rule violation?

The AI Act foresees a right to lodge a complaint with a national authority. On this basis national authorities can launch market surveillance activities, following the procedures of the market surveillance regulations.

Additionally, the proposed AI Liability Directive aims to provide persons seeking compensation for damage caused by high-risk AI systems with effective means to identify potentially liable persons

and obtain relevant evidence for a damage claim. For this purpose, the proposed Directive provides for the disclosure of evidence about specific high-risk AI systems that are suspected of having caused damage.

Moreover, the revised Product Liability Directive will ensure that compensation is available to individuals who suffer death, personal injury or property damage that is caused by a defective product in the Union and clarify that AI systems and products that integrate AI systems are also covered by existing rules.

How do the voluntary codes of conduct for high-risk AI systems work?

Providers of non-high-risk applications can ensure that their AI system is trustworthy by developing their own voluntary codes of conduct or adhering to codes of conduct adopted by other representative associations.

These will apply simultaneously with the transparency obligations for certain AI systems.

The Commission will encourage industry associations and other representative organisations to adopt voluntary codes of conduct.

How do the codes of practice for general purpose AI models work?

The Commission invites providers of general-purpose AI models and other experts to jointly work on a code of practice.

Once developed and approved for this purpose, these codes can be used by the providers of general-purpose AI models to demonstrate compliance with the relevant obligations from the AI Act, following the example of the GDPR.

This is especially relevant to detail out the rules for providers of general-purpose AI model with systemic risks, to ensure future-proof and effective rules for risk assessment and mitigation as well as other obligations.

Does the AI Act contain provisions regarding environmental protection and sustainability?

The objective of the AI proposal is to address risks to safety and fundamental rights, including the fundamental right to a high-level environmental protection. Environment is also one of the explicitly mentioned and protected legal interests.

The Commission is asked to request European standardisation organisations a standardisation deliverable on reporting and documentation processes to improve AI systems resource performance, such as reduction of energy and other resources consumption of the high-risk AI system during its lifecycle, and on energy efficient development of general-purpose AI models.

Furthermore, the Commission by two years after the date of application of the Regulation and every four years thereafter, is asked to submit a report on the review of the progress on the development of standardisation deliverables on energy efficient development of general-purpose models and asses the need for further measures or actions, including binding measures or actions.

In addition, providers of general purpose AI models, which are trained on large data amounts and therefore prone to high energy consumption, are required to disclose energy consumption.

The Commission is asked to develop an appropriate methodology for this assessment.

In case of general purpose AI models with systemic risks, energy efficiency furthermore needs to be assessed.

How can the new rules support innovation?

The regulatory framework can enhance the uptake of AI in two ways. On the one hand, increasing users' trust will increase the demand for AI used by companies and public authorities. On the other hand, by increasing legal certainty and harmonising rules, AI providers will access bigger markets, with products that users and consumers appreciate and purchase. Rules will apply only where strictly needed and in a way that minimises the burden for economic operators, with a light governance structure.

The AI Act further enables the creation of **regulatory sandboxes** and **real world testing,** which provide a controlled environment to test innovative technologies for a limited time, thereby fostering innovation by companies, SMEs and start-ups in compliance with the AI Act. These, together with other measures such as the additional **Networks of AI Excellence Centres** and the **Public-Private**

Partnership on Artificial Intelligence, Data and Robotics, and access to **Digital Innovation Hubs** and **Testing and Experimentation Facilities** will help build the right framework conditions for companies to develop and deploy AI.

Real world testing of High-Risk AI systems can be conducted for a maximum of 6 months (which can be prolonged by another 6 months). Prior to testing, a plan needs to be drawn up and submitted it to the market surveillance authority, which has to approve of the plan and specific testing conditions, with default tacit approval if no answer has been given within 30 days. Testing may be subject to unannounced inspections by the authority.

Real world testing can only be conducted given specific safeguards, e.g. users of the systems under real world testing have to provide informed consent, the testing must not have any negative effect on them, outcomes need to be reversible or disregardable, and their data needs to be deleted after conclusion of the testing. Special protection is to be granted to vulnerable groups, i.e. due to their age, physical or mental disability.

Besides the AI Act, how will the EU facilitate and support innovation in AI?

The EU's approach to Artificial Intelligence is based on excellence and trust, aiming to boost research and industrial capacity while ensuring safety and the protection of fundamental rights. People and businesses should be able to enjoy the benefits of AI while feeling safe and protected. The European AI Strategy aims at making the EU a world-class hub for AI and ensuring that AI is human-centric and trustworthy. In April 2021, the Commission presented its AI package, including: (1) a review of the Coordinated Plan on Artificial Intelligence and (2) its proposal for a regulation laying down harmonised rules on AI.

With the Coordinated Plan on AI the European Commission has adopted a comprehensive strategy to promote the development and adoption of AI in Europe. It focuses on creating enabling conditions for AI development and uptake, ensuring excellence thrives from the lab to the market, increasing the trustworthiness of AI, and building strategic leadership in high-impact sectors.

The Commission aims to leverage the activities of Member States by coordinating and harmonizing their efforts, to foster a cohesive and synergistic approach towards AI development and adoption. The Commission also put in place the European AI Alliance platform, which brings together stakeholders from academia, industry, and civil society to exchange knowledge and insights on AI policies.

Moreover, the Coordinated plans foresees several measures that aim to unlock data resources, foster critical computing capacity, increase research capacities, support a European network of Testing and Experimentation Facilities (TEFS) and support SMEs through European Digital Innovation Hubs (EDIHs).

What is the international dimension of the EU's approach?

The AI Act and the Coordinated Plan on AI are part of the efforts of the European Union to be a global leader in the promotion of trustworthy AI at international level. AI has become an area of strategic importance at the crossroads of geopolitics, commercial stakes and security concerns.

Countries around the world are choosing to use AI as a way to signal their desires for technical advancement due to its utility and potential. AI regulation is only emerging and the EU will take actions to foster the setting of global AI standards in close collaboration with international partners in line with the rules-based multilateral system and the values it upholds. The EU intends to deepen partnerships, coalitions and alliances with EU partners (e.g. Japan, the US, India, Canada, South Korea, Singapore, or the Latin American and Caribbean region) as well as multilateral (e.g. OECD, G7 and G20) and regional organisations (e.g. Council of Europe).

**Updated on 14/12/2023*

QANDA/21/1683

Press contacts:

Johannes BAHRKE (+32 2 295 86 15)
Thomas Regnier (+32 2 29 9 1099)

General public inquiries: Europe Direct by phone 00 800 67 89 10 11 or by email