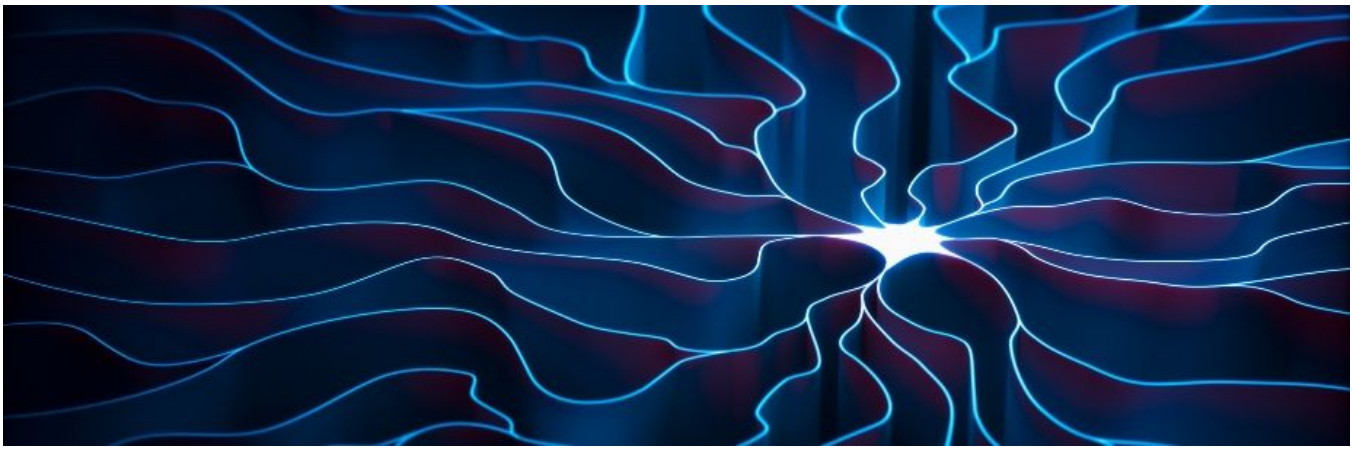

UNITED KINGDOM

EU AI Act - Questions and Answers

PUBLICATION · 07 JUL 2025

Last updated in July 2025

We’re pleased to share our updated Questions & Answers on the EU AI Act—a practical resource designed to help businesses navigate this landmark regulation with clarity and confidence.

The AI Act Q&A breaks down the Act’s key objectives, obligations, and compliance measures from a business perspective. Whether you're a provider, deployer, or other stakeholder, this guide helps you understand what the AI Act means for your role—and how to prepare.

It also explores:

- Risk management strategies and internal governance
- Sector-specific requirements in areas like healthcare, finance, and law enforcement
- International and territorial implications for global operations
- Targeted insights for Legal, Risk, and Compliance teams

Whether you're just getting started or refining your compliance roadmap, the AIA Q&A is your go-to reference for aligning innovation with regulation.

Should you have any further questions on the AI Act or any other feedback, please contact any of the Key Contacts listed on this page.

Please note that the legal position is subject to regular change; the following information reflects the current status. It is advisable to review the information with regard to any changes in the legal situation that may have taken place.

Key Objectives and Scope of the AI Act

1. What are the key objectives of the AI Act, and how do they align with our business goals?

The AI Act aims to establish a harmonized legal framework for the development, marketing, and use of

AI systems within the EU. Its key objectives include:

- **Promoting trustworthy and human-centric AI.** The AI Act seeks to ensure that AI systems are developed and used in a manner that is trustworthy and centred around human values. This aligns with business goals that prioritize ethical practices and customer trust;
- **Protecting fundamental rights and safety**. The Act aims to protect fundamental rights, health, safety, democracy, and the environment from potential harmful effects of AI. For businesses, this means ensuring that AI systems do not infringe on individual rights or pose safety risks, thereby maintaining a positive public image and avoiding legal liabilities;
- **Supporting innovation.** While ensuring safety and rights protection, the AI Act also promotes innovation within the EU. This aligns with business goals of leveraging cutting-edge AI technologies to drive growth and competitiveness;
- **Preventing market fragmentation**. By establishing uniform rules across the EU, the AI Act helps prevent EU market fragmentation, making it easier for businesses to operate across different member states without facing significantly varying regulations.

2. How does the AI Act classify AI systems based on risk, and which category do our AI systems fall into?

The AI Act adopts a risk-based framework to regulate AI systems, aiming to balance innovation with the protection of fundamental rights and safety. This framework categorizes AI systems into distinct risk levels, each subject to specific regulatory requirements:

- **Unacceptable Risk**: AI systems that pose a clear threat to health, safety or fundamental rights are prohibited. Examples include systems that deploy subliminal techniques to manipulate behavior, exploit vulnerabilities of specific groups, enable social scoring or emotion recognition at the workplace;
- **High Risk**: These systems significantly impact health, safety, or fundamental rights. They encompass areas such as biometric identification, critical infrastructure management, educational and vocational training, employment, essential private and public services, law enforcement, migration, asylum, border control management, and administration of justice. High-risk systems are subject to stringent obligations, including rigorous conformity assessments, quality management systems, and continuous monitoring;
- **Limited Risk**: AI systems with limited risk, e.g. chatbots must disclose that users are interacting with an AI system, ensuring informed user consent;
- **Minimal or No Risk**: This category includes AI systems like spam filters or AI-enabled video games, which pose minimal risk and are permitted without any regulatory intervention.

To determine the specific category applicable to your AI systems, a thorough assessment of their intended use, operational context, and potential impact on individuals and society is essential. Particularly, if your systems are utilized in areas outlined in Annex III of the AI Act, they may be classified as high-risk, necessitating compliance with the corresponding regulatory requirements.

AI Literacy and Governance under the AI Act

3. What does the AI Act regulate in terms of AI literacy and governance, and what is the impact on businesses?

Under Article 4 of the AI Act, providers and deployers of AI systems are obliged to ensure *AI literacy* of

their staff and other persons dealing with the operation and use of AI systems on their behalf. This should be done by taking into account technical knowledge, experience, education and training. As such, there is not a “one size fits all” as the sufficient level of knowledge will vary across different roles, AI systems and sectors.

AI governance should include a framework of policies, processes, and practices that guide responsible development, deployment, and use of AI systems.

With respect to high-risk AI systems which make use of techniques involving the training of AI models with data, Article 10 of the AI Act i.a. prescribes that these shall be developed on the basis of training, validation and testing data sets that meet the following quality criteria:

i. data governance and management practices appropriate for the intended purpose of the high-risk AI system;
ii. relevance, sufficiently representative, and to the best extent possible, free of errors and complete in view of the intended purpose;
iii. appropriate statistical properties, including, where applicable, as regards the persons or groups of persons in relation to whom the high-risk AI system is intended to be used.

4. What kind of internal governance structures and training concepts are recommended to ensure compliance with the AI Act?

A practical and legally sound approach to ensure compliance with the AI Act is the **three-pillar model**, which ensures the promotion of AI literacy, established compliance, and embeds accountability across the organization.

Pillar 1 – AI Literacy

The first pillar focuses on equipping employees with the knowledge and skills needed to use AI systems responsibly. AI literacy is the foundation for all further compliance efforts—it enables staff to understand how AI works, assess risks, and apply the technology lawfully and ethically in their roles. The level of knowledge required varies depending on the function, risk exposure, and complexity of the AI systems used.

This includes:

- Modular, role-specific training programs covering technical, legal, and ethical aspects of AI.
- A baseline understanding for all staff, from marketing to legal to development.
- Ongoing upskilling to adapt to evolving technologies and regulatory changes.

Pillar 2 – Legal Compliance

The second pillar ensures that the company’s use of AI systems adheres to all relevant legal requirements. The AI Act introduces a risk-based classification of AI systems and imposes different obligations depending on their risk level. In addition, companies must consider overlapping laws such as GDPR, anti-discrimination law, and IT security regulations.

This includes:

- Risk classification of each AI system based on AI Act criteria.
- Fulfillment of obligations such as transparency, documentation, and accountability.
- Legal assessments of AI use cases and alignment with applicable EU and national law.

Pillar 3 – Organizational Measures

The thrid pillar translates compliance into operational reality by establishing internal rules, responsibilities, and monitoring processes. Even though the AI Act does not mandate an AI Officer assigning central responsibility for coordination is highly recommended to ensure consistency and oversight.

This includes:

- Internal AI policies defining permitted use, approval procedures, and documentation requirements.
- Clear allocation of responsibilities, escalation paths, and compliance oversight.
- Optionally appointing an AI Officer to coordinate governance, training, and risk management.

5. What does “AI literacy” mean under Article 4 of the AI Act?

AI is the ability of a machine to display human-like capabilities such as reasoning, learning, planning and creativity.

AI enables technical systems to perceive their environment, deal with what they perceive, solve problems and act to achieve a specific goal. The computer receives data - already prepared or gathered through its own sensors such as a camera - processes it and responds.

AI systems are capable of adapting their behaviour to a certain degree by analysing the effects of previous actions and working autonomously.

AI however does not possess human intelligence - it can only provide outputs influencing human environment based on predictions, content, recommendations, or decisions.

- How AI Works (At a High Level)
  - **Algorithms**: Set of rules the system follows to make decisions.
  - **Training Data:** AI learns from large datasets – what you feed it matters.
  - **Machine Learning**: A common approach where systems improve performance based on past data, applying discovered patterns to future unseen data.
  - **Neural Network**s: A model inspired by the brain, used in tasks like language and vision.
- Strengths and Limitations
  - **Strengths**: Speed, scale, pattern recognition.
  - **Weaknesses**: Bias in data, lack of common sense, inability to explain its reasoning in a way for humans to understand.
- Biases, Ethics, and Fairness
  - AI can inherit or amplify biases from the training data it has received.
  - This may result in unintended discrimination or other unwanted results.
  - For AI to be used ethically, oversight, accountability, and inclusion is needed in all parts of the system’s lifecycle.
- Interaction between AI and Humans
  - Have knowledge in when AI is involved in processes.
  - Understand the importance of having a human person “in-the-loop", meaning that there is someone supervising and providing oversight.
- Security and Privacy
  - AI systems often collect personal data and other sensitive information.
  - Understand the pitfalls of this, and how this collection of data may impact privacy regulations and the protection of confidential information.
- Critical Thinking in Procurement

- Make sure to ask the following questions before engaging with AI.
- Who built the system?
- Why did they build it?
- What data was it trained on?
- What are the consequences if something goes wrong? Literacy

6. How can businesses practically implement AI literacy in their organization?

Needs and Requirements

- AI literacy practices should take into account technical knowledge, experience, education and training. As such, there is not a “one size fits all” as the sufficient level of knowledge will vary across different roles, AI systems and sectors.
- Appoint a cross-functional working group to map current AI usage across the organization. Assess how each department applies AI and the potential implications of its use. Develop a competency matrix that outlines departmental responsibilities and skill requirements. This matrix provides a clear overview of training needs, helping to prioritize and tailor AI literacy efforts across the company
- Implement AI literacy education as a part of the onboarding process, make sure that new hires get a basic understanding of how AI is used in the company and what consequences this entails.
- Deploy regular education programs about the use of AI in the company, tailored to different departments or professions. Baseline AI literacy should be mandatory and can be tested using self-assessment surveys. These surveys should serve the purpose of ensuring that all employees have a basic understanding of the tools they use, and the risks associated with them. When evaluating results, common misunderstandings or pitfalls should be identified and addressed more rigorously in future training. When developing educational material, introduce workshops with all parts of the workforce, making sure no important perspectives are lost between the cracks in the process. Make sure to include all levels of management, they translate policy into daily practice, transforming AI governance from an abstract corporate guideline into concrete ways of ingraining AI literacy into the company culture.
- Document everything, this will save time, money and effort the day an audit takes place.
- Develop an AI policy that covers the rules on how employees of the company should use and not use AI in their daily duties. This policy may cover, amongst other things:
  - why the policy exists and who it applies to;
  - definitions;
  - whether it applies differently to in-house tools and third-party tools;
  - acceptable use;
  - ethical use;
  - accountability;
  - monitoring;
  - rules on bias, inclusion, and fairness;
  - what one needs to consider before deploying AI as a tool;
  - how use of AI may impact different stakeholders;
  - rules on human oversight;
  - rules on procurement and vendor selection;
  - considerations on data privacy and security; and
  - clear rules on how to report AI-related incidents as well as how to respond to them.

Although this answer is mainly about regulatory matters, do not forget to highlight how AI can be of

benefit for the company, suggest use-cases and evaluate productivity to further the organization's goals. Introduce courses or educational material that helps employees understand the strengths and weaknesses of the usage of AI tools in their day-to-day tasks.

7. Is there a requirement to appoint an AI Officer, and how does this relate to AI literacy and compliance?

While the AI Act does not explicitly require the appointment of an AI Officer, it is strongly recommended as a best-practice measure to ensure effective compliance and operational clarity. The AI Officer plays a central role in bridging knowledge, responsibility, and oversight.

- Key functions of an AI Officer include:
- Coordinating compliance efforts related to internal AI policies and legal requirements.
- Supervising training and upskilling to ensure employees meet the AI literacy standards required by Article 4 of the AI Act.
- Serving as a central point of contact between management, legal, IT, and development teams.
- Monitoring AI usage to ensure ethical, safe, and compliant deployment.
- Supporting documentation, reporting, and audit processes in the event of inspections or liability concerns.

Obligations for Providers and Deployers

8. What are the specific obligations for providers of high-risk AI systems under the AI Act?

Providers must ensure that their high-risk AI systems comply with all requirements set out within the AI Act, particularly those in Section 2 of Chapter III (Article 8 et seq. AI Act). This includes requirements related to risk management, data quality, technical documentation, transparency, human oversight, robustness, accuracy, cybersecurity, and accessibility. These obligations are designed to ensure that high-risk AI systems are safe, transparent, and respect fundamental rights throughout their lifecycle, from development to deployment and beyond.

Registered trade name: Providers of high-risk AI systems shall indicate on the high-risk AI system or, where that is not possible, on its packaging or its accompanying documentation, as applicable, their name, registered trade name or registered trade mark, the address at which they can be contacted

Quality Management System: Providers must implement and maintain a documented quality management system. This system must cover regulatory compliance strategies, design and development procedures, quality control, data management, post-market monitoring, reporting of incidents, record-keeping, resource management, and accountability frameworks. The system must be proportionate to the provider’s size and the risks involved.

Technical Documentation: Before placing a high-risk AI system on the market or putting it into service, providers must prepare and keep up-to-date technical documentation. This documentation must demonstrate compliance with the AI Act’s requirements and provide all necessary information for national authorities and notified bodies to assess compliance. For SMEs and start-ups, a simplified documentation form is available.

Instructions for Use: High-risk AI systems must be accompanied by clear, complete, and accessible

instructions for use. These instructions should include information on system capabilities, limitations, intended and precluded uses, human oversight measures, maintenance, and logging mechanisms.

Risk Management System: Providers must establish, implement, document, and maintain a continuous risk management system throughout the AI system's lifecycle. This system must identify, analyze, estimate, and evaluate known and foreseeable risks, including those arising from misuse, and adopt appropriate mitigation measures.

Data and Data Governance: For AI systems using data-driven techniques, providers must ensure that training, validation, and testing datasets meet quality criteria, are relevant, representative, and free from bias as much as possible. Data governance practices must be appropriate for the intended purpose.

Human Oversight: Providers must design and develop high-risk AI systems to allow effective human oversight. This includes enabling natural persons to understand, monitor, and, if necessary, override or halt the system's operation to prevent or minimize risks.

Robustness, Accuracy, and Cybersecurity: High-risk AI systems must be robust, accurate, and secure against errors, faults, and malicious attacks. Providers must implement technical and organizational measures to ensure resilience, including protection against data poisoning, adversarial attacks, and other AI-specific vulnerabilities.

Conformity Assessment: Before placing a high-risk AI system on the market or putting it into service, providers must ensure the system undergoes the appropriate conformity assessment procedure. This may involve internal control or, in some cases, third-party assessment by a notified body. Providers must draw up an EU declaration of conformity and affix the CE marking.

Registration in the EU Database: Providers must register themselves and their high-risk AI systems in the EU database before market placement or use, except for certain systems (e.g., those used in law enforcement or critical infrastructure, which may have different registration requirements).

Post-Market Monitoring: Providers must establish and document a post-market monitoring system to collect and analyze data on the system's performance throughout its lifecycle. This is to ensure ongoing compliance and to identify and address emerging risks.

Reporting Serious Incidents: Providers must report any serious incidents or malfunctions that result in death, serious harm, disruption of critical infrastructure, or infringement of fundamental rights to the relevant market surveillance authorities without undue delay.

Cooperation with Authorities: Providers must cooperate with competent authorities, providing all necessary information and documentation to demonstrate compliance, including access to logs and technical documentation upon request.

Corrective Actions: If a provider becomes aware that a high-risk AI system is not in conformity with the AI Act, they must immediately take corrective actions, which may include withdrawing, disabling, or recalling the system, and informing relevant parties.

Appointment of an Authorised Representative (for non-EU providers): Providers established outside the EU must appoint an authorised representative within the EU before making their high-risk AI systems available in the Union. The representative acts as a contact point for authorities and ensures compliance.

Accessibility: Providers must ensure that high-risk AI systems comply with EU accessibility requirements, ensuring equal access for persons with disabilities.

Record-Keeping: Providers must keep all relevant documentation, including technical documentation, conformity assessment records, and logs, for at least 10 years after the system is placed on the market or put into service.

Information Sharing Along the Value Chain: Providers must cooperate with other parties in the AI value chain, sharing necessary information, technical access, and assistance to ensure compliance, while protecting intellectual property and trade secrets.

The obligations related to high-risk AI systems will come into force 2 August 2026 regarding annex III and 2 August 2027 regarding annex I. High-risk AI Systems intended for government use need to comply with the AI Act by 2 August 2030.

9. How can we ensure that our AI systems comply with the transparency obligations outlined in the AI Act?

The EU AI Act aims to create a trustworthy and transparent ecosystem for AI technologies. Transparency in AI means that systems should be designed and used in a way that allows their processes to be tracked and easily understood. The key part is informing users that they are interacting with AI, explaining how the system work like, and making sure that people know their rights when affected by AI. This helps both businesses and individuals understand how AI systems are designed and used, while also encouraging responsible development and use of AI.

To ensure that your AI systems comply with the transparency obligations outlined in the AI Act, follow these key steps:

1. Understand Your Role:

The starting point is to identify your role in the chain (provider, deployer, importer etc.) as well as the categories of AI systems you accordingly produce, use in professional activity or place in the market.

2. Implement Transparency Measures:

- **Notification and Information:** Clearly inform users that they are interacting with an AI system. For example, if you deploy AI for emotion recognition or biometric categorization, inform individuals exposed to the system about its operation through disclaimers, notifications, labels, or other forms of communication.
- **Marking of AI Content:** Ensure that AI-created synthetic content is marked as artificially generated or manipulated. This applies to deployers of AI systems that create deep fakes or texts published for public interest. Use watermarks or labels for images, videos, and text generated or manipulated by AI.
- **Transparency by Design:** For high-risk AI systems, design and develop them with a focus on providing sufficient information for deployers to understand the system’s output and use it correctly. Provide clear and understandable explanations of how the system works and produces output.
- **Guiding Instructions:** Provide relevant guidance for deployers of high-risk AI systems, including clear and complete information on the characteristics, functioning, and other key features of the system.

3. Audits and Monitoring:

Conduct regular audits, monitoring, and risk assessments of your AI systems to ensure ongoing compliance. Stay informed about any changes to the legislation and best practices in AI transparency.

4. Awareness:

- **Updating:** Stay informed about any changes in the legislation and best practices in AI transparency. Implement changes and update your AI systems as necessary to ensure compliance.
- **Training:** Train your team and staff on the requirements of the AI Act and the importance of transparency. Ensure that everyone involved in the development and deployment of AI systems understands the importance of transparency and how to implement it in their work.
- **Campaigns:** Carry out awareness campaigns to share information with users and the public about the implemented transparency measures. This can help build trust and ensure that users know their rights and the safeguards in place.
- **Feedback:** Create a system to collect feedback from users and stakeholders about the transparency of your AI systems.

10. What are the requirements for technical documentation and record-keeping for high-risk AI systems?

Deployers of High-Risk AI Systems

- **With regard to deployers,** they must retain the automatically generated logs of high-risk AI systems for at least 6 months, unless other EU law requires otherwise, as in the case of obligations under the GDPR. Financial sector deployers may keep the logs as part of the ordinary documentation required by sectoral financial services law.
- **If a serious incident occurs**, the deployer has an obligation to report it to the provider, the importer/distributor and the relevant market surveillance authorities. It is therefore necessary for deployers to ensure that incidents and their effects can be tracked down after the fact.
- **Documentation** of all kinds should be retained for an extended period of time to enable the deployer to demonstrate compliance. This applies to all stages of the compliance process, not just for technical documentation and record-keeping. For example, records should be kept of who has responsibility for human supervision in different parts of the organisation. This could also be the case with documenting any and all AI training that employees partake in. Deployers also need to inform natural persons who are subject to decisions or processes aided by the high-risk AI systems listed in Annex III. This obligation is without prejudice to the rules on transparency in Article 50 of the Act.
- **Before first putting a high risk AI system into service** , certain deployers (public authorities, private entities providing public services, and other entities that determine creditworthiness or risk on life and health insurance) must draw up a written Fundamental Rights Impact Assessment (FRIA) covering the items in Article 27(1)(a)–(f) (process description, duration/frequency of use, affected groups, risk analysis, human oversight measures, mitigation steps). The FRIA must be kept up to date whenever relevant factors change and its results must be notified to the competent market surveillance authority.

Providers of High-Risk AI Systems

- **Create A Technical File Before Launch** Draft one clear dossier that shows how the AI system meets every high-risk requirement. Use the Annex IV template or the simplified form available for SMEs if applicable. Keep it up-to-date. If an AI system is also regulated under product-safety laws in Annex I of the act, compile one integrated technical file for this purpose.
- **Storage of Documents** Companies must store all core documents for 10 years. These documents are listed in Article 18. These include:
  - the technical documentation referred to in Article 11;
  - the documentation concerning the quality management system referred to in Article 17;
  - the documentation concerning the changes approved by notified bodies, where applicable;

    - the decisions and other documents issued by the notified bodies, where applicable and;
    - the EU declaration of conformity referred to in Article 47.

- **Quality-Management System (QMS)** Implement a QMS that itself includes record-keeping procedures and which in turn should include policies, detailed procedures, and logs of all relevant documentation and information.
- **Maintaining Logs** High-risk AI systems must be technically capable of automatically recording events (logs) over the lifetime of the system to ensure traceability. The logs shall be kept for at least six (6) months or longer if other law so requires and must be sophisticated enough to identify situations that may pose a risk to health, safety or fundamental rights. The logs must also take into account the information required for post-market surveillance. In addition, the logs must function as intended in Article 26(5) of the Act so that deployers can identify potential risks and report them to the provider. There are additional requirements for entities which provide remote biometric identification systems. Financial-sector providers may keep the logs as part of the ordinary documentation required by sectoral financial-services law.
- **Manuals** High-risk AI systems shall be accompanied by instructions for use, in an appropriate digital format or otherwise, that provide concise, complete, accurate and clear information that is relevant, accessible and understandable to users. These instructions should review and explain at minimum the following:
    - provider identity & contacts – include the provider and, if relevant, its authorised representative;
    - system purpose & scope – state the intended purpose and any target user groups or contexts;
    - expected accuracy metrics and robustness/cyber security levels (tested under Art 15) and factors that could materially affect those levels;
    - risk related information – any foreseeable circumstances (normal use or reasonably foreseeable misuse) that could endanger health, safety or fundamental rights;
    - explainability features – describe any technical capabilities that help clarify how the system generates its outputs;
    - population specific details – where relevant, note performance for particular persons or groups:
    - data specifications – where relevant, summarise input data requirements and key attributes of the training/validation/testing data sets; and
    - output interpretation guidance – provide information enabling deployers to read and appropriately act on the system’s outputs.

- human oversight – the human oversight measures needed, as well as the technical measures put in place to facilitate the interpretation of the outputs of the high-risk AI systems by the deployers;
- the computational and hardware resources required, the expected lifetime of the high-risk AI system, and any maintenance and servicing required, and the frequency of such maintenance and servicing, to ensure the proper functioning of that AI system, including software updates; and
- where relevant, a description of the mechanisms included within the high-risk AI system that allows deployers to properly collect, store and interpret logs generated as described in Article 12.

Providers of General-Purpose AI (GPAI)

- There are special rules for those supplying GPAIs. Some obligations apply to all providers of GPAI and some only for GPAIs that are deemed may carry “systemic risk”. GPAIs with systemic risk are those which may have a significant impact on the Union market due to their reach, or due to actual or reasonably foreseeable negative effects on public health, safety, public security, fundamental rights, or the society as a whole, that can be propagated at scale across the value chain. Providers of GPAI may rely on the codes of practice published by the AI Office within the meaning of Article 56 to demonstrate compliance with the obligations set out in paragraph 1 of this Article, until a

harmonised standard is published.

Obligations for All Providers Of GPAI

- Draw up and keep up-to-date technical documentation for the model containing at least the items listed in Annex XI (e.g. model description, training data provenance, compute used, energy use).
- Maintain and supply technical documentation and information that lets AI-system providers understand capabilities/limits and meet their own compliance duties. The minimum contents are set out in Annex XII.
- Annex XI vs. Annex XII – Annex XI lists what must be in the regulatory technical file that must be available upon request by a competent authority; Annex XII lists what must be shared with integrators. Both are living obligations , keep them up-to-date.
- Publish a sufficiently-detailed summary of the training-data content using the AI Office template. This summary should be publicly accessible and updated when the model is retrained.
- Put in place and document a copyright-compliance policy (identify reservations of rights under the DSM Directive).
- Co-operate and supply any technical documentation or other information requested by the Commission / AI Office for compliance checks.
- For open-source AI systems, paragraph (a) and (b) do not apply, unless the GPAI may incur systemic risks.

Obligations for Providers of GPAI with Systemic Risk

- Perform model evaluation in accordance with standardised protocols including documenting adversarial testing of the model with a view to identifying and mitigating systemic risks.
- Monitor, document and report without delay to the European AI Office and, where appropriate, to the competent national authorities, relevant information on serious incidents and possible corrective actions to address them.
- Ensure that the GPAI has an adequate level of cybersecurity protection both for the model and its physical infrastructure.

11. What measures should we implement to ensure the accuracy, robustness, and cybersecurity of our AI systems?

Ensuring the accuracy, robustness, and cybersecurity of AI systems requires a comprehensive set of technical and organisational measures that reflect the state of the art and remain proportionate to the AI system’s intended purpose. In keeping with the European Union’s regulatory requirements, providers and deployers should begin by establishing a clear risk-management process that is in place throughout the AI system’s lifecycle. This process should identify the known and reasonably foreseeable risks arising from both ordinary use and potential misuse, as well as from potential errors, biases, or vulnerabilities in data, algorithms, and software infrastructure.

First, it is important to safeguard accuracy by designing the AI system in such a way that it consistently performs as intended, without producing faulty or misleading inferences. Relevant measures include reliable validation and testing protocols, especially prior to market placement or deployment. These protocols should apply defined metrics to gauge correctness and precision.

Where the AI system continues to learn post-deployment, additional safeguards must be in place to prevent undesired feedback loops that could amplify mistakes over time, for example by flagging unexpected performance anomalies and having appropriate thresholds at which human intervention takes place. Data governance strategies are equally essential. These should ensure that training, validation, and testing sets are representative and free of errors to the greatest extent possible, while

maintaining data minimisation principles.

Next, providers should reinforce robustness by incorporating fail-safes, resilience testing, and built-in operational constraints that cannot be overridden by the system itself. Such constraints assure that, when unexpected behaviours or identifiable faults arise, the AI system can be halted, scaled back, or otherwise directed into a safe operational state. An effective human oversight framework further enhances robustness by ensuring that trained personnel can interpret critical alerts from the AI system, verify its outputs, and intervene if harmful or unlawful results appear likely. To achieve these aims, providers and deployers can deploy risk-control procedures adapted to the gravity of potential harms, keeping in mind that certain contexts, such as health or safety applications, necessitate stricter oversight and more vigorous controls.

To address cybersecurity, the companies should implement security measures proportionate to the vulnerabilities inherent in both the AI system and the wider ICT environment in which it operates. This involves conducting ongoing risk assessments that consider well-known attack vectors such as data poisoning where adversaries insert corrupt training data to subvert the system, model extraction methods, or adversarial inputs designed to manipulate the system's outputs. Appropriate controls can include:

- regular penetration tests;
- encryption for data at rest and in transit; and
- effective access management policies, particularly in the post-deployment phase where external threats frequently arise.

For models that pose a higher risk under applicable rules, including those deemed "high-risk" within the EU AI Act, providers should adopt more sophisticated defensive measures, such as differential privacy or advanced adversarial testing. To ensure confidence in the system's cybersecurity, continuous monitoring and prompt patching regimes, coupled with detailed logging of relevant events, are strongly recommended.

Finally, all of these measures should be documented, reviewed frequently, regularly audited and updated as technology and threats evolve. These measures form part of providers' and deployers' accountability obligations and helps demonstrate compliance to oversight bodies.

12. What are the penalties for non-compliance with the AI Act and how can we avoid them?

The AI Act outlines extensive penalties for non-compliance, which vary based on the nature and severity of the infringement. These can be found in Article 99 of the Act, specifying what circumstances should be taken into consideration when fines are administrated. The rules regarding penalties for violations of the Act are set to enter into force on 2 August 2025.

- **Serious infringements (Article 99(3)):** regulates the types of AI practices that are considered to be completely prohibited (with very few exceptions) under Article 5. Fines can reach up to EUR 35 000 000 or 7% of the company's total annual worldwide turnover, whichever is higher.
  The preventive measures that need to be put in place to ensure that prohibited AI practices do not occur will be similar to those that should be put in place for high-risk AI systems. By using established risk management systems, companies can identify, analyse and assess the risks associated with emerging systems that may be prohibited. Not only should the systems themselves be carefully assessed, but also their use cases - both intended and unintended.
- **Other serious infringements (Article 99(4)):** include infringements not covered by Article 5 or concerning the supply of incorrect, incomplete or misleading information to notified bodies or

national competent authorities. Fines can reach up to EUR 15 000 000 or 3% of the company's total worldwide annual turnover, whichever is higher. Violations that could result in a fine include having an inadequate risk management system - or failing to implement required transparency measures. Given the scope of this category of non-compliance, it is likely that the most frequently imposed fines will be based on this article.

- **Risk Assessment and Management:** Implement a robust risk assessment framework throughout the AI system's lifecycle, from development or implementation to deployment, and continuously monitor it during operation. At the design stage, organizations should identify and assess potential risks associated with the AI system. This includes evaluating the system's impact on human rights, safety, privacy, and fairness. A risk matrix can be used to classify risks as low, medium, or high, helping prioritize actions based on the severity of the risks. Once an AI system is deployed or implemented, the risk assessment process should be ongoing. Organizations should conduct periodic audits and use feedback mechanisms (e.g., monitoring data for unexpected outcomes or biases to assess the system's operational performance). Ensure that proper documentation procedures are in place when implementing as well as monitoring the system, aligning with relevant developed frameworks for recordkeeping. Organising these assessments and the continuous monitoring under recognized frameworks for risk management like ISO 31000 and ISO/IEC 27001 is highly recommended, even if the organisation does not possess a formal certificate of compliance with such frameworks. These records will be critical in demonstrating compliance with the AI Act in the event of an audit or regulatory inspection.
- **Frameworks for risk management** help align an organisation's supervisorial infrastructure, assigning roles and responsibilities. Having dedicated personnel ensures accountability and oversight, which is essential for demonstrating compliance with the AI Act. Using tools like risk registers to systematically identify and document potential risks related to AI systems can greatly improve an organisation’s ability to respond to potential issues. This involves reviewing the entire AI lifecycle – from development to deployment and ongoing operations. Moreover, implementing an intuitive reporting processes that are regularly reviewed by senior management ensures that issues do not slip between the cracks. Implementing a system that automates the collection, documentation, and submission of required reports to regulatory bodies may also serve this purpose.
- For each high-risk AI system, it is advantageous to develop a risk treatment plan that outlines specific actions to mitigate identified risks. This plan should include timelines, allocated resources, and personnel responsible for addressing each risk.
- **The provision of false information (Article 99(5))** : regulates offences of providing false, misleading or incomplete information to the authorities when required to do so under the Act. Fines can reach up to EUR 7 500 000 or 1% of the company's total worldwide annual turnover, whichever is higher. Violations that could result in a fine include submitting data to a Notified Body that inaccurately represents an AI system’s compliance with safety standards. For example, a supplier may claim that the AI system has undergone certain safety tests that it has not actually completed. Additionally, a vendor’s failure to disclose known vulnerabilities or risks associated with its AI system—when requested by a Notified Body – may also be considered a violation.
  To ensure that your company provides accurate and complete information to the authorities, it is beneficial to implement a comprehensive quality management system (QMS) within your organisation, in line with an international standard such as ISO 9001. This will ensure that the company is heading in the right direction by implementing a compliance strategy, including procedures for managing changes to the AI system. In addition, it's important to establish systems for data capture, collection, analysis, labelling, storage and retention, as well as keeping detailed descriptions of the methods and steps taken during the development or implementation of the AI system. Finally, maintain a comprehensive checklist of 1) what needs to be reported, 2) how it

needs to be reported, and 3) when it needs to be reported. Schedule regular reviews of the progress and timing of reporting requirements.

For small and medium-sized enterprises, fines amount to the percentages and amounts above, but whichever thereof is lower. To be considered such an enterprise, the annual turnover of the enterprise may not exceed EUR 50 million, and/or have an annual balance sheet total exceeding EUR 43 million.

Companies that fail to comply with the EU AI Act risk serious reputational damage. Given the public sensitivity around privacy, bias, transparency and the ethical use of AI, non-compliance or misconduct can quickly lead to negative media attention, social media backlash and public condemnation. Reputational damage can be immediate, long-lasting and difficult to repair, directly affecting a company's image and brand value. According to research conducted by the Global Risk Advisory Council in 2025, during Q1, the misuse of AI was the leading reputational risk for organizations.

Negative narratives about ethical breaches in AI can quickly erode public goodwill, and extensive media coverage reinforces negative perceptions and amplifies public reaction. Customers may abandon products or services that violate AI ethics, resulting in an immediate loss of revenue. This can also lead to a decline in user engagement and loyalty due to mistrust, suspicion or fear of AI use. Violations can also be leveraged by competitors using their compliance as a unique selling point, eroding a company’s market position. This is certainly the case with the acquisitions of public contracts. These effects will likely not only be apparent in customers, but also investors, banks, and insurance companies. Besides the damage caused by sanctions and distrust of the public, internal investigations, process overhauls, staff retraining, or recruitment of compliance specialists will inevitably increase operational expenses.

Prohibited Practices

13. What is the role of Article 5 within the EU AI Act?

Article 5 of the EU AI Act defines AI practices that are strictly prohibited across the EU. These bans protect core rights such as human dignity, privacy, and non-discrimination. Unlike other provisions, these prohibitions apply unconditionally—regardless of user consent or business interests. They reflect the EU’s commitment to setting clear red lines for AI use.

14. Which AI practices are explicitly prohibited under Article 5 of the EU AI Act?

Article 5 prohibits several AI practices, including: (a) subliminal manipulation that may cause harm, (b) exploitation of vulnerable groups, (c) social scoring by public or private actors, and (f) inferring emotions in workplaces or educational settings. These practices are banned because they can seriously infringe on individuals' rights and freedoms. Violations may trigger significant legal and financial consequences.

15. What does Article 5(1)(f) specifically prohibit in relation to emotion recognition systems?

Article 5(1)(f) bans the use of AI systems to infer emotions of individuals in the workplace or educational environments. This applies to any system intended to assess internal emotional states

based on biometric data, such as facial expressions or voice tone. The only exceptions are for specific medical or safety-related purposes. The rule is designed to protect employee dignity and prevent misuse in power-imbalanced settings.

16. What are “emotions” within the meaning of Article 5(1)(f) of the AI Act?

"Emotions" are understood broadly to include states like happiness, anger, sadness, surprise, and more. The law covers both directly expressed emotions and those inferred from subtle cues. These are considered deeply personal and can reveal sensitive aspects of someone’s identity, which justifies the strict limitations on their use in AI systems.

Importantly, the law distinguishes between “apparently readily expressed” behaviors—such as smiling or frowning—and the inference of emotions from those behaviors using AI. Merely observing visible expressions is not prohibited. However, using AI to analyze those expressions to draw conclusions about internal emotional states falls under the ban in Article 5(1)(f), unless a narrow medical or safety exception applies.

17. What does it mean to “infer emotions” using AI?

“Infer emotions” means using AI to interpret internal emotional states from external signals like facial movements, voice tone, or body language. This goes beyond simply detecting visible reactions (e.g., a smile) and involves drawing conclusions about how someone feels inside. In workplace settings, this practice is generally banned unless strictly for medical or safety reasons.

18. How is the term “in the workplace” interpreted under this provision?

“In the workplace” is interpreted broadly and includes any setting related to employment—offices, remote work setups, mobile roles, and even during job applications or training. What matters is the functional connection to an employment relationship and whether the AI use is attributable to the employer. This ensures protection in any scenario where workers may be in a dependent or pressured situation.

19. How should the exception for medical or safety purposes be understood?

These exceptions are interpreted narrowly. Medical use is only allowed if the AI system qualifies as a certified medical device with a clear health-related purpose. Safety-related use is limited to preventing serious harm—such as fatigue monitoring in hazardous jobs—and cannot be used for performance evaluation. The purpose must be strictly protective, not for monitoring productivity or behavior.

General-Purpose AI Models (GPAI)

20. What are the specific requirements for general-purpose AI models (GPAI) under the AI Act?

The AI Act establishes obligations for GPAI models providers. Therefore, there should be a GPAI model and a GPAI model provider.

An AI model is a GPAI model when: (i) it displays "a considerable degree of generality", (ii) it is capable of competently performing a wide variety of different tasks, and (iii) it is capable of being integrated into systems or applications. The most decisive part of the definition is usually the first one. Recital 98 of the AI Act clarifies that “models with at least a billion of parameters and trained with a large amount of data using self-supervision at scale should be considered to display significant generality and to competently perform a wide range of distinctive tasks”.

As clarified by the AI Office, there is a provider of a GPAI model when a person “develops a general-purpose AI model or that has such a model developed and places it on the market, whether for payment or free or charge (Article 3(3))”, meaning when it is made available on the Union market (Article 3(9)). As explained in Whereas 97 of the AI Act, “when the provider of a general-purpose AI model integrates an own model into its own AI system that is made available on the market or put into service, that model should be considered to be placed on the market”.

According to the European Commission, In the case of a modification or fine-tuning of an existing general-purpose AI model, the obligations for providers of general purpose AI models in Article 53 should be limited to the modification or fine-tuning, for example, by complementing the already existing technical documentation with information on the modifications (Recital 109)”.

The specific requirements for GPAI models are five:

- To have at the disposal of the AI Office and the competent authorities the **technical documentation** of the model (including its training, the tests performed and their outcome);
- To make available to AI system providers (who will integrate the model into AI systems) **up-to-date information and documentation** on the model (sufficient to reach a good understanding of its capabilities and limitations, and at least with the information set out in Annex XII of the AI Act);
- To implement a policy to identify and respect the decision of **copyright** holders not to undergo "data mining", pursuant to Art. 4.3 of Directive (EU) 2019/790;
- To publish a sufficiently detailed **summary of the content used for model training** , following an outline to be approved by the IA Office, and
- To appoint an **authorised representative** in the EU.

These obligations will be developed further when the first General-Purpose AI Code of Practice be drafted and approved. There is a third draft of the General-Purpose AI Code of Practice that may be consulted.

21. What are the copyright-related obligations for GPA models?

The EU AI Act contains two copyright-related obligations for GPAI models.

The EU DSM Directive (Directive (EU) 2019/790) introduced an exception allowing the use of copyright works for text and data mining for any purpose. Rightsholders can opt out from this exception by reserving their rights over the relevant works.

Providers of GPAI models are required to put in place a policy to comply with EU law on copyright and related rights and, in particular, to identify and comply with a reservation of rights under the EU DSM Directive. Recital 106 of the EU AI Act says that this obligation should apply to any provider placing a GPAI model on the EU market, even if the “copyright-relevant acts underpinning the training” of the GPAI model take place outside the EU.

Where rightsholders have opted out in accordance with the EU DSM Directive, Recital 105 of the EU AI Act says that providers of GPAI models will need to obtain authorisation from the rightsholders before

carrying out text and data mining over the relevant works.

Providers of GPAI models are also required to publish a “sufficiently detailed” summary of the training content for the GPAI model. The summary should be “generally comprehensive in its scope instead of technically detailed”, for example, by listing the main datasets used to train the model and providing a narrative explanation about the use of other data sources. The AI Office is in the process of creating a template for this summary, although a draft has not been published yet.

GPAI model providers can rely on codes of practice to demonstrate compliance with these copyright-related obligations, until a harmonised standard is published. Drafts of the General-Purpose AI Code of Practice have been published, with the final version expected in April 2025.

22. What are the additional obligations for providers of GPAI models with systemic risk?

Some GPAI models are classified as having “systemic risk”. The definition of the said is not precise, but requires that the model have “high impact capabilities” (which shall be presumed when the cumulative amount of computation used for its training measured in floating point operations is greater than 10^{25}) or an equivalent impact. “High impact capabilities” is a concept that has two elements: capabilities that equal or exceed those of the most advanced GPAI models, and risk of impact to certain assets with certain scope and scale along the IA value chain.

Examples of the above may be, for instance, systems with foreseeable negative effects in relations to major accidents, disruptions of critical sectors, serious consequences to public health and safety, negative effects on democratic processes or economic security, dissemination of illegal, false or discriminatory content at scale, etc. The second draft of GPAI models Code of Practice identifies cyber offences, chemical, biological, radiological and nuclear risks, large-scale harmful manipulation, large-scale illegal discrimination, loss of human oversight in autonomous systems, risk for infrastructure reliability or for fundamental rights.

There are four additional obligations for providers of GPAI models with systemic risk:

- To conduct an assessment of the model including "adversary simulation testing", which must be documented;
- To identify and mitigate potential risks in the EU;
- To record and notify the IA Office and where appropriate the competent national authorities of "serious incidents" and corrective actions taken, and
- To ensure an adequate level of cybersecurity.

The Code of Practice, which is being drafted now (see its current second draft here:Third Draft of the General-Purpose AI Code of Practice published, written by independent experts | Shaping Europe’s digital future), will explain how these obligations should be complied with.

23. What contractual clauses should we include to ensure compliance with the AI Act when acquiring generative AI systems?

A previous due diligence on the system we are purchasing is always advisable and allows to shorten the number of contractual obligations.

The answer to the question above depends on our role in the AI value chain. Assuming that we are a company that purchases a GAI system for its own use, which is not a high-risk use, the following topics

should be addressed in the contract:

- The provider of the GPAI model used by the system should have complied with its obligations as explained above, including making available to the provider up-to-date information and documentation, that according to the contract the provider may be obliged to deliver to its professional customer. This obligation also includes representations and guarantees regarding copyright, summary of the content used for model training, and existence of a EU representative.
- Some of the obligations that are imposed by the AI Act to high-risk systems may also be imposed by the deployer of a non-high-risk system to its provider through contract, regarding the following topics, among others:
  - Data sets used in the training;
  - Record-keeping obligations;
  - Transparency and provision of information obligations;
  - The way in which human oversight of the system is performed;
  - Cybersecurity.

- A critical issue is whether the AI system provider may or not use the prompts and data given by the deployer or by the user in order to train the model, or for any other use. When possible, this should be prohibited in the contract.
- The right to use the contents generated by the AI system, including any intellectual property or trade secrets if any, should also be addressed, as well as the survival of the relevant clauses after the termination of the contract.
- Regarding the indemnity in the case of fines being imposed, please see below.

24. How can we address liability and indemnification in contracts for generative AI systems with systemic risk?

An adequate due diligence can reduce the risk of unforeseen liability.

Assuming we are representing the deployer or the user of a GAI system, two different types of liability should be considered: contractual and extracontractual. In a contract between a provider of GAI and a deployer (or a user) of GAI, it is possible to address contractual liability as well as indemnification in the case of extracontractual liability towards third parties (or certain fines imposed to the deployer or the user as a consequence of a non-compliance by the provider).

Regarding contractual liability of the provider of GAI, the contract may establish, for the benefit of the deployer (or user) (inspired in the draft AI Liability Directive, mutatis mutandis):

- The contractual obligation to fully comply with AI Act;
- A discovery obligation, obliging the provider to deliver pertinent, necessary and proportionate evidence when damage has been caused;
- A iuris tantum presumption of the existence of breach of contract, if the discovery obligation is not complied with;
- A iuris tantum presumption of the existence of causal relationship, if it is reasonably likely that the breach of contract has caused the output, and there is evidence that the output caused the damage.

Usually, the main negotiation will refer to the limitations of liability imposed by the provider, as well as the applicable law.

Adequate indemnification clauses can also be established by the deployer (or user) in the case it is condemned to pay compensation for damages caused to third parties as a consequence of a breach of

contract by the provider (linked to the possible joint and several liability of both the provider and the deployer towards third parties, or to the possibility of fines imposed to the deployer or user acting as data controller because of incorrect actions of the provider acting as data processor).

Of course, insurance should also be taken into account.

25. What are the key considerations for intellectual property provisions in contracts allowing individuals to use generative AI models?

In the same way as for use of proprietary software, individuals wanting to use generative AI models should check that they are granted appropriate usage rights (in other words, they should check what they are allowed and not allowed to do with the generative AI model).

In addition, individuals should check:

- who owns any rights in the output of the generative AI model; and
- what happens if a third party brings a claim alleging that the individual's use of the generative AI model or output from that generative AI model infringes the third party's intellectual property rights.

While the position varies, a number of the tech companies already say in their terms of use for generative AI models that:

- the individual user owns any rights in output generated by that user; and
- the tech company indemnifies the individual user for third-party intellectual property infringement claims.

However, individuals should be aware that it is possible for a different user to generate the same content using the generative AI model and it's unclear if AI-generated output is capable of protection under intellectual property law.

If a tech company is considering offering an indemnity, it is important to consider:

- whether liability under that indemnity should be capped financially; and
- any guardrails or exceptions from that indemnity. For example, will the indemnity apply if the individual user switched off any guardrails built into the generative AI model or prompted the generative AI model to create a lookalike or a soundalike?

Transparency and User Information

26. How do we ensure that our AI systems are transparent and that users are informed when interacting with AI?

Ensuring transparency in AI systems is fundamental to building trust and safeguarding the rights of users. Companies must design and develop their AI systems with transparency at the forefront, providing clear, accessible, and comprehensive information about how these systems operate, internally and externally. This includes offering detailed instructions for use, outlining the system's capabilities and limitations, and explaining any circumstances that may affect its performance. For high-risk AI systems, it is especially important to provide information that enables users to interpret outputs correctly and understand the potential impact of AI-driven decisions. All documentation and

notifications should be tailored to the technical knowledge and needs of the intended users, ensuring accessibility for everyone, including persons with disabilities.

A critical aspect of transparency is informing users when they are interacting with an AI system. Companies must ensure that users are clearly notified at the first point of interaction, unless it is obvious that they are engaging with AI. This notification should be provided in a manner that is easy to understand and accessible to all, including those with disabilities. Furthermore, when AI systems generate or manipulate content—such as text, images, audio, or video—that could be mistaken for authentic or human-generated material, it is essential to clearly label this content as artificially created or manipulated. This is particularly important in contexts where the content could influence public opinion or decision-making, such as news and advertising, or public interest communications.

To maintain transparency throughout the AI lifecycle, companies should implement robust record-keeping and documentation practices, ensuring that all relevant information about the AI system's operation, data processing, and decision-making logic is available for review by users and authorities. Staff must receive ongoing training to develop sufficient AI literacy, enabling them to use AI systems responsibly and interpret outputs appropriately.

Summary of practical steps

- Clearly inform end users when they are interacting with AI, both at the point of first contact and throughout their engagement.
- Mark and label all AI-generated or manipulated content, especially where there is a risk of confusion with authentic content.
- Provide comprehensive, accessible, and understandable instructions and information about the AI system's operation, limitations, and risks.
- Ensure all staff are trained to understand and appropriately use AI systems.
- Maintain robust documentation and logging to support transparency, traceability, and compliance in accordance with the latest guidance.
- Regularly review and update your transparency practices in line with technological and regulatory developments.

27. What are the requirements for AI literacy and training for our staff and other relevant persons?

Businesses should provide training on AI to their staff, tailoring the level of training based on the skills and roles of their staff.

Providers and deployers of AI systems are required to put in place measures to ensure "*to their best extent*" a "*sufficient level of AI literacy*" in respect of individuals (including staff) dealing with the operation and use of AI systems on their behalf.

Here, AI literacy means the "*skills, knowledge and understanding*" that enables providers, deployers and affected persons: (a) to make an "*informed deployment*" of AI systems; and (b) to gain awareness about the opportunities, risks and potential for harm presented by AI, in each case taking into account their rights and obligations under the EU AI Act.

What will be considered sufficient will depend on the technical knowledge, experience, education and training of those individuals, as well as the context in which (and the individuals on whom) the AI systems will be used.

In particular, deployers should ensure that any individuals tasked with implementing the instructions

for use for the relevant AI system and human oversight measures (as set out in the EU AI Act) have the *"necessary competence"*, including an "*adequate level"* of AI literacy and training, to fulfil those tasks properly.

According to Recital 165 of the EU AI Act, providers and (where appropriate) deployers of AI systems or AI models should be encouraged (but not required) to apply additional requirements related to AI literacy measures. The EU AI Office and member states are tasked with facilitating the creation of a voluntary code of conduct in relation to the promotion of AI literacy (particularly, the AI literacy of those individuals dealing with the development, operation and use of AI), although there's no deadline for this code of conduct.

28. What are the key considerations for conducting a Fundamental Rights Impact Assessment (FRIA) for our AI systems?

In order to efficiently ensure that fundamental rights are protected, **deployers of high-risk AI systems**, should carry out a FRIA prior to putting these high-risk AI systems into use. The businesses should first determine whether they are a deployer of high-risk AI systems. The aim of the FRIA is for the deployer to identify the specific risks to the rights of individuals or groups of individuals likely to be affected and to identify measures to be taken in the case of a materialisation of those risks. The impact assessment should be performed prior to deploying the high-risk AI system, and should be updated when the deployer considers that any of the relevant factors have changed. The relevant factors to consider are listed below. Conducting a FRIA therefore involves several key considerations to ensure compliance with the AI Act (see Article 27 (1) AI Act):

- **Description of AI system use.** Clearly describe the processes in which the AI system will be used, including its intended purpose and the context of use.
- **Usage frequency and duration.** Specify the period of time and frequency with which the AI system will be used.
- **Identify affected individuals**. Identify the categories of natural persons and groups likely to be affected by the AI system's use.
- **Risk assessment.** Assess the specific risks of harm that the AI system may pose to the identified individuals and groups, taking into account information provided by the AI system provider.
- **Human oversight.** Describe the implementation of human oversight measures, ensuring that there is meaningful human intervention in critical decision-making processes.
- **Mitigations measures.** Outline the measures to be taken in case the identified risks materialize, including governance arrangements, complaint handling, and redress procedures.
- **Stakeholder involvement.** Involve relevant stakeholders in the assessment process, including representatives of affected groups, where relevant also independent experts, and ethical committees, to gather comprehensive insights and ensure transparency.

After performing the FRIA, the deployer should notify the relevant market surveillance authority. The relevant market surveillance authorities are established by each EU member state. The EU AI Office shall develop a template for a questionnaire, including through an automated tool, to facilitate deployers in complying with their notification obligations related to the FRIA.

29. How do we ensure that our AI systems comply with data protection regulations, including GDPR?

Data protection laws become relevant if AI systems are using personal data. To ensure compliance

with data protection laws, including GDPR, ensure that the relevant data protection rules and principles as covered in the local laws are fully adhered to, including:

- **Lawful basis for processing.** Ensure that the processing of personal data by AI systems is based on one of the available legal bases provided by data protection regulations, including those available under the GDPR (consent, contract with a data subject, legal obligation, vital interests, public interest, or legitimate interests).
- **Purpose limitation and data minimization.** Collect and process personal data only for specific, legitimate purposes and limit the data to what is necessary for those purposes, i.e. training, development and use of the AI models or AI systems. Communicate clearly in your policies about these (additional) purposes.
- **Data accuracy.** Implement mechanisms to ensure that personal data used by AI systems is accurate and up-to-date.
- **Storage limitation**. Store personal data only for as long as necessary to achieve the purposes for which it was collected. Ensure transparency about the data retention term per purpose of personal data processing. Apply techniques which enable you to fully anonymise or delete the personal data following the expiration to the applicable data retention term.
- **Automated decision-making**. Provide individuals with the right not to be subject solely to automated decision-making that produces legal effects or significantly affects them, and ensure meaningful human oversight in such processes.
- **Security measures**. Implement appropriate technical and organizational (cyber)security measures to protect personal data from unauthorized access, alteration, loss, or damage.
- **Transparency and data subject rights.** Inform individuals about how (long) their data is being processed, and provide mechanisms for them to exercise their rights, such as access, rectification, erasure, and data portability.
- **Data protection impact assessments (DPIAs)**. Conduct DPIAs for high-risk data processing activities performed by AI systems to identify and mitigate potential risks to individuals' privacy and data protection rights.
- **Privacy by design and by default**. When designing and putting into use an AI system, make sure to take into account and implement privacy by design and by default addressing the risks resulting from the processing by the AI system. These measures ensure that a proactive and preventative approach that requires organisations to incorporate data protection measures from the very beginning of the design process of any AI system or AI model and to anticipate and prevent privacy-invasive events before they happen.
- **Reporting of incidents**. Where a notification obligation exists under the applicable data protection laws, like under the GDPR, ensure that any incidents resulting in loss, unauthorised disclosure or alteration of personal data by use of AI system can timely be reported as a data breach to the relevant supervisory authority. Providers of high-risk AI systems placed on the EU market must report any serious incident to the market surveillance authorities of the EU member states where that incident occurred within 15 days after the provider or, where applicable, the deployer, becomes aware of the serious incident (Article 73 (2) AI Act). Serious incident is an incident or malfunctioning of an AI system that leads to any of the following (a) the death of a person, or serious harm to a person’s health; (b) a serious and irreversible disruption of the management or operation of critical infrastructure; (c) the infringement of obligations under EU law intended to protect fundamental rights or (d) serious harm to property or the environment (Article 3 (49) AI Act).

30. What are the specific transparency obligations for AI systems generating synthetic content, such as deepfakes?

Providers of AI systems generating synthetic content (whether audio, image, video or text) are required to ensure that the outputs of the relevant AI system are "*marked in a machine-readable format and detectable as artificially generated or manipulated*", whether using watermarks, cryptographic methods or other techniques.

In addition to a law enforcement exception, this obligation does not apply where an AI system:

- performs an "*assistive function*" for standard editing; or
- does not substantially alter the input data.

Deployers of AI systems generating or manipulating content (whether audio, image or video) that "resembles existing persons, objects, places, entities or events and would falsely appear to a person to be authentic or truthful" (and, as such, constitutes a deep fake) are required to disclose that the content is artificially generated or manipulated.

In addition to a law enforcement exception, where AI-generated or manipulated content is part of an "evidently artistic, creative, satirical, fictional or analogous" work or programme, the deployer is instead required to disclose the existence of such content "in an appropriate manner that does not hamper the display or enjoyment of the work".

Finally, deployers of AI systems generating or manipulating text "*published with the purpose of informing the public on matters of public interest*" are required to disclose that the text is artificially generated or manipulated.

In addition to a law enforcement exception, this obligation does not apply where the AI-generated content has been through a process of "*human review or editorial control*" and someone (whether an individual or a legal entity) has "*editorial responsibility*" for publication of that AI-generated content.

The AI Office is tasked with encouraging and facilitating the creation of codes of practice to facilitate the effective implementation of these transparency obligations.

Human Oversight and Bias Mitigation

31. How do we ensure that our AI systems are free from biases and do not lead to discriminatory outcomes?

Ensuring that AI systems are free from impermissible biases and do not lead to discriminatory outcomes is a multifaceted task that calls for diligence throughout the entire lifecycle of the system, including its design, development, testing, and deployment. Under the EU's AI Act, as well as broader data protection and fundamental rights frameworks, several recommended practices can help identify, prevent, and mitigate undue bias so that AI tools do not adversely affect individuals or groups because of protected characteristics such as gender, age, or ethnicity.

First and foremost, the AI Act emphasises that providers of AI systems—particularly those assessed as high-risk—must systematically evaluate and mitigate potential bias at each step of the AI system's development. This obligation includes careful selection of training and validation datasets, implementing data governance and management practices to detect hidden patterns of discrimination, and handling special categories of personal data strictly in accordance with data protection laws. The principle of data minimisation, laid down in Article 5(1)(c) of the General Data Protection Regulation (GDPR), also applies, meaning that organisations should only collect and process the minimum amount of personal data needed to address the relevant purpose, including the detection and correction of biases.

Where high-risk systems are concerned, Article 10 of the AI Act and related recitals specify that the training, validation, and testing data must be relevant, representative, and, to the best extent possible, free of errors and complete in view of the intended purpose. If this condition is not satisfied, the AI model risks perpetuating flawed assumptions about disadvantaged groups. The AI Act recognises that mitigating bias can sometimes require the limited processing of sensitive personal data. In such cases, personal data may only be used where it is strictly necessary for bias detection and correction, and even then strict technical, organisational, and legal safeguards must be in place to avoid infringing on individuals' rights.

In addition to data-related safeguards, providers and deployers of AI systems must maintain robust risk management systems that continuously monitor for potentially unfair or discriminatory effects. This extends across both the development stage—where the model is trained and validated—and the deployment stage, where the model is put into service and begins to interact with real-world conditions. The organisation should regularly test the model, including through recognized adversarial or stress-testing approaches, to identify unintended outcomes that may adversely affect certain groups. If these tests reveal disproportionate impacts on protected characteristics or an unexpected correlation in the model's outputs that could lead to discrimination, the AI Act requires providers and deployers to implement mitigating measures or adapt the model to address these findings.

Human oversight is likewise pivotal in ensuring non-discriminatory outcomes. The AI Act lays down an overarching requirement that human operators be able to understand, overlook, and, if needed, intervene in the AI system's workings to prevent erroneous or harmful outputs. Where the AI system is high-risk, human oversight measures may be particularly stringent, requiring the operator to confirm or review the AI output before it is actually applied—thus serving as a safeguard against biases the algorithm might produce.

Transparency is also essential. Organisations must furnish clear information to end users—and, where relevant, to affected persons—about the capabilities, limitations, and design assumptions of an AI system. This transparency helps people understand when an AI model might be more prone to certain errors or biases and can encourage them to challenge decisions that seem unfair.

Finally, there is a strong impetus in the AI Act on continuous education and training—referred to as AI literacy. Training employees to recognise and respond to possible instances of bias is a recommended strategy. This includes equipping developers, operators, and compliance teams with regular, up-to-date knowledge on how to detect, interpret, and address biases in AI systems. Incorporating feedback from diverse teams that reflect different cultural or social backgrounds can likewise help illuminate blind spots in systems that might otherwise go undetected.

Taken together, these practices—thoughtful dataset composition and governance, risk management, human oversight, transparency, and comprehensive internal training—serve as integral safeguards against discrimination, ensuring that AI systems uphold equality and fairness in their outcomes. By following these requirements and recommended procedures from the AI Act and broader data protection law, an organisation can demonstrate accountability and more effectively guard against impermissible biases, thereby enhancing trust and fostering inclusive innovation.

Importers, Distributors, and Market Placement

32. What are the obligations for importers and distributors of high-risk AI systems under the AI Act

Importers and distributors play a crucial role in ensuring that high-risk AI systems entering the EU market comply with the AI Act's stringent standards.

Under the AI Act:

- An **importer** is a natural or legal person resident or established in the EU who places an AI system on the market that bears the name or trademark of a natural or legal person established in a third country. The importer acts as an entry point for AI systems from non-EU suppliers and must ensure compliance with EU rules before the system is placed on the market for the first time.
- A **distributor** is a natural or legal person in the supply chain, other than the supplier or importer, who makes an AI system available on the EU market. The distributor does not place the product on the EU market but must ensure that AI systems already placed on the market are distributed or supplied in compliance with the requirements of the AIA.

Please note, that the same entity may act as both importer and distributor. Distinguishing between the two roles is crucial for determining the applicable obligations and must be done on a case-by case basis.

The AI Act imposes a wide range of obligations on importers and distributors. These include:

- **Formal review obligations**:

Importers and Distributors must ensure that the AI system has undergone the appropriate conformity assessment procedure, bears the CE marking, and is accompanied by the required documentation, including the EU declaration of conformity and detailed instructions for use.

- **Non-Compliance Response:**

If importers or distributors have reason to believe that an AI system does not conform to the AI Act, they must not place it on the market until it complies. They are also obligated to inform the provider or authorized representative and cooperate with authorities to address any non-compliance.

- **Record-Keeping and Cooperation:**

Both importers and distributors must keep a copy of the EU declaration of conformity and ensure that technical documentation can be made available to national authorities upon request. They are also required to cooperate with these authorities, providing information and documentation necessary to demonstrate the compliance of the AI system.

33. How do we ensure that our AI systems are compliant with the AI Act when placing them on the EU market?

To ensure compliance with the AI Act when placing AI systems on the EU market, your organisation should:

- **Classify AI systems** into appropriate risk categories, such as prohibited, high risk, limited risk or minimal/no risk. For high-risk AI systems, ensure compliance with obligations such as implementing risk management protocols, using high-quality and representative datasets, enabling logging capabilities, and completing conformity assessments. These systems must be CE marked and, where applicable, registered in the EU database of AI systems.
- **Provide detailed and transparent documentation** describing the design, intended purpose and operational procedures of the AI system. Transparency obligations include informing users when interacting with AI, clearly labelling AI-generated content, and disclosing the use of biometric or emotion recognition systems.

- Establish and maintain a robust **post-market monitoring framework** to continuously evaluate the performance of the AI system and its compliance with the requirements of the Act. Any serious incidents, such as significant malfunctions or breaches of fundamental rights, must be reported promptly to the relevant authorities within the prescribed timeframes.
- Actively **engage with the regulatory framework** by appointing authorised representatives in the EU if operating from outside, using regulatory sandboxes to test AI systems in a controlled and innovation-friendly environment, and working with Member State authorities to align with compliance standards and adopt best practices.

34. What are the requirements for the appointment of an authorized representative for third-country providers?

Under the AI Act, third country providers of AI systems must appoint an authorised representative within the European Union to ensure compliance with the requirements of the Act. The key requirements for appointing an authorised representative are:

- **Establishment within the EU**: The authorised representative must be a natural or legal person established in the EU and act as a point of contact for regulatory matters.
- **Documented mandate**: A written agreement must set out the authorised representative's responsibilities, which include ensuring the provider's compliance with the law, such as maintaining technical documentation, responding to requests from authorities and cooperating during inspections or assessments.
- **Scope of responsibilities**: The representative must have access to and be able to provide relevant documentation (e.g. EU Declaration of Conformity, technical records) to the competent authorities upon request. They are responsible for supporting market surveillance and addressing compliance issues related to the provider's AI systems.
- **Accountability and legal representation**: The authorised representative is legally responsible for compliance with the specific obligations set out in the AI Act, making it a key intermediary between non-EU providers and EU regulators.

35. How do we handle the storage and transport conditions for our AI systems to ensure compliance?

To ensure that AI systems comply with the AI Act when placed on the EU market, it is essential that all requirements relating to their storage and transport are met.

This includes following the provider's guidelines for proper handling, storage and transport to ensure that the systems are handled in a way that maintains their integrity and functionality. It is equally important to maintain detailed records of storage and transport conditions to demonstrate compliance with regulatory requirements. These records provide evidence that systems have been stored and transported under conditions that preserve their software and hardware components. In addition, precautions must be taken to protect the systems from environmental, physical or cyber risks during these processes.

Internal Risk Management and Policies

36. What are the key considerations for the development of AI-specific internal risk management frameworks and policies?

The AI Act requires a risk management system to be established, implemented, documented and maintained in relation to high-risk AI systems. This risk management system is to be understood as a continuous iterative process planned that needs to be run throughout the entire lifecycle of a high-risk AI system, requiring regular systematic review and updating. High-risk AI systems must be tested for the purpose of identifying the most appropriate and targeted risk management measures. Testing ensures that high-risk AI systems perform consistently for their intended purpose and that they are in compliance with the risk management requirements of the AI Act. For the development of an AI-specific internal risk management frameworks and policies several key elements can be identified:

- **Comprehensive risk identification and assessment**. Identify and assess risks associated with development and use of AI systems, including technical, ethical, legal, and operational risks.
- **Clear policies and procedures**. Establish clear policies and procedures for AI systems risk mitigation and governance, ensuring consistent practices across the organization. Appoint the policy owner in the relevant business line (within the first line of defence).
- **Dedicated roles and responsibilities**. Create dedicated roles for AI risk management and ethics, such as a (Chief) AI Ethics Officer or AI Compliance Officer, and define clear lines of accountability, available resources and reporting.
- **Stakeholder involvement.** Involve a diverse group of stakeholders, including legal, technical, and business experts, in the risk identification and management process.
- **Regular audits and testing**. Conduct ongoing audits and testing to ensure that AI systems operate as intended and comply with legal requirements.
- **Bias prevention and mitigation**. Use diverse and representative datasets to reduce bias in AI systems and implement measures to detect and mitigate biases. Training, validation and testing data sets must be relevant, sufficiently representative, and to the best extent possible, free of errors and complete in view of the intended purpose. They should have the appropriate statistical properties, including, where applicable, as regards the persons or groups of persons in relation to whom the high-risk AI system is intended to be used.
- **User training**. Train users on the proper use and limitations of AI systems, ensuring they understand the potential risks and how to manage them. Ensure, a sufficient level of AI literacy of the 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.
- **Security measures**. Implement strong cybersecurity protocols to protect AI systems from data breaches and other security threats. The technical solutions aiming to ensure the cybersecurity of high-risk AI systems or for the general-purpose AI model with systemic risk and the physical infrastructure of the model, must be appropriate to the relevant circumstances and the risks.
- **Documentation and transparency**. Create an AI systems inventory and maintain detailed, up-to-date documentation of AI systems, the used data sources, processing activities, and implemented risk management measures as well as performed audits to demonstrate compliance and accountability.

37. How do we ensure that our AI systems are designed to operate with varying levels of autonomy and adaptiveness?

The definition of AI systems in the AI Act contains that AI systems may exhibit adaptiveness after deployment. The adaptiveness that an AI system could exhibit after deployment, refers to self-learning capabilities, allowing the system to change while in use. Adaptiveness is an optional element of AI system definition. Autonomy

Autonomy (at least on varying levels) is part of the definition of AI System in the AI Act. The level of autonomy of the AI systems may increase the risk of the given AI system, in particular in case of general purpose AI systems. The level of autonomy of the AI system will influence the human oversight measures for mitigating the risks of high-risk AI systems pursuant to the AI Act.

To ensure AI systems are designed to operate with varying levels of autonomy and adaptiveness in compliance with the EU AI Act, a good practice is implementing adaptive and autonomous design controls. AI systems should account for varying autonomy levels and adaptability:

- **Human Oversight**: Ensure mechanisms for human intervention or control, particularly for high-risk AI systems, e.g.:
  - Provide "stop" mechanisms or override options for users.
  - Implement user-friendly dashboards or interfaces to manage adaptiveness.
- **Dynamic Risk Assessment**: Include built-in monitoring to detect changes in AI behaviour or operational contexts and adjust autonomy levels accordingly.
- **Transparency and Explainability**: Ensure users understand the system's autonomy and decision-making processes.
  - Provide clear information about how the system adapts and the boundaries of its autonomy.

For high-risk AI systems, follow these mandates:

- **Risk Management System**: Establish procedures to identify, evaluate, and mitigate risks associated with adaptiveness and autonomy.
- **Data Governance**: Use high-quality, representative, and unbiased data to train adaptive systems, reducing risks of unexpected autonomy escalation.
- **Technical Documentation**: Maintain comprehensive documentation covering:
  - Adaptive algorithms.
  - Autonomy thresholds.
  - Safety mechanisms for varying autonomy levels.
- **Conformity Assessments**: Regularly test AI systems for compliance with EU AI Act requirements.
  - Simulate scenarios to validate safety at different autonomy levels.
- **Control Transparency**: Clearly indicate to users when the AI's autonomy changes, such as in decision-making scenarios.
- **Feedback Loops**: Design mechanisms for users to provide feedback and fine-tune the AI's behaviour.
- **Behavioural Monitoring**: Include real-time analytics to track changes in the system's adaptiveness and detect anomalies.
- **Incident Reporting**: Set up processes to report and address safety incidents or malfunctions related to autonomy.
- **Auditability**: Ensure logs and records are maintained to track how and why decisions were made under varying autonomy levels.

By embedding these considerations into the design, development, and deployment processes, your AI systems will be better positioned to align with the EU AI Act's goals of safety, accountability, and human-centric innovation while supporting varying levels of autonomy and adaptiveness.

Sector-Specific Requirements

38. What are the specific requirements for the use of AI systems in critical infrastructure?

Because critical infrastructure systems are so fundamental to society, the use of AI in critical infrastructure invites enhanced scrutiny. Article 6 of the EU AI Act defines high-risk AI systems and includes among others "*critical infrastructure*", which is generally accepted to mean *essential support systems, functions, and services that are essential to sustaining and maintaining a civil society*. The Act lays down an expansive functional sector list and includes utilities and energy, water, transportation, food, water, waste, public services administration, communications digital infrastructure, and space as already defined under Directive (EU) 2022/2557 and Regulation (EU) 2023/2450. Likewise, Annex III (2) of the AI Act states that high risk AI system are: "*AI systems intended to be used as safety components in the management and operation of critical digital infrastructure (emphasis added), road traffic, or in the supply of water, gas, heating or electricity*." Recital 55 of the AI Act provides guidance in that it is intended to mean management and operational systems within the critical infrastructure sectors and subsectors delineated in Annex 1 to Directive (EU) 2022/22557. Although not expressly stated in the AI Act, it is prudent to assume that any AI system that serves any operational or management control function for critical infrastructures could be classified as high-risk whether or not the AI system has an intended safety function. As noted earlier, other sectors that fall within the EU's critical infrastructure law's definition may be assigned a high-risk classification by reference and incorporation of a Union harmonization legislation list in Annex 1 which is not limited to use in safety systems.

Aside from the qualification of critical infrastructure, the general differentiation between "smart or artificially intelligent?" remains relevant to determine if AI in the sense of the EU AI Act lies at hand or not. Critical infrastructure systems and technologies are usually complex. They might e.g. be real time sensing technologies leveraging network connectivity or use predictive models to make decisions and take actions (e.g. notifications and alerts). These systems can be found in everything e.g. trading systems in the financial sector or rail systems. Although such systems are often "smart," the question remains whether they have a sufficient degree of autonomy and should constitute AI systems in the sense of the EU AI Act. Likely, companies will attempt to exclude their AI tools developed or deployed from this definition ambit to also avoid falling under the EU AI Act's critical infrastructure provisions.

Where there is ambiguity in the high-risk classification in general, the AI Act attempts to provide some relief from definitional uncertainty through Article 6 para. 3. It carves out AI systems from a high-risk classification if the system "*… does not pose a significant risk of harm to the health, safety or fundamental rights of natural persons, including by not materially influencing the outcome of decision making*." Thus, the AI system should not qualify as high risk if it is intended to perform a narrow procedural task and is intended to only improve the result of a previously completed human activity or the AI system is intended to detect decision-making patterns and is not meant to replace or influence the previously completed human assessment, without proper human review or the AI system is intended to perform a preparatory task to an assessment. This is likely to be a key provision for critical infrastructure system providers if they choose to opt out and can firmly establish the Article 6 (3) safe harbor is met. Nonetheless, even if this exception is met, the critical infrastructure provider will not be free from classification risk or regulation. Article 6(4) of the AI Act requires that a provider of a purported non-high-risk Annex III system registers it under Article 49(2) and document its non-high-risk assessment and make it available to authorities upon request.

Should no out of scope classification or exception listed above, apply, deployers of AI-systems in critical infrastructures will have to establish:

- A risk management system throughout the high risk AI system's lifecycle;

- Conduct data governance, ensuring that training, validation and testing datasets are sufficiently representative and, to the best extent possible, free of errors and complete for the intended purpose;
- Draw up technical documentation to demonstrate compliance and provide authorities with the information to assess that compliance;
- Design their high-risk AI system for record-keeping and enable it to automatically record events relevant for identifying risks and modifications throughout the system's lifecycle;
- (If a provider) provide instructions for use to downstream deployers to enable the latter's compliance;
- Design their high risk AI system to allow deployers to implement human oversight. Design their high risk AI system to achieve appropriate levels of accuracy, robustness, and cybersecurity;
- Establish a quality management system to ensure compliance.

Companies where advanced technology/IT-systems play important functions in critical infrastructure, e.g. banking and finance, education and/or other product safety regulated markets and use advanced algorithm levels should analyze them through an EU AI Act lens. If significant market exposure exists, it is prudent to pursue registration as a non-high-risk system rather than taking the self-determined position that a smart system is not by definition an AI system to avoid application of the EU AI Act.

39. How do we ensure that our AI systems are compliant with the AI Act when used in the public sector?

Local public Law legislation should be taken into account.

As regards general principles, the following are considered best practices:

- Previous approval of the specifications, programs, maintenance, supervision and quality control by the competent body (sometimes, there will be two different competent bodies: one for the technical issues, another one for the criteria to be applied and the decisions to be taken on the merits).
- Transparency on the above.
- Administrative decisions should have enough motivation to be understood and eventually challenged, even when based on an AI system. For this reason, "machine learning" systems not transparent enough should be avoided.
- Clear identification of the competent body for appeals against the automated decision.

Compliance with art. 22 GDPR is compulsory, when applicable.

The public sector should always determine if the use is a high-risk use, and in the case it is, Chapter III of the AI Act should be complied with.

Use of AI by judicial office holders have specific guidance (see for instance, for the UK, the Guidance for Judicial Office Holders available at AI Judicial Guidance).

40. What are the requirements for the use of AI systems in the context of law enforcement and migration?

AI systems used in the context of law enforcement and migration are classified as high-risk in Annex III AI Act - in so far as their use is permitted under relevant Union or national law. This classification is due to their potential impact on (procedural) fundamental rights such as the right to an effective remedy, a fair trial, the right to free movement and the protection of private life and personal data. If the AI system is not trained with high-quality data, does not meet adequate requirements in terms of

its performance, its accuracy or robustness, or is not properly designed and tested before being put on the market or into service, it may single out people in a discriminatory or otherwise incorrect or unjust manner.

The requirements for **law enforcement and migration** authorities using high-risk AI Systems under the AI Act are as follows:

- **Registration:** High-risk AI Systems shall be registered in the EU database. The registration of the high-risk AI Systems in the areas of law enforcement and migration shall be in a secure non-public section of the EU database (Article 49 AI Act).
- **Conformity assessment:** In general the provider may choose any of the notified bodies for the purposes of the conformity assessment procedure. However, where the high-risk AI system is intended to be put into service by law enforcement or immigration authorities the market surveillance authority shall act as the notified body.

No separate verification needed: The requirement for a separate verification by at least two natural persons shall not apply to high-risk AI systems used for the purposes of law enforcement and migration, where Union or national law considers the application of this requirement to be disproportionate.

There are additional specific requirements for **law enforcement** authorities using high-risk AI Systems under the AI Act:

- **'Real-time' remote biometric identification systems**: The use of 'real-time' remote biometric identification systems for the purpose of law enforcement should be prohibited, except in exhaustively listed and narrowly defined situations in Article 5 (1) (h) AI Act, where the use is strictly necessary to achieve a substantial public interest, the importance of which outweighs the risks.
- **Prior authorisation:** Each use of a 'real-time' remote biometric identification system in publicly accessible spaces for the purpose of law enforcement should be subject to express and specific authorisation by a judicial authority or by an independent administrative authority of a Member State whose decision is binding. Such authorisation should be obtained prior to the use of the AI system (Recital 35 and Article 5 (3) AI Act).
- **Fundamental rights impact assessment:** 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 and has registered the system in the database (Article 5 (2) AI Act).

41. How do we ensure that our AI systems are compliant with the AI Act when used for credit scoring and creditworthiness evaluation?

AI systems intended for evaluating the creditworthiness of natural persons or establishing their credit score, except those used to detect financial fraud, are referenced in Annex III of the AI Act and classified as high-risk AI systems. This classification arises from their significant influence on individuals' access to financial resources or essential services such as housing, electricity, and telecommunications. Consequently, these AI systems must comply with the requirements for high-risk AI systems as outlined in the AI Act.

As a specific rule, prior to deploying an AI system intended for creditworthiness evaluation or credit scoring, deployers must conduct an assessment of the system's impact on fundamental rights.

AI systems used for credit scoring and creditworthiness evaluation are not considered high-risk if they do not pose a significant risk to the health, safety, or fundamental rights of natural persons, including cases where they do not materially influence the outcome of decision-making.

This exemption applies under any of the following conditions:

a. The AI system is designed to perform a narrow procedural task.
b. The AI system is intended to enhance the results of a previously completed human activity.
c. The AI system identifies decision-making patterns or deviations from prior decision-making patterns but does not replace or influence a prior human assessment, without proper human review.
d. The AI system performs a preparatory task relevant to credit scoring or creditworthiness evaluation.

Notwithstanding the above, an AI system used for credit scoring and creditworthiness evaluation is always considered high-risk if it performs profiling of natural persons.

42. What are the requirements for the use of AI systems in the context of financial services and insurance?

AI systems used for risk assessment and pricing for natural persons in life and health insurance are classified as high-risk in Annex III of the AI Act. This classification is due to their potential impact on individuals' livelihoods - if not properly designed, developed, and used, they could infringe fundamental rights and lead to serious consequences, such as financial exclusion and discrimination. These AI systems are subject to the same requirements as those used for credit scoring and creditworthiness evaluation, including the specific obligation to assess their impact on fundamental rights.

The specific requirements for financial institutions using high-risk AI Systems under the AI Act are as follows:

- **Quality management system compliance of providers.** Financial institution providers of high risk AI-systems subject to EU financial services law requirements regarding internal governance, arrangements, or processes are considered compliant with the quality management system obligations of the AI Act, except for risk management system requirements (Article 9 of the AI Act) and reporting procedures for serious incidents.
- **Documentation obligations of providers**. Financial institution providers of high risk AI-systems must maintain technical documentation as part of the existing documentation under EU financial services law. Automatically generated logs from high-risk AI systems must also be retained as part of this documentation.
- **Monitoring and log retention obligations of deployers**. Financial institution deployers of high-risk AI systems must monitor these systems in accordance with instructions, promptly inform relevant parties and authorities of risks or serious incidents, and suspend use if necessary, excluding sensitive data of law enforcement authorities. For financial institution deployers subject to internal governance, arrangements, or processes under Union financial services law, the monitoring obligation shall be deemed fulfilled by complying with the governance rules, processes, and mechanisms outlined in the relevant financial services law.

Financial institution deployers of high-risk AI systems must retain system-generated logs for at least six months or as specified by applicable laws, with integrating these logs into their documentation under relevant financial services regulations.

Post-market monitoring for high-risk AI systems under Article 72 of the AI Act

Specific rules apply to high-risk AI systems used for:

- Evaluating creditworthiness or establishing credit scores (excluding systems for detecting financial fraud).
- Risk assessment and pricing in life and health insurance.

If financial institutions subject to EU financial services law already have post-market monitoring systems and plans, they may integrate the required elements from Article 72 into their existing internal governance, arrangements or processes to ensure consistency, avoid duplication, and minimise burdens, provided an equivalent level of protection is achieved. Article 72 of the AI Act includes the following requirements for providers:

- Providers must document a post-market monitoring system proportionate to the nature and the risks of the high-risk AI system.
- The system must actively gather, document, and analyse performance data (excluding sensitive operational data from law enforcement authorities) to ensure continuous compliance, including interactions with other AI systems where relevant.
- The plan must be included in the technical documentation of the high-risk AI system. The European Commission will establish a template for the plan and its required elements through an implementing act.

43. How do we ensure that our AI systems are compliant with the AI Act when used for fraud detection

AI systems used for detecting fraud in financial services and for prudential purposes to calculate credit institutions' and insurance undertakings' capital requirements are not classified as high-risk under the AI Act. Therefore, only the AI literacy obligations for all deployers and providers of AI systems outlined in Article 4 of the AI Act, and the transparency obligations for providers and deployers of certain AI systems in Article 50, apply. It is important to note that Recital (58) specifies such systems are exempt only if they are "provided for by Union law".

44. What are the specific requirements for the use of AI systems in healthcare and emergency response services?

The regulatory framework for AI in healthcare across the EU encompasses several interconnected areas of law and professional practice, including but not limited to the following.

Medical device. AI software falls under the EU Medical Device Regulation (MDR) when it is intended for medical purposes such as diagnosis, prevention, monitoring, prediction, prognosis, treatment, or alleviation of disease. The determination is based on the software's intended purpose and its role in medical decision-making: systems analyzing medical data to support clinical decisions are typically regulated as medical devices, while purely administrative systems are not. For qualifying AI systems, the MDR mandates comprehensive requirements including in terms of clinical evaluation and technical documentation; additionally, AI systems qualifying as medical devices will be considered "high risk" under the AI Act and subject to additional requirements (see dedicated section on conducting a gap analysis between the MDR and the AIA).

Medical practice. The prohibition against the illegal exercise of medical practice in some countries significantly impacts AI system design and deployment. AI systems must be clearly positioned as support tools rather than autonomous decision-makers, with qualified medical professionals

maintaining supervision and responsibility for all medical decisions. This framework creates specific requirements for how AI systems present their outputs and recommendations, ensuring they support rather than replace medical judgment.

Processing of medical data. The processing of medical data by AI systems must follow strict protocols to ensure compliance with legal requirements and protect patient privacy and safety. The foundation begins with GDPR compliance, requiring a clear legal basis for processing - typically either explicit consent from patients or processing necessary for medical diagnosis or treatment under Article 9(2)(h). This must be accompanied by specific safeguards under Article 9(3), including processing under the responsibility of healthcare professionals subject to professional secrecy obligations. If medical data is used for training of the AI system or research using or regarding the AI system, additional national requirements applicable to medical research may apply, including ethics committee approval and/or authorization from national data protection authorities.

Medical secrecy. Medical secrecy requirements are particularly stringent, with healthcare AI systems falling under the same strict confidentiality obligations as healthcare professionals. These obligations are typically enforced through criminal penalties at the national level, and they can extend to operators of AI systems that process medical data. The systems must incorporate robust technical measures to ensure confidentiality, including comprehensive access logging and secure transmission protocols.

Electronic health records. The European Health Data Space introduces additional complexity through its comprehensive regulation of electronic health records and health data sharing, for both primary and secondary use of health data. AI systems must comply with those rules if they claim interoperability with EHR systems (medical devices and other high risk AI systems) or if they meet the definition of EHR systems. In such case they must especially comply with the essential requirements on the interoperability software component and logging software component.

45. How do we ensure that our AI systems are compliant with the AI Act when used for biometric identification and categorization?

Biometric identification: A biometric identification AI system is defined in Art. 3(35) of the AI Act as an AI system for the purpose of identifying natural persons, without their active involvement, typically at a distance through the comparison of a person's biometric data with the biometric data contained in a reference database. The AI Act differentiates based on (i) the time of identification, distinguishing between real-time remote biometric identification ("**RBI**"), where the comparison and the identification all occur without a significant delay and post-RBI, (ii) the location of deployment, whether it is a publicly accessible place or a privately accessible one, and (iii) the purpose of application, distinguishing between law enforcement and other purposes. The AI Act does not provide a unified approach to RBI, but rather defines certain types and establishes various prohibitions and obligations for them according to its general risk-based approach:

- The AI Act prohibits the use of real-time RBI systems in publicly accessible spaces for law enforcement purposes (Art. 5(1)(h)), only allowing limited exceptions.
- Additionally, all RBI systems are classified as high-risk AI systems under Annex III.

Biometric categorisation: A biometric categorisation system means pursuant to Art. 3(40) an AI system for the purpose of assigning natural persons to specific categories on the basis of their biometric data, unless it is ancillary to another commercial service and strictly necessary for objective technical reasons. Following the risk-based approach,

- biometric categorisation that categorises 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 pose unacceptable risks and is therefore prohibited (Art. 5(1)(g)).
- On the other hand, AI systems intended to be used for biometric categorisation, according to sensitive or protected attributes or characteristics based on the inference of those attributes or characteristics are classified as high-risk AI systems under Annex III.

In each case, high-risk AI systems shall be subject to the stricter compliance regime of the AI Act, such as (i) risk management and documentation, where providers must implement a continuous risk management system, conduct impact assessments, and maintain detailed technical documentation demonstrating compliance, (ii) data quality & bias mitigation to ensure that training datasets are diverse, representative, and free from discriminatory biases to minimize errors and inaccuracies in identification, (iii) transparency and human oversight, so that deployers inform individuals when RBI is used, except in law enforcement scenarios where exemptions apply. Real-time RBI requires human intervention in decision-making to prevent unjustified automated enforcement, and (iv) logging and traceability, maintaining logs of system operations, including identification attempts and decision rationales, to allow for audits and compliance monitoring by authorities. Finally, providers must undergo conformity assessments before placing the system on the market and register the AI in the EU database for high-risk AI.

Additionally, considering that both biometric identification and biometric categorisation require the processing of personal data under Regulation 2016/679(EU) on the General Data Protection Regulation ("**GDPR**"), and such processing of personal data constitutes special categories of personal data (Art. 9(1) GDPR), both providers and deployers of such AI systems must adhere to the requirements of the GDPR, including designating and appropriate legal basis and transparency obligations.

46. How do we ensure that our AI systems are compliant with the AI Act when used for monitoring and evaluation of employee performance?

AI systems used to monitor and evaluate employee performance are classified as high-risk under the AI Act. Therefore, they must comply with all requirements for high-risk AI systems, unless classified otherwise under Article 6 section 3 of the AI Act. To ensure compliance, follow these steps:

1. **Inform Employees and Their Representatives**: Before using such a system, provide necessary information to workers' representatives and the affected employees, informing them that they will be subject to the high-risk AI system for monitoring and evaluation.
2. **Mitigate Bias**: Regularly monitor the AI system's operation and outputs to prevent discrimination based on race, gender, age, or other sensitive characteristics. Implement measures to mitigate any identified biases.
3. **Ensure Privacy and Data Protection**: Comply with data protection laws, particularly the GDPR and local privacy laws. Pay special attention to GDPR rules on automated decision-making and ensure measures are in place to protect workers' rights, freedoms, and legitimate interests. Guarantee that workers can obtain human intervention, express their views, and contest automated decisions.
4. **Avoid Prohibited AI Practices in Workplace**: Ensure that the AI system does not analyse or detect the emotional state of individuals in the workplace, as this would be classified as a prohibited practice under the AI Act. In this category, an example could be a system developed by an HR technology company and offered to businesses as a tool to monitor employees' emotions in the workplace. Its goal is to improve employee efficiency and well-being by analysing their

emotions in real-time. It uses cameras and microphones installed in offices, conference rooms, and other workspaces to record facial expressions, voice tones, gestures, and other emotional indicators during daily activities. AI algorithms analyse the collected data in real-time, drawing conclusions about employees' emotions, such as stress, satisfaction, frustration, or engagement. The system then creates reports and emotional profiles for each employee. Employees are not fully aware that their emotions are being monitored and analysed. Managers use the reports generated by the system to make personnel decisions. Employees showing emotions like stress or frustration are marked as less productive, leading to unfair performance evaluations and being overlooked for promotions.

47. What are the specific requirements for the use of AI systems in the context of recruitment and personnel management?

Employers deploying AI systems in the recruitment process can likely fall under the rules for "high risk"-AI-categories under EU AI Act. This may apply as soon as AI systems are intended to be used in the recruitment or selection process, for instance to place targeted job advertisements or to analyze/filter job applications or to evaluate candidates. AI systems purported for making decisions affecting terms of work-related relationships, promotion and/or termination of work-related contractual relationship or to allocate working tasks based on individual behavior/personal traits or to monitor performance and behavior of persons are likely to qualify as high-risk AI systems under the EU AI Act.

High-risk AI systems need to conform to certain requirements, in particular risk management measures must be in place, data quality, transparency, human oversight and accuracy as well as non-discrimination and fairness must be ensured. The business deploying such technology has an obligation of registration, quality management, monitoring, record-keeping and incident reporting of such high-risk-AI-systems. Especially in the employment and recruitment process, the rules under the EU AI Act are aimed at avoiding bias/discrimination, health and safety as well as data protection risks.

By reason of the foregoing, HR-professionals and recruiters should prepare for the entry into force of the EU AI Act and implement legislative obligations in advance. In particular, they should:

- Be transparent on the use of AI towards employees or potential prospects (e.g. with employee- or applicant notices). Create clear explanations of how AI is used in your HR/recruitment processes and ensure accessibility of such information. Furthermore, make sure to use high-risk AI systems only in accordance with instruction of use issued by the AI-provider;
- Ensure that input data collected is relevant and sufficiently representative in view of the intended purpose of the high-risk AI system (no excessive data feeding);
- Data bears high worth, but with power also comes responsibility. The EU AI Act demands that data used in AI-driven recruitment processes is relevant, consistent and securely maintained. Therefore, ensure data integrity and secure record-keeping;
- Be vigilant about potential bias in AI systems and strive to minimize it. Measures should be implemented to ensure that discrimination laws/provisions are not infringed due to the manner, in which an AI tool's output is used (e.g. to assess who should be recruited based on protected characteristics of a particular group of people);
- Be aware that the use of AI technology may have adverse impact on the mental health of employees (e.g. employees impacted by a sense of constant monitoring and inability to maintain an adequate work-life balance. This may trigger implications under many national employment laws;
- Where an non-compliance event/incident is identified, use of AI should be suspended and a report should be made to the relevant AI provider and/or data protection authorities, if required by data privacy laws;

- Make sure to avoid scope expansion, i.e., where the original purpose of deploying an AI tool evolves and data collected for one purpose (e.g. training) is later used for other purposes (e.g. disciplinary ones);
- Ideally, blend AI with human expertise. A synergy between AI and human expertise is likely to avoid the inference that a recruiter has overly relied on AI-output/automated decision making. Maintaining human oversight is a key requirement of the EU AI-Act and is also to some degree required under most applicable data privacy laws;
- If required under national employment laws, consult with employee representatives before deploying high-risk AI systems in the work place and incorporate feedback into AI strategies of the company;
- For multinational employers, make sure to carefully analyze the applicability of different national statutes. The EU AI Act does not only apply to businesses using AI systems in the EU. E.g. if AI systems are used outside the EU but used to make decisions on potential employees based in the EU, multinational businesses will fall under the ambit of the EU AI Act; and
- Conduct a data protection impact assessment (DPIA) and a fundamental human rights assessment (FHRA) before deploying the relevant AI-system.

Organizations *developing their own AI systems for use* or where they put into service a high-risk AI system under their own name or trademark or make a substantial modification to an existing high-risk AI-system will no longer be deemed a mere deployer of AI (i.e. the person using an AI system under its authority), but rather a *provider* of AI (i.e., a developer who places the system on the market under its own name or trademark). It is pertinent to mention that further obligations under the AI Act are applicable to providers of AI. HR professionals qualifying as AI-providers should therefore put in place robust AI governance to implement controls, policies and frameworks to address all challenges brought by HR systems using AI (see answers provided to duties of AI-providers).

48. How do we ensure that our AI systems are compliant with the AI Act when used for automated decision-making?

To ensure compliance with the AI Act when using AI systems for automated decision-making in employment and personnel management, consider the following steps:

- **Risk assessment**. Identify whether the AI system falls under the high-risk category, particularly if it is used for recruitment, promotions, task allocation, or employee monitoring.
- **Transparency**. Inform employees and their representatives about the use of AI systems in the workplace, including how decisions are made and the data used.
- **Human oversight**. Implement meaningful human oversight to review and intervene in critical decisions made by AI systems, ensuring that decisions are fair and non-discriminatory.
- **Data quality and bias mitigation**. Use relevant and representative input data to train AI systems, and regularly test for and mitigate biases to prevent discriminatory outcomes.
- **Log keeping**. Maintain logs of system-generated data for a minimum of six months to ensure traceability and accountability.
- **Prohibited practices and high-risk AI systems**. if an AI system is prohibited or presents a high risk which cannot be mitigated, suspend its use and inform the developer or relevant authorities. For example, AI systems providing social scoring of candidate employees may lead to discriminatory outcomes, detrimental or unfavourable treatment and the exclusion of certain groups and are therefore prohibited. AI systems used in employment, workers management and access to self-employment, in particular for the recruitment and selection of persons, for making decisions affecting terms of the work-related relationship, promotion and termination of work-related contractual relationships, for allocating tasks on the basis of individual behaviour, personal

traits or characteristics and for monitoring or evaluation of persons in work-related contractual relationships, are classified as high-risk, since those systems may have a significant impact on future career prospects, livelihoods of those persons and workers' rights

- **Compliance with data protection laws**. Ensure that AI systems comply with all applicable data protection laws, including GDPR and its principles as required, by implementing appropriate data processing, security, and transparency technical and organisational measures prior to the deployment of these systems.
- **Employee training**. provide AI literacy training to employees, taking into account their technical knowledge, experience, education 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. Consider the limitations of various AI systems, including the risks associated with their use, ensuring the employees understand how to interact with and oversee these systems.
- **Consultation with work councils**. engage with work councils or employee representatives to discuss the implementation and impact of AI systems in the workplace. Under the AI Act, employers (deployers) of high-risk AI systems must inform their work council about and prior to the deployment and use of these systems. This obligation is part of ensuring transparency and protecting the rights of employees who may be affected by the AI systems.

49. How do we ensure that our AI systems are compliant with the AI Act when used for customer support and chatbots?

Customer support functions or chatbots are likely to be classified in category 3 (limited risk). Therefore, the most important requirements are:

- Transparency and labelling obligations: In the case of chatbots, this means that it must be clear to users that they are engaging with a bot and not a human. The underlying rational is to ensure that users understand the nature of their interaction and can react in an appropriate manner;
- Options to cancel a dialog with a chatbot: While this sounds self-understanding (and humans also have a right to cancel dialogs with humans at anytime), it is an important safeguard with chatbots to ensure that users remain in control of their interactions at any time. Not only should a user be able to cancel a dialog, but also should he be able to seek for interaction with a human, if desired;
- Protection of privacy rights: While it is self-evident that any business practice should be compliant with data privacy laws, the EU AI Act states this as a fundamental principle as well. Thus, any personal data collected in the intercourse with an AI-based Chatbot or similar customer support instrument, should be treated in the same transparent manner as for personal data shared through other channels (e.g. phone or e-mails).

It is pertinent to mention that the EU AI Act affects all market participants who use resp. deploy chatbots. Companies and organizations will be uniformly required to design their chatbots in a transparent and ethical manner.

50. What are the requirements for the use of AI systems in the context of marketing and personalized advertising?

Marketers have huge potential to include the use of AI into their marketing practices, such as e.g. AI-powered chatbots, personalized content recommendations and targeted advertising practices. Marketers now have a diverse array of capabilities to enhance their advertising campaigns. This capability spans from content creation to lead generation (e.g. users following ads to brand websites and into online-purchases), email marketing and market research. Especially, AI empowers advertisers to create more "engaging" experiences for their audiences. For instance, advertisers can ask

audiences to engage in polls or design artwork based on logos or designs of a brand owner). It will be vital for companies to understand how these systems work and to ensure they respect the principles established in the EU AI Act and other adjacent laws.

- A marketer needs to be aware of specifically forbidden practices. For instance, it is forbidden to use AI in a non-transparent manner to manipulate customer behaviour. That includes for example posting fake reviews or testimonials from fake customers. Another perceivable field prohibited is using AI to target specific demographic groups based on sensitive attributes like their race or religion;
- Marketers that use an AI-tool for automatic decision making in campaigns should respect certain requirements. Those include conducting a risk assessment, documenting all relevant processing steps of the AI-tool and ensuring that there are human options to override decisions made by the software;
- The EU AI Act places a lot of emphasis on transparency and customer control. Marketers need to make transparent to customers when they are interacting with AI-driven systems. For instance, a customer should be able to understand that he is interacting with an AI-chat bot and/or be able to opt out or to get help from a human when dealing with AI-driven content. Or, a customer should understand that he is dealing with a personalized advertisement (which might not always be clear from circumstances) and not a general offering-advertisement. Bear in mind that non-transparent practices are also likely to violate data privacy laws and/or unfair competition law practices, which all the more make transparency a must;
- Another rather pervasive legal risk in AI-based advertising practices to avoid is that AI tools can spread misinformation. This can trigger claims against false advertising and deceptive practices. The most common unlawful practices known and detected so far have been the AI-based creation of deepfake videos, voice clones to personal features, placing ads within a widely used AI-tool in an attempt to have them placed next to search results or selling fake views, likes and followers;
- Regulators have warned businesses in public announcements not to use AI-tools in a manner, which could have biased or discriminatory impacts. Therefore, deployers of AI-tools in the advertising industry should be wary of creating advertisements which replicate biased messages that could bear discriminatory meaning to the exclusion of certain minority groups;
- Since AI-based image tools enable the creation of deepfake photographs or videos (e.g. of persons not involved in a certain visual setting), this also raises questions on data privacy, since identifying features of a person are used without his/her consent or prior information. The creation and commercial use of such photographs or so to speak "doubles" of someone's face or other personal characteristics is relying on the use of one's personality traits. This can trigger wider potential personality right claims and disputes which should be avoided in the first place.

51. What are the requirements for the use of AI systems in the context of entertainment and media?

The EU AI Act does not contain specific requirements for the use of AI systems in the context of entertainment and media.

Where an entertainment or media organisation uses an AI system falling within the scope of the EU AI Act, it will need to comply with the general rules applicable to that AI system.

However, the requirements likely to be of most relevance in the context of entertainment and media are the transparency requirements for AI-generated or manipulated content (see Question **13** above) and the copyright-related requirements (see Question **5** above).

International and Territorial Aspects

52. How does the AI Act apply to AI systems developed outside the EU but used within the EU?

- **Extraterritoriality Principle.** As explained by the EU Commission in its AI Q&A, the legal framework of the AI Act 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 has an impact on people located in the EU. The extraterritoriality effect is similar to what was adopted in the past for the REACH regulations.
- Non-EU providers of AI systems will have to respect obligations when they place products in the EU as provided in the recitals 21 and 22 of the AI Act. In addition, the prohibited AI practices described article 5 of the AI Act (such as AI systems that deploy subliminal techniques or that classify people on their social behaviour) are applicable to non-EU deployers which place or put into service or the use of these AI systems in the EU.
- **Exemptions.** There are certain exemptions to the applicability of these regulations. Research, development, and prototyping activities that take place before an AI system is released on the market are not subject to these regulations. Additionally, according to recital 24 of the AI Act, AI systems that are exclusively designed for military, defence, or national security purposes are also exempt, regardless of the type of entity carrying out those activities.

53. What are the obligations for non-EU providers of AI systems when placing their products on the EU market?

- **The appointment of an authorized representative.** According to recital 21 of the AI Act, non-EU providers of AI systems will have to respect obligations when they place products in the EU. According to article 54 of the AI Act, prior to placing a general-purpose AI model on the Union market, providers established in third countries shall, by written mandate, appoint an authorised representative which is established in the Union.
- **Specific regulations regarding high-risk AI systems.** Before introducing a high-risk AI system to the EU market or putting it into service, providers must conduct a **conformity assessment**. This process ensures that the system meets mandatory requirements for trustworthy AI, such as data quality, documentation and traceability, transparency, human oversight, accuracy, cybersecurity, and robustness. If the system or its purpose undergoes significant changes, the assessment must be repeated. AI systems that function as safety components in products governed by sectorial Union legislation will always be classified as high-risk when subjected to third-party conformity assessment under that legislation. Additionally, all biometric systems, regardless of their application, will require third-party conformity assessment.
- Providers of high-risk AI systems must also **implement quality and risk management systems** to ensure compliance with new requirements and minimize risks for users and affected individuals, even after the product is on the market. High-risk AI systems deployed by public authorities or entities acting on their behalf must be registered in a public EU database, except when used for law enforcement and migration purposes.

54. What are the limitations of the AI Act concerning AI systems used for defence and national security?

Outside the scope of the AI Act. The field of defence is a unique domain: AI finds specific

applications here, escaping many regulatory restrictions that enable innovation while also preserving civilian and military lives. Defence is outside the scope of the AI Act. Thus, Recital 24 specifies: if "AI systems are placed on the market, put into service or used with or without modification of these systems for military, defence or national security purposes, these systems should be excluded from the scope of this Regulation, regardless of the type of entity carrying out these activities, for example, whether it is a public or private entity. Regarding the use for military and defence purposes, such an exclusion is justified both by Article 4, paragraph 2, of the Treaty on the European Union and by the specificities of the defence policy of the Member States and the common defence policy of the Union under Title V, Chapter 2, of the Treaty on the European Union."

Company-created Guidelines. Leading companies in security and defence have however established guidelines for the development of AI in their services and products. The first rule concerns AI validity: AI should only perform its intended functions and not exceed its defined role. The second rule pertains to cybersecurity: the system must be resilient against cyberattacks. The third rule emphasizes the explainability of AI systems. Lastly, the fourth rule focuses on the responsibility of AI-based systems and the necessity of maintaining ethical AI practices within the defence industry.

NATO strategy. NATO's Artificial Intelligence Strategy aims to accelerate the adoption of AI to strengthen NATO's technological advantage while protecting against AI-related threats. NATO is committed to collaboration and cooperation among Allies on AI-related issues for transatlantic defence and security. The key points of NATO's strategy are as follows:

- Responsible use: encouraging the responsible development and use of AI for defence and security purposes
- Widespread adoption: accelerating the adoption of AI in capability development, interoperability, and new programs
- Protection and monitoring: protecting AI technologies and innovation capacity
- Threat mitigation: identifying and countering threats related to the malicious use of AI by state and non-state actors.

Specific Considerations for Legal, Risk, and Compliance Departments

55. How do we ensure that our AI systems comply with the AI Act's requirements for data minimization and purpose limitation?

Biometric identification: A biometric identification AI system is defined in Art. 3(35) of the AI Act as an AI system for the purpose of identifying natural persons, without their active involvement, typically at a distance through the comparison of a person’s biometric data with the biometric data contained in a reference database. The AI Act differentiates based on (i) the time of identification, distinguishing between real-time remote biometric identification (“**RBI**”), where the comparison and the identification all occur without a significant delay and post-RBI, (ii) the location of deployment, whether it is a publicly accessible place or a privately accessible one, and (iii) the purpose of application, distinguishing between law enforcement and other purposes. The AI Act does not provide a unified approach to RBI, but rather defines certain types and establishes various prohibitions and obligations for them according to its general risk-based approach:

- The AI Act prohibits the use of real-time RBI systems in publicly accessible spaces for law enforcement purposes (Art. 5(1)(h)), only allowing limited exceptions.

- Additionally, all RBI systems are classified as high-risk AI systems under Annex III.

Biometric categorisation: A **biometric categorisation** system means pursuant to Art. 3(40) an AI system for the purpose of assigning natural persons to specific categories on the basis of their biometric data, unless it is ancillary to another commercial service and strictly necessary for objective technical reasons. Following the risk-based approach,

- biometric categorisation that categorises 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 pose unacceptable risks and is therefore prohibited (Art. 5(1)(g)).
- On the other hand, AI systems intended to be used for biometric categorisation, according to sensitive or protected attributes or characteristics based on the inference of those attributes or characteristics are classified as high-risk AI systems under Annex III.

In each case, high-risk AI systems shall be subject to the stricter compliance regime of the AI Act, such as (i) risk management and documentation, where providers must implement a continuous risk management system, conduct impact assessments, and maintain detailed technical documentation demonstrating compliance, (ii) data quality & bias mitigation to ensure that training datasets are diverse, representative, and free from discriminatory biases to minimize errors and inaccuracies in identification, (iii) transparency and human oversight, so that deployers inform individuals when RBI is used, except in law enforcement scenarios where exemptions apply. Real-time RBI requires human intervention in decision-making to prevent unjustified automated enforcement, and (iv) logging and traceability, maintaining logs of system operations, including identification attempts and decision rationales, to allow for audits and compliance monitoring by authorities. Finally, providers must undergo conformity assessments before placing the system on the market and register the AI in the EU database for high-risk AI.

Additionally, considering that both biometric identification and biometric categorisation require the processing of personal data under Regulation 2016/679(EU) on the General Data Protection Regulation ("**GDPR**"), and such processing of personal data constitutes special categories of personal data (Art. 9(1) GDPR), both providers and deployers of such AI systems must adhere to the requirements of the GDPR, including designating and appropriate legal basis and transparency obligations.

56. What are the specific obligations for conducting a Data Protection Impact Assessment (DPIA) under the AI Act?

It is important to note that carrying out a data protection impact assessment ("**DPIA**") is a requirement under Regulation 2016/679(EU) on the General Data Protection Regulation ("**GDPR**"), and pursuant to Art. 35 GDPR, it must be conducted when the development of an AI system involves processing personal data and is likely to pose a high risk to individuals' rights and freedoms. The European Data Protection Board (EDPB) provides nine criteria to determine when a DPIA is required, including processing sensitive data, large-scale data collection, processing data from vulnerable individuals, and using innovative AI techniques. A key point to consider is that AI systems not classified as "high-risk" under the AI Act may still involve the processing of personal data that poses a high risk under the GDPR, requiring a separate risk assessment under data protection laws. While AI systems are not automatically considered "innovative use," certain techniques, such as deep learning and generative AI, typically fall within this category, and require a DPIA. Moreover, high-risk AI systems under the AI Act are presumed to require a DPIA when personal data is processed, aligning with the risk-based approach of the GDPR.

A DPIA should assess specific risks related to AI systems, including data misuse, discrimination, and automated decision-making biases. Foundation models and general-purpose AI systems, while not inherently classified as high-risk under the AI Act, often necessitate a DPIA due to the broad and unpredictable nature of their deployment. The assessment must also consider technical vulnerabilities, such as data poisoning, model inversion, and backdoor attacks, which could compromise both data integrity and confidentiality. Additionally, certain data protection supervisory authorities, e.g., the French CNIL suggests that systemic risks, such as societal impact and loss of user control over their personal data, should be incorporated into the DPIA, especially when AI systems rely on large-scale web scraping.

The scope of the DPIA depends on the data controller's role in the AI supply chain. If the provider is also the controller during deployment, a comprehensive DPIA covering both development and operational phases is recommended. Where future uses remain uncertain, the DPIA should focus on the development phase, while the controller overseeing deployment must conduct a separate assessment. In cases where a provider can foresee potential applications, a DPIA template may be shared to assist downstream users in compliance. Given the iterative nature of AI development, DPIAs should be updated as system functionalities and risks evolve.

Lastly, The AI Act's documentation requirements overlap with DPIA obligations, therefore AI providers could potentially consolidate compliance documentation, such as DPIA and a fundamental rights impact assessment mandated by Art. 27 of the AI Act.

57. How do we address the AI Act's requirements for ensuring the quality and representativeness of training data?

Articles 10(3) and 10(4) of the AI Act stipulate that training data sets shall be relevant, sufficiently representative, and to the best extent possible, free of errors and complete in view of the intended purpose. They shall have the appropriate statistical properties, including, where applicable, as regards the persons or groups of persons in relation to whom the high-risk AI system is intended to be used. Those characteristics of the data sets may be met at the level of individual data sets or at the level of a combination thereof. Data sets shall take into account, to the extent required by the intended purpose, the characteristics or elements that are particular to the specific geographical, contextual, behavioural or functional setting within which the high-risk AI system is intended to be used.

Annex IV of the AI Act rules that the technical documentation of high-risk AI systems must contain a detailed description of the data requirements in terms of datasheets describing the training methodologies and techniques and the training data sets used, including a general description of these data sets, information about their provenance, scope and main characteristics; how the data was obtained and selected; labelling procedures (e.g. for supervised learning), data cleaning methodologies (e.g. outliers detection).

In practice it means the following:

Data Quality Management

- **Accuracy**: Ensure that training data is accurate, consistent, and free from significant errors.
  - Use data validation techniques to eliminate inaccuracies.
  - Regularly clean and preprocess data to improve reliability.
- **Completeness**: Collect data that comprehensively covers all scenarios the AI system will encounter.
  - Identify and fill gaps in datasets to avoid under-representation of critical use cases.

- **Timeliness**: Use up-to-date datasets relevant to the context of the AI system's deployment.
  - Continuously refresh data to reflect changes in user behaviour or environmental conditions.

Representativeness

- **Demographic Diversity**: Include datasets reflecting the diversity of populations that the AI system will affect, considering:
  - Age, gender, ethnicity, socio-economic status, and other relevant demographic variables.
- **Context-Specific Representation**: Ensure that data reflects the specific operational environment.
  - Example: For a language model deployed in Europe, ensure linguistic and cultural nuances across EU countries are captured.
- **Edge Case Inclusion**: Identify and incorporate edge cases to ensure performance across a wide range of scenarios.
  - Example: In autonomous vehicles, include rare but critical driving scenarios, such as extreme weather or unusual road conditions.

Bias and risk mitigation

- **Bias Identification**: Conduct statistical analysis to detect biases in the dataset.
  - Use fairness metrics such as disparate impact analysis or equal opportunity measures.
- **Data Balancing**: Correct imbalances by:
  - Over-sampling under-represented groups.
  - Under-sampling over-represented groups.
- **Iterative Testing**: Continuously test for and mitigate unintended biases during development and after deployment.
- **Risk Assessment**: Evaluate the risks associated with the dataset, such as potential biases or quality gaps, and document mitigation plans.
- **Conformity Assessments**: For high-risk systems, perform and document conformity assessments to verify compliance with data quality and representativeness standards.
- **Prohibited Practices**: Ensure data collection and usage avoid practices prohibited under the EU AI Act, such as data that manipulates human behavior in harmful ways.

Transparent Documentation

- **Data Source Traceability**: Document where and how training data was collected.
  - Ensure it adheres to ethical and legal standards, such as GDPR for data privacy.
- **Preprocessing Logs**: Keep records of any modifications made to raw data, such as anonymization, cleaning, or normalization.
- **Stakeholder Transparency**: Share summaries of dataset characteristics, representativeness efforts, and measures taken to mitigate bias with relevant stakeholders, including regulators and users.
- **Detailed technical documentation** according to Annex IV of the AI Act.

Testing and Validation

- **Cross-Dataset Testing**: Validate AI performance using separate, representative test datasets to avoid overfitting or biased outcomes.
- **Stress Testing**: Simulate high-risk scenarios or unusual operational conditions to evaluate system robustness.

- **Performance Metrics**: Track key performance indicators (e.g., accuracy, fairness, and inclusivity) for different demographic and contextual groups.

58. What are the specific obligations for ensuring the explainability of AI system decisions?

The European AI Act establishes several specific obligations – mainly directed at high-risk AI systems – to ensure the explainability of decisions made by AI systems. These obligations are designed to promote transparency, accountability, and the protection of fundamental rights for individuals affected by AI-driven decisions. They collectively ensure that high-risk AI systems are not “black boxes” but are instead transparent, interpretable, and accountable, allowing both deployers and affected individuals to understand, challenge, and seek redress for AI-driven decisions.

The key requirements are as follows:

Transparency and Provision of Information to Deployers: High-risk AI systems must be designed and developed to ensure sufficient transparency, enabling deployers to interpret the system’s output and use it appropriately. This includes:

- Providing clear, complete, correct, and accessible instructions for use, which must include information on the system’s characteristics, capabilities, and limitations of performance.
- Detailing possible known and foreseeable circumstances related to the use of the system, including actions by deployers that may influence system behavior and performance, and under which the system can lead to risks to health, safety, or fundamental rights.
- Including illustrative examples, where appropriate, to enhance the legibility and accessibility of information, such as limitations and intended or precluded uses of the AI system.
- Ensuring that all documentation and instructions are meaningful, comprehensive, and understandable, taking into account the needs and foreseeable knowledge of the target deployers (Article 13 AI Act).

Human Oversight and Interpretability: High-risk AI systems must be designed to allow effective human oversight, which is directly linked to explainability:

- The system must enable natural persons assigned to oversight to properly understand the relevant capacities and limitations of the AI system and to monitor its operation, including detecting and addressing anomalies or unexpected performance.
- Oversight measures must ensure that humans can correctly interpret the system’s output, using available interpretation tools and methods.
- The system must allow the human overseer to decide, in any situation, not to use the AI system or to disregard, override, or reverse its output.
- There must be mechanisms (such as a ‘stop’ button) to intervene in or interrupt the system’s operation if necessary (Article 14 AI Act).

Right to Explanation for Affected Persons: The AI Act grants affected individuals a specific right to obtain an explanation when a deployer’s decision is based mainly on the output of a high-risk AI system and that decision produces legal effects or similarly significantly affects them:

- The explanation must be clear and meaningful, providing the affected person with an understanding of the role of the AI system in the decision-making process and the main elements of the decision taken.
- This right is intended to enable individuals to exercise their rights effectively and is applicable unless already provided for under other Union law or subject to exceptions or restrictions under

Union or national law (Recital 171 and Article 86 AI Act).

Technical Documentation and Traceability: Providers must prepare and maintain technical documentation that demonstrates compliance with the explainability and transparency requirements. This documentation must include:

- A general description of the AI system, its intended purpose, and how it interacts with other systems.
- Detailed information on the system's development, including the logic of the algorithms, key design choices, and the rationale behind them.
- Information on the human oversight measures needed and the technical means to facilitate interpretation of outputs by deployers.
- A description of the system's capabilities and limitations, foreseeable unintended outcomes, and sources of risk to health, safety, and fundamental rights (Annex IV AI Act).

Logging and Record-Keeping: High-risk AI systems must allow for the automatic recording of events (logs) over their lifetime. These logs are essential for:

- Enabling traceability of the system's functioning.
- Facilitating post-market monitoring and compliance verification.
- Supporting the investigation and explanation of decisions made by the AI system (Article 12 AI Act).

Information to Natural Persons: Deployers of high-risk AI systems that make or assist in making decisions related to natural persons must inform those individuals that they are subject to the use of such a system. This information must include:

- The intended purpose of the system.
- The type of decisions it makes.
- The right to an explanation as provided under the Regulation (Recital 93 and Article 26(11) AI Act).

Accessibility of Explanations: All information and explanations provided must be accessible, including to persons with disabilities, ensuring equal access to the rights and remedies established by the Act (Recital 80 and Article 16(l) Ai Act).

59. How do we address the AI Act's requirements for human oversight in AI system deployment?

AI Act stipulates that high-risk AI systems shall be designed and developed in such a way, including with appropriate human-machine interface tools, that they can be effectively overseen by natural persons during the period in which they are in use. The human oversight measures may contain – depending on the risks, level of autonomy and context of use of the high-risk AI system – the following types of measures:

- Appointing a person or a unit for human oversight of the high-risk AI system with the necessary authority and support.
- Providing comprehensive **training program** to natural persons to whom human oversight is assigned on relevant capacities and limitations of the high-risk AI system, possible disfunctions, performance problems, possible anomalies;
- Preparing internal guidelines and procedures for handling AI system malfunctions, ethical dilemmas, or unexpected outcomes and scenarios when the output of the AI system must be disregarded, overridden or reversed or when the operation AI system must be interrupted.
- Conducting fundamental rights assessment which must contain a description of the implementation

of human oversight measures.
- Using AI monitoring tools for supporting human oversight, for example for identifying system errors or biases.
- Regularly reviewing AI system outputs and operator interventions to assess the effectiveness of human oversight.
- Simulating various operational scenarios, including edge cases, to evaluate the AI system's performance under human supervision.
- Incorporating interfaces that allow human operators to monitor AI system decisions in real time. Ensuring that these interfaces display key decision-making metrics and flags for unusual behaviour or errors.

60. What are the implications of the AI Act for AI systems used in high-risk sectors such as healthcare and finance?

Under the AI Act, AI systems intended for use in high-risk sectors such as healthcare and finance must comply with a set of mandatory requirements designed to safeguard fundamental rights, protect health and safety, and ensure robust risk management. In healthcare, for example, AI-based medical devices or diagnostic tools that influence treatment decisions or patient outcomes will be classified as high-risk AI systems where the relevant product legislation requires third-party conformity assessment or these tools otherwise fall within the high-risk uses listed in Annex III of the Act. Practically, this classification entails compliance with key obligations, such as implementation of a risk management system, demonstration of appropriate data governance measures to maintain high-quality datasets, provision of technical documentation, and establishment of mechanisms for meaningful human oversight, depending on the role. These requirements recognise the particular vulnerability of patients and the acute impact that inaccurate or biased AI outputs may have on diagnoses, care pathways, and broader patient well-being.

In the financial sector, AI applications that inform lending decisions, evaluate creditworthiness, or detect fraudulent activity are often regarded as high-risk and therefore attract a similarly rigorous set of obligations. The AI Act underscores that financial institutions and other operators using AI in a high-risk context must ensure that their systems undergo structured pre-deployment assessments and ongoing post-market monitoring. They are also expected to meet transparency duties: for instance, where personal data is processed, the system must facilitate meaningful information for individuals about how decisions are reached and how errors or adverse outcomes can be challenged. The AI Act's risk-based approach means that these high-risk finance systems must undergo strict conformity assessment procedures, which can involve the external involvement of notified bodies or self-assessment if harmonised standards are fully applied. This holistic compliance framework aims to mitigate discrimination in automated credit scoring or loan allocation processes, thereby ensuring that AI-driven decisions in finance are fair, traceable, and properly overseen.

More broadly, the AI Act requires providers in both healthcare and finance to adopt a quality management system that includes detailed recordkeeping and event-logging features so that competent authorities may trace how AI systems typically function and how they respond to real-world data. The systems are also expected to integrate cybersecurity protections and adapt reliability thresholds that match the sector's significance. In healthcare, these thresholds should reflect patient safety imperatives, while in finance they centre on guarding against potentially ruinous financial outcomes or exclusionary practices. Although the AI Act imposes these obligations only on AI systems that meet its high-risk criteria, it potentially applies to a wide range of AI tools within healthcare and finance, reflecting the heightened risks posed in environments where errors may seriously undermine personal welfare, threaten livelihoods, or violate fundamental rights. Overall, the AI Act's requirements

—particularly around risk management, transparency, and human intervention—are intended to ensure that AI systems operate in a manner that is trustworthy, safe, and respectful of natural persons' rights in both of these critical sectors.

Qualification of Deployer vs Providers

61. How do we determine whether we are acting as a deployer or a provider when offering managed AI services or custom AI models?

Definitions under the AI Act. Under Art. 3 (3) of the AI Act, a 'provider' is the person which:

- develops an AI system or a general-purpose AI model or has an AI system or a general-purpose AI model developed, and
- places it on the market or puts the AI system into service under its own name or trademark, whether for payment or free of charge.

On the other hand, under Art. 3 (4), a 'deployer' is a person using an AI system under its authority.

General situation. The distinction between a deployer and a provider is therefore, in general, quite straightforward in the sense that the qualification of a provider goes, as a starting point, with the name or brand used to place the AI system on the market or to put it into service. An entity which provides managed services including a third-party AI system to its own clients, or an entity which customizes a third-party AI system for its own clients or for its own use, should therefore not be considered a provider under the AI Act when such AI system is provided under the third-party's name or trademark.

If it does provide the AI system under its own name or trademark (as agreed upon with the third-party), it will still not become the provider of the AI system where such AI system was previously developed and placed on the market (i.e. first made available on the EU market) or put into service (i.e. supply of an AI system for first use directly to the deployer or for own use in the Union for its intended purpose) by the third party.

The qualification may be more complex if the AI system provided by a third-party is modified and further developed by a new entity: if it becomes a new AI system, the entity modifying such AI system to place it on the market or put it into service under its own name or trademark would be considered the provider.

Derogation for high-risk systems. A specific rule applies for high-risk systems (Article 25 of the AI Act). This article derogates to the definition of a provider since an entity would become a provider by meeting any of these conditions, even if the system has already been placed on the market or put into service by a third party:

Putting its name or trademark on a high-risk AI system (irrespective of the contractual arrangements), even if it did not develop or modify the system.

Making a substantial modification to such high-risk AI system, in such a way that it remains a high-risk AI system, even if it does not put its name or trademark.

Modifying the intended purpose of an AI System in such a way that it becomes high risk AI.

In such case, the initial provider will no longer be considered a provider and will cooperate with the

new provider to make available information and reasonable technical access or assistance (except if the initial provider specified that the system should not be changed into a high-risk AI system in which case there is no obligation to hand over the documentation).

62. What are the specific obligations for providers and deployers in cases where AI systems are customized for individual clients?

In any arrangement where an AI system will undergo customisation for a deployer, both parties – but especially the deployer – ought to carefully consider the impact that this may have on their roles and responsibilities under the AI Act before commencing the customisation. This is because the AI Act sets out a number of scenarios in which deployers of high-risk AI systems may also become providers under the AI Act, which will result in them being subject to the AI Act's far more extensive provider obligations.

This change of roles is dealt with in Article 25, which sets out three scenarios in which deployers may be considered providers: the deployer (1) puts their name or trade mark on a high-risk AI system, without prejudice to any contractual arrangements stipulating that the obligations are otherwise allocated (Article 25(1)(a)), (2) makes a 'substantial modification' (as defined in the AI Act) to a high-risk AI system (Article 25(1)(b)), or (3) modifies the intended purpose of a non-high-risk AI system, such that it becomes high-risk (within the classification rules set out in Article 6) (Article 25(1)(c)).

Where Article 25 applies, and the deployer is considered a new provider of the customised AI system, the initial provider will not be considered to be a provider of that specific system under the AI Act.

The deployer should determine in advance of the proposed customisation whether or not it will result in them being considered a provider, in order to ensure that they comply with the provider obligations in the AI Act in respect of the customised system. It is unlikely that a deployer who makes this determination retrospectively will have complied with such obligations.

Where a provider itself undertakes the customisation for a deployer, the provider should remain provider of the customised AI system (and this should not result in the deployer being considered the provider). However, in this scenario the deployer will nevertheless be considered the provider of the customised AI system if the system is a high-risk AI system and the deployer deploys it under their own name or trade mark (Article 25(1)(a)), or the system is not high-risk but the deployer modifies its intended purpose or uses it in a way that it becomes high-risk (Article 25(1)(c)).

The AI Act envisages that where the deployer deploys a customed high-risk AI system under their own name or trade mark (Article 25(1)(a)), such that the deployer will be considered the provider of the system, the deployer and initial provider may contractually agree that the provider will remain responsible for the provider obligations in the AI Act. Notwithstanding that agreement, the deployer will still be considered the provider under the AI Act (which makes sense in this scenario, because this is what most end users will understand to be the case based on the name or trade mark that is applied to the system).

Where customisation is undertaken by a deployer, a key factor in determining whether they will be considered a provider is whether the customisation amounts to a 'substantial modification'. This is defined in the AI Act as being any change to an AI system that is made after it is put on the market or put into service which is not foreseen or set out in the initial conformity assessment carried out by the provider, and which affects the compliance of the AI system with the requirements for high-risk AI systems set out in the AI Act or modifies the intended purpose for which the AI system has been assessed.

Ideally, deployers will have the opportunity to analyse the initial conformity assessment or documentation that provides equivalent information before any modification is made, in order to understand whether they will be considered a provider. In any event, the intended purpose of a high-risk AI system and any changes to it and its performance that have been pre-determined by the provider should be set out in the instructions for use. The instructions for use are a key compliance document for deployers of high-risk systems. They should be made available by the provider along with the system. If the proposed customisation has been pre-determined in the instructions for use, deployers will not be considered providers of the customised high-risk AI system. If it is not possible to determine whether the proposed customisation will amount to a 'substantial modification' based on a review of the documentation available to the deployer, technical analysis of the system may be required (again, before any modification commences).

Where customisation is taking place as part of a multi-party project, complexity will arise where the provider, deployer and/or other third parties (such as a service provider acting on behalf of either the provider or deployer) may each have a role in customising the AI system. The AI Act does not expressly deal with this scenario. Therefore, before any modification is commenced, the parties should carefully document in a written agreement their respective roles and obligations, so that even if they cannot alter their statutory obligations as providers of the customised system, they have a contractual arrangement between them that clearly allocates responsibility for delivering the provider obligations and ensuring requirements of the AI Act are met in case of any enforcement action.

If the customisation does result in the deployer being considered a provider of a high-risk AI system, the initial provider will be obliged by the AI Act to closely cooperate with the new provider and make available necessary information and provide reasonable technical access and assistance to enable the new provider to comply with the obligations in the AI Act. Note that this obligation will not apply where the initial provider clearly specified that its system is not to be changed into a high-risk AI system (another reason why deployers need to fully understand the situation before making changes to an AI system).

If the customised AI system is not a high-risk AI system (and therefore is outside of the scope of Article 25), deployers should consider whether the customisation changes their role pursuant to other regulatory regimes. For example, if they apply their name or trade mark to the system or make a substantial modification to it, they may be deemed to be a manufacturer of it for the purposes of the General Product Safety Regulation (EU 2023/998) and be subject to the obligations of the manufacturer in that Regulation.

Whether a proposed customisation will result in a deployer being considered a provider will require a factual analysis on a case-by-case basis. Key factors to be considered include the following:

- Whether or not the AI system is high-risk;
- Who is undertaking the customisation;
- Whether the deployer will put a high-risk AI system into use under their own name or trade mark;
- The extent of the customisation being undertaken and whether this results in 'substantial modification' to a high-risk AI system that remains high-risk;
- The deployer's intended use of the customised AI system and whether this means that the deployer's use will be 'high-risk' in accordance with Article 6;
- The intended purpose of the AI system and any pre-determined changes set out by the provider in the initial conformity assessment and/or the instructions for use;
- Whether any other regulations will apply to the deployer as a result of the customisation.

63. How do we ensure compliance with the AI Act when transitioning from a deployer to a provider role or vice versa?

Understanding the transition between deployer and provider roles

Under the EU AI Act, the roles of "deployer" and "provider" are clearly defined, each carrying distinct legal obligations. A "provider" is the natural or legal person who develops an AI system or has it developed and places it on the market or puts it into service under their name or trademark. A "deployer" is any natural or legal person, including public authorities, who uses an AI system under their authority, except when used for personal non-professional activities. When a company transitions from being a deployer to a provider, or vice versa, it must carefully assess which obligations apply to its new role and ensure that all relevant requirements are met for the AI system in question.

Obligations when assuming the provider role

If a company, previously acting as a deployer, modifies an AI system in a way that it becomes a high-risk AI system, or changes its intended purpose such that it now falls under the high-risk category, the company is considered a provider under the AI Act and must assume all provider obligations. This includes ensuring the system’s compliance with all requirements for high-risk AI systems, such as conducting a conformity assessment, maintaining technical documentation, implementing a quality management system, and drawing up an EU declaration of conformity. The company must also ensure the system is appropriately CE marked, register the system in the EU database, and provide comprehensive instructions for use. If the company puts its name or trademark on an existing high-risk AI system, it similarly assumes the provider’s responsibilities. The original provider is no longer responsible for the system in these circumstances but must cooperate with the new provider by supplying necessary information and technical access, unless it has expressly excluded such changes.
Obligations when assuming the deployer role
Conversely, when a company transitions from provider to deployer—such as when it begins using an AI system it has not developed or placed on the market—it must comply with the deployer’s obligations. These include using the AI system in accordance with the instructions for use, assigning human oversight to competent and trained staff, monitoring the system’s operation, and keeping relevant logs. Deployers must also inform affected individuals when high-risk AI systems are used in decision-making processes, conduct fundamental rights impact assessments where required, and cooperate with competent authorities. If the deployer makes substantial modifications to the system or changes its intended purpose, it may again become the provider and must fulfil all associated obligations. Throughout any transition, companies must ensure robust documentation, clear contractual arrangements, and ongoing cooperation with other parties in the AI value chain to maintain compliance and legal certainty.

Summary of practical steps

- Assess whether your activities or modifications to an AI system trigger a change in role under the AI Act.
- When becoming a provider, ensure full compliance with all provider obligations: conformity assessment, technical documentation, quality management, CE marking, registration, and comprehensive instructions for use.
- When acting as a deployer, follow all deployer obligations: use the system as instructed, assign trained human oversight, monitor operation, keep logs, inform affected persons, and conduct impact assessments where required.
- Ensure clear contractual arrangements and cooperation with other parties in the AI value chain, especially when roles change.
- Maintain robust documentation and record-keeping to support compliance and facilitate regulatory

oversight.
- Regularly review and update compliance practices in line with evolving legal requirements and technological developments.

Gap Analysis for High-Risk AI Systems (Medical Devices)

64. What are the specific requirements for obtaining CE marking for high-risk AI systems that are also medical devices?

Providers of high-risk AI systems are required to undergo a conformity assessment procedure, either based on the internal control referred to in Annex VI AI Act, or on the assessment of the quality management system and the technical documentation, with the involvement of a notified body, as set out in Annex VII AI Act. This less burdensome procedure is only available to providers of high-risk AI systems if they comply with harmonized standards and, where applicable, any common specifications referred to in Article 41 of the AI Act.

If the high-risk AI system qualifies as a medical device, the manufacturer must undergo the relevant conformity assessment procedures in accordance with the MDR and incorporate the established requirements for high-risk AI systems (e.g. establishment, implementation, and maintenance of a risk management system, provision of technical documentation, automatic recording of events, extensive transparency obligations) into the evaluation (Article 43 (3) AI Act). For this assessment the notified body shall review the technical documentation and, where necessary to perform its duties, be granted full access to the training, validation, and testing datasets. It may also request additional evidence or testing from the provider, and, upon a reasoned request, gain access to the AI system's training and trained models, including relevant parameters.

The handling of changes to high-risk AI systems that have already undergone a conformity assessment procedure is governed by Article 43 (4) AI Act. In the case of a substantial modification, the system must undergo a new conformity assessment procedure, regardless of whether it will be further distributed or continue to be used by the current deployer. A substantial modification occurs when changes to the system go beyond what was pre-determined and documented in the technical documentation at the time of the initial assessment.

Where high-risk AI systems are subject to other Union harmonization legislation which also requires an EU declaration of conformity, a single EU declaration of conformity shall be drawn up in respect of all Union law applicable to the high-risk AI system (for example, in the case of software as a medical device, this would include both the MDR and the AIA). The declaration shall contain all the information required to identify the Union harmonization legislation to which the declaration relates (Article 47 (3) AI Act).

65. How do we ensure continuous compliance and post-market monitoring for high-risk AI systems in the healthcare sector?

Providers of AI systems must establish a post-market monitoring system. This system must be based on a post-market monitoring plan that enables providers to continuously assess whether their systems comply with the requirements for high-risk AI systems (Chapter III Section 2 AI Act; Articles 8 et seq. AI Act). The post-market monitoring system shall actively collect, document, and analyse relevant data on the AI systems' performance throughout their lifetime, using input from deployers or other sources.

For providers of high-risk AI systems subject to the EU harmonization legislation listed in Annex I, Section A AI Act it is possible to rely on an already established post-market surveillance system, provided that the monitoring plan for the AI system is integrated into the existing system and ensures an equivalent level of protection (Article 72 (4) AI Act).
The AI Act obligates providers of high-risk AI systems to report serious incidents to the competent market surveillance authorities of the Member States where that incident occurred. The deadlines for reporting depend on the severity of the incident, staggered at 15 days as a general rule, and 10 days in cases involving fatalities. The report must contain comprehensive information about the incident, details of any investigations carried out, risk assessments performed, and any corrective measures adopted.

By contrast, Articles 83 to 95 of the MDR set out the framework for post-market surveillance of medical devices, establishing a system of administrative intervention powers. Under Article 95 of the MDR, competent authorities may order mandatory corrective measures if there is an unacceptable risk to health or safety. In addition, the MDR also provides for administrative measures if a product does not meet the requirements of the MDR, even if there is no immediate health or safety risk. Article 98 MDR expands the authorities' powers under Articles 95 and 97 of the MDR and permits measures to be taken where there are indications of potential risks.

Conversely, Article 82 AI Act also permits measures against AI systems that comply with the act if, following an assessment, such systems nonetheless pose a risk to health. This provision introduces a structural difference in the level of protection: while the MDR exercises restraint with regard to compliant products, the AI Act clearly goes further. This approach may lead to regulatory uncertainty for AI-based medical devices, as the AI Act partially supersedes or challenges existing post-market surveillance mechanisms under the MDR. It thus remains questionable whether such an expansion of post-market oversight by the AI Act is compatible with the goals set forth in the MDR (Article 94 MDR).

You might also be interested in this!

International Digital Regulation Hub | CMS

Artificial Intelligence

Looking ahead to the EU AI Act

Digital Regulation Tracker Tool

PUBLICATION PDF 420.1 KB

AI procurement clauses template high risk

Download

PUBLICATION PDF 389.5 KB

AI procurement clauses template non high risk

Download

Key Contacts

Dóra Petrányi
Budapest, London
Partner
Global TMIC Practice Group Leader

Tom Jozak
Amsterdam
Of Counsel

Authors

Tom Jozak
Amsterdam
Of Counsel

David Rappenglück
Brussels - EU Law Office
Senior Associate
Rechtsanwalt

Daniel Gallagher
London
Senior Associate

Sarah Hopton
London
Senior Associate

Dr Dirk Spacek, LL.M.
Zurich
Partner
Co-Head of the practice groups TMC and IP

Javier Torre de Silva
Madrid
Partner

Márton Domokos
Budapest
Senior Counsel
Co-ordinator of the CEE Data Protection Practice, CMNO

Julie Tamba
Associate
left_cms

Dr. Anne-Marie Toledo-Wolfsohn
Counsel
left_cms

Anna Zsófia Horváth
Budapest
Associate

Katalin Horváth
Budapest
Partner

Adriana Zdanowicz - Leśniak
Warsaw
Counsel

Johannes Juranek
Vienna
Managing Partner

Jennie Nilsson
Stockholm
Partner