# New Rules for Artificial Intelligence – Questions and Answers

13 December 2023

Following the political approval of the European Union ("EU") artificial intelligence ("AI") act on Friday 8th December 2023 (covered here), certain questions remain regarding the consequences. In this document we provide answers to key questions to help provide further guidance.

## Why did the European Commission need to regulate the use of artificial intelligence?

The potential advantages of Artificial Intelligence ("AI") for societies are diverse, ranging from enhanced medical care to improved education. In response to the swift technological progress in AI, the European Union ("EU") has chosen to unite in order to leverage these opportunities.

The EU EU AI Act (the "Act" or "Regulation") represents the world's inaugural comprehensive AI legislation. Its primary objective is to tackle risks related to health, safety, and fundamental rights. The regulation also safeguards democracy, the rule of law, and the environment.

While the majority of AI systems present minimal to no risk, specific AI systems introduce risks that must be managed to prevent undesirable outcomes. An example of such risk is the lack of transparency in many algorithms, which can create uncertainty and impede the effective enforcement of existing laws on safety and fundamental rights. In response to these challenges, legislative measures were deemed necessary to establish a well-functioning internal market for AI systems, ensuring that both benefits and risks are appropriately addressed.

This encompasses applications like biometric identification systems or AI decisions that impact crucial personal interests in areas such as recruitment, education, healthcare, or law enforcement.

The recent progress in AI has given rise to increasingly powerful Generative AI. These "general-purpose AI models," integrated into numerous AI systems, have become too significant for the economy and society to remain unregulated. Recognizing the potential systemic risks, the EU has implemented effective rules and oversight to manage this development.

## Which risks do the new AI rules address?

The adoption of AI systems holds significant promise for delivering societal benefits, fostering economic growth, and boosting innovation and global competitiveness within the European Union (EU). Nevertheless, certain AI systems with distinct characteristics may introduce new risks concerning user safety and fundamental rights. Some highly influential AI models currently in widespread use may even present potential systemic risks.

This situation contributes to legal uncertainty for companies and has the potential to hinder the adoption of AI technologies by businesses and citizens due to a lack of trust. The absence of uniform regulations across national authorities poses a risk of fragmenting the internal market, as disparate regulatory responses could emerge.

## Who does the EU EU AI Act apply to?

The legal framework is applicable to both public and private entities, whether within or outside the EU, provided that the AI system is placed on the Union market or its use impacts individuals within the EU. This applies to both providers, such as developers of tools like CV-screening software, and deployers of high-risk AI systems, like a bank purchasing such a screening tool. However, it excludes private, non-professional uses.

Importers of AI systems are also required to ensure that the foreign provider has completed the necessary conformity assessment procedure, bears a European Conformity (CE) marking, and is accompanied by the required documentation and usage instructions.

Moreover, specific obligations are outlined 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. The obligations also do not extend to research, development, and prototyping activities conducted before the market release. Furthermore, the regulation does not apply to AI systems exclusively intended for military, defence, or national security purposes, irrespective of the entity conducting these activities.

## What are the risk categories?

The Commission introduces a risk-based approach encompassing four levels to govern AI systems:

- **Minimal risk**: This category includes all AI systems that can be developed and used within the existing legal framework without additional obligations. The majority of AI systems currently in use within the EU fall into this classification. Providers of such systems may voluntarily choose to adhere to the requirements for trustworthy AI and voluntary codes of conduct.

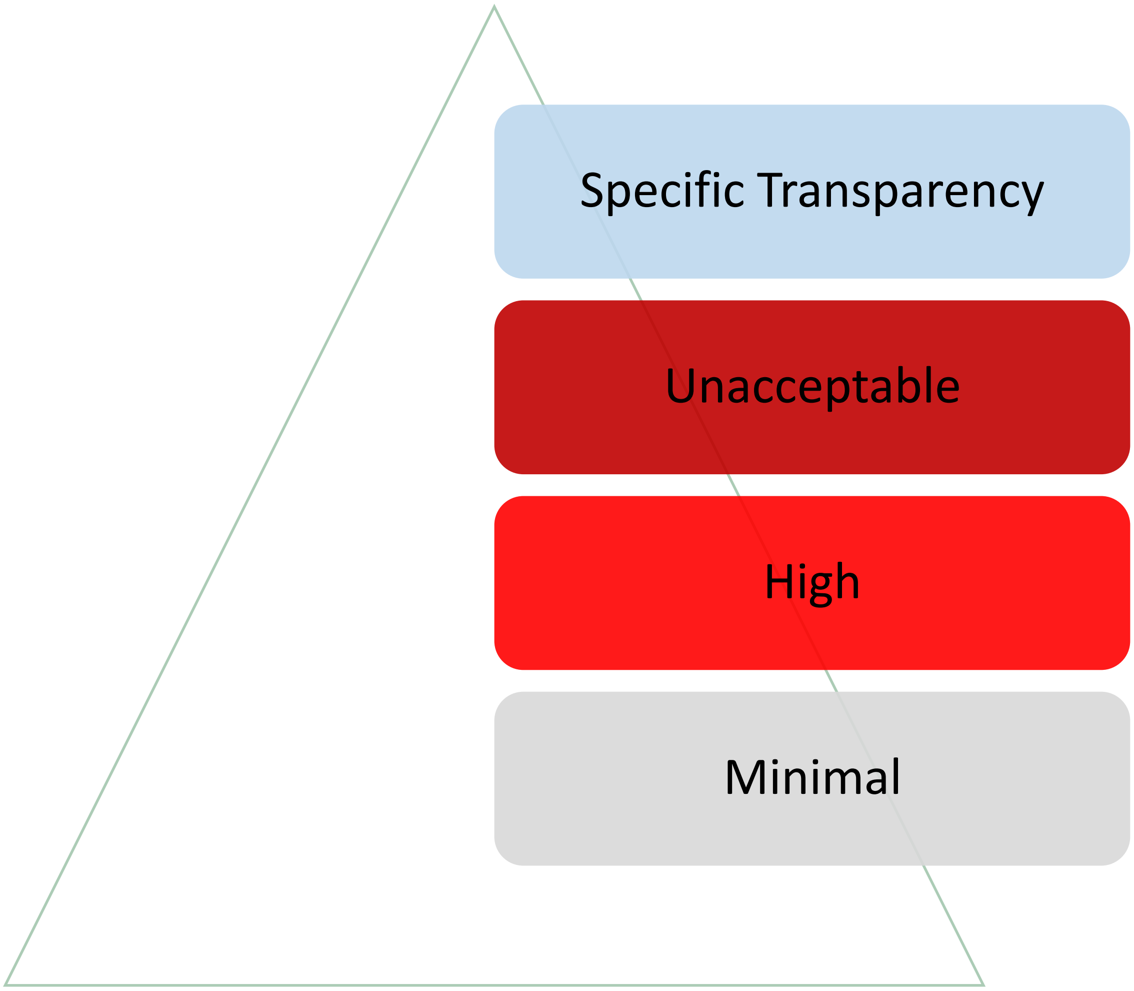
- **High-risk**: The proposal identifies a limited number of AI systems with the potential to adversely impact people's safety or fundamental rights as high-risk. The Act includes an annex listing high-risk AI systems, which may be periodically reviewed to align with evolving AI use cases. This category encompasses safety components of products covered by sector-specific Union legislation, remaining high-risk when subjected to third-party conformity assessment under that legislation.

- **Unacceptable risk**: This category encompasses a highly restricted set of particularly harmful AI uses that violate EU values by contravening fundamental rights. The following uses are banned:

    - Social scoring for public and private purposes.

    - Exploitation of vulnerabilities of individuals and the use of subliminal techniques.

  - Real-time remote biometric identification in publicly accessible spaces by law enforcement, with narrow exceptions.
  - Biometric categorization of individuals based on data inferring race, political opinions, trade union membership, religious or philosophical beliefs, or sexual orientation, unless used to identify victims. Filtering datasets based on biometric data in law enforcement is still possible.
  - Individual predictive policing.
  - Emotion recognition in workplaces and educational institutions, except for medical or safety reasons.
  - Untargeted scraping of the internet or CCTV for facial images to build or expand databases.
- **Specific Transparency risk**: Certain AI systems are subject to specific transparency requirements, particularly where there is a clear risk of manipulation (e.g., through the use of chatbots). Users should be informed when they are interacting with a machine.



Additionally, the EU AI Act addresses systemic risks that may arise from general-purpose AI models, including large generative AI models. These models, capable of various tasks, form the basis for many AI systems in the EU. The Act acknowledges the potential for systemic risks, such as serious accidents or widespread cyberattacks, associated with highly capable or widely used models. The propagation of harmful biases across multiple applications could impact numerous individuals.

## When is a AI system considered high-risk?

In conjunction with a clear definition of 'high-risk,' the Commission introduces a robust methodology designed to facilitate the identification of high-risk AI systems within the legal framework. The primary objective is to offer legal certainty to businesses and other operators.

The classification of risk is grounded in the intended purpose of the AI system, aligning with existing EU product safety legislation. This implies that the risk categorization depends on the function performed by the AI system and the specific purpose and modalities for its use.

The Act includes an annex listing use cases deemed high-risk. The Commission commits to maintaining the relevance and currency of this list. Systems on the high-risk list that engage in narrow procedural tasks, enhance the outcomes of prior human activities, do not influence human decisions, or exclusively perform preparatory tasks are exempt from the high-risk designation. However, an AI system is consistently deemed high-risk if it engages in the profiling of natural persons.

## What obligations apply to high-risk AI systems?

Prior to introducing a high-risk AI system to the EU market or putting it into operation, providers are mandated to undergo a conformity assessment. This process is essential for demonstrating that their system aligns with the mandatory requirements for trustworthy AI, encompassing aspects such as data quality, documentation and traceability, transparency, human oversight, accuracy, cybersecurity, and robustness. This assessment must be repeated in cases where the system or its intended purpose undergoes substantial modifications.

AI systems designated as safety components within products covered by sector-specific Union legislation will consistently be classified as high-risk when subjected to third-party conformity assessments under that legislation. Additionally, third-party conformity assessments are universally required for biometric systems.

Providers of high-risk AI systems are further obligated to establish quality and risk management systems to ensure ongoing compliance with the new requirements and to minimize risks for users and affected individuals, even post-market placement.

High-risk AI systems employed by public authorities or entities acting on their behalf must be registered in a public EU database, unless deployed for law enforcement and migration purposes. In such cases, registration must occur in a non-public segment of the database accessible solely to relevant supervisory authorities.

Market surveillance authorities will play a role in post-market monitoring through audits and by providing providers with the option to report serious incidents or breaches of fundamental rights obligations that come to their attention. Any market surveillance authority may grant authorization for placing specific high-risk AI on the market for exceptional reasons. In the event of a breach, the established requirements empower national authorities to access the necessary information to investigate whether the use of the AI system aligns with the law.

## What are examples of high-risk AI systems?

- 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 thelearning process and monitoring of cheating;
- Employment, workers management and access to self-employment, e.g. to place targetedjob 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 tolife and health insurance;
- Certain systems used in the fields of law enforcement, border control, administration ofjustice and democratic processes;
- Evaluation and classification of emergency calls
- Biometric identification, categorisation and emotion recognition systems.
- 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, have the capacity to perform a diverse array of tasks and can be integrated into numerous AI systems. When a provider seeks to build upon such a general-purpose AI model, it is crucial to possess all the necessary information to ensure the safety and compliance of their system with the EU AI Act.

As per the EU AI Act, providers of these models are obliged to disclose specific information to downstream system providers, fostering transparency and enhancing the understanding of these models. Additionally, model providers must implement policies to uphold copyright laws while training their models.

Moreover, certain general-purpose AI models carry potential systemic risks due to their significant capabilities or widespread use. Currently, models trained with a total computing power exceeding 10^25 FLOPs are deemed to pose systemic risks, as larger compute-trained models tend to be more powerful. The AI Office reserves the right to update this threshold in response to technological advancements and may designate other models with systemic risks based on additional criteria such as the number of users or the autonomy of the model.

Providers of models identified with systemic risks are mandated to assess and mitigate these 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. To achieve this, they are encouraged to collaborate with the European AI Office in developing Codes of Conduct as a central tool for detailing the rules in coordination with other experts. Oversight of general-purpose AI models will be entrusted to a scientific panel.

## Why is 10^25 FLOPs a viable 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 additonal 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.

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

## How resilient is the EU EU AI Act?

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 future proof to enable new technological solutions.

In addition, the EU 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 systemic risk (delegated act), to amend modalities to establish regulatory sandboxes and elements of the real-world testing plan (implementing acts).

## How is biometric identification regulated under the EU EU AI Act?

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. In case of urgency, the use of the system may be commenced without the registration.

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.

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 specific rules needed for remote biometric identification?

Biometric identification can take different forms. It can be used for user authentication i.e. to lock 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 are fundamental rights safeguarded under the EU EU AI Act?

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 EU 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 an obligation 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 deployers 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 the EU EU AI Act account for 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 dataset 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 EU EU AI Act be fully applicable?

Following its adoption by the European Parliament and the Council, the EU 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 face out prohibited systems;
- **12 months**: obligations for general purpose AI governance become applicable;
- **24 months**: all rules of the EU AI Act become applicable including obligations for high-risks systems defined in Annex III (list of high-risk use cases);
- **36 months**: obligations for high-risks systems defined in Annex II (list of Union harmonisation legislation) apply-.

## How will the EU EU 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, 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 required and what will it undertake?

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 responsibilities 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 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 are the differences between the different AI governance entities?

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, startups, 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 non-compliance?

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 EU 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 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 proposal for a Product Liability Directive would ensure that compensation is available to individuals who suffers 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 function?

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 function?

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

Once developed and approved, these codes can be used by the providers of general-purpose AI models to demonstrate compliance with the relevant obligations from the EU 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 EU EU 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 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 help 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 EU EU 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 EU AI Act. These, together with other measures such as the additional Networks of AI Excellence Centres and the PublicPrivate 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.

## Other than the EU EU 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 aspect of the EU's approach?

The proposal for regulatory framework 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, Canda, South Korea, Singapore, or the Latin American and Carribean region) as well as multilateral (e.g. OECD, G7 and G20) and regional organisations (e.g. Council of Europe).

EU AI Act – Advisory | Consultancy | Compliance Software
+31 6 57285579 and +44(0)75 35994 132
s.musch@ai-and-partners.com and m.borrelli@ai-and-partners.com
https://www.ai-and-partners.com/
https://twitter.com/AI_and_Partners @AI_and_Partners
https://www.linkedin.com/company/ai-&-partners/