CMS
law·tax·future

2024 EU AI Act: a detailed analysis

March 2025

2024 EU AI Act: a detailed analysis

Tom Jozak[1]

SUMMARY

The European Union (EU) has taken a significant step towards regulating artificial intelligence (AI) with the introduction of the regulation for Artificial Intelligence: the AI Act.[2] This regulation aims to establish harmonised rules for the development, marketing, and use of AI systems[3] within the EU, ensuring safety, protecting fundamental rights, and promoting innovation while preventing market fragmentation.

Effective from 1 August 2024, this comprehensive regulation addresses various risk aspects with the development and use of AI technology. Among others, it regulates AI systems and AI models, obligations for providers and deployers of AI systems, prohibited practices, high-risk systems, transparency obligations, obligations of providers of general-purpose AI models with systemic risk, enforcement regime and many more. The regulation's primary objective is to create a trustworthy and human-centric approach to AI, balancing the need for technological advancement and innovation with the protection of individual rights and public interests.

This article aims to offer a current understanding of the AI Act's implications for all stakeholders involved in the AI ecosystem and those interested in what this new EU law gives through a detailed analysis.

1. MATERIAL AND TERRITORIAL SCOPE

1.1 Material Scope

Encompassing a wide range of applications, products and IT systems, the material scope of the AI Act is notably broad. The scope includes AI systems used in various sectors, such as healthcare, finance, insurance, transportation, and education. The act aims to address the unique challenges and risks associated with each sector by covering a diverse array of systems and applications. For instance, AI systems used in healthcare involve sensitive medical data and require stringent data protection measures, while AI systems in finance also need to comply with specific regulatory requirements to prevent fraud and ensure transparency.

1.2 Territorial Scope

Providers placing AI systems or general-purpose AI models on the EU market must comply with the AI Act, irrespective of whether these providers are established within the EU or in a third country. This means that any entity, regardless of its geographical location, which intends to introduce AI systems or general-purpose AI models into the EU market must comply with the regulations set forth in the AI Act. The Act also extends its applicability to deployers of AI systems that have their place of establishment or are located within

---

[1] Tom Jozak LL.M., is an Of Counsel IP/TMC at CMS Netherlands, strategic legal advisor specialised in digital regulations and regulatory compliance with focus on AI, data protection, cybersecurity and IT from a combination of corporate, IT and legal expertise.

[2] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (AI Act).

[3] Article 3(1) AI Act: "'AI system' means a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.". The Commission has published non-binding guidelines on AI system definition to explain the practical application of this legal concept: Commission Guidelines on the definition of an artificial intelligence system established by AI Act, https://ec.europa.eu/newsroom/dae/redirection/document/112455. These guidelines are subject to evolving opinion of the Commission, in light of practical experiences, new questions and use cases that arise.

the EU. This includes organisations and individuals using AI systems within the EU, ensuring that the deployment of AI technologies adheres to the established standards and requirements.

Furthermore, the AI Act encompasses providers and deployers of AI systems located in third countries where the output produced by the AI system is used in the EU. This provision ensures that AI systems developed or operated outside the EU but whose outputs impact the EU market are subject to the same regulatory scrutiny.

Additionally, the act covers importers and distributors of AI systems, product manufacturers placing AI systems on the market or putting them into service under their own name or trademark, authorised representatives of providers not established in the EU, and affected persons located in the EU. This comprehensive scope ensures that all relevant stakeholders involved in the AI ecosystem are accountable for compliance with the AI Act.

The territorial scope of the AI Act is very comprehensive, ensuring that all AI systems or general-purpose AI models impacting the EU market are subject to the same regulatory standards. This approach is crucial in maintaining a level playing field for all stakeholders and preventing regulatory arbitrage, where entities might seek to exploit less stringent regulations in other jurisdictions. The AI Act promotes fairness and accountability in the AI ecosystem by holding all providers and deployers to the same standards.

1.3 Exceptions

The regulation does not apply to areas intentionally placed outside the scope of the AI Act, such as military, defence, or national security purposes. AI systems specifically developed and put into service for the sole purpose of scientific research and development are also excluded from the act's purview. This exclusion is intended to foster innovation and scientific advancement without imposing regulatory burdens that could hinder research activities.

Additionally, the AI Act does not affect the application of other EU law on the protection of personal data, privacy, and the confidentiality of communications. These areas are governed by existing legal frameworks, such as the General Data Protection Regulation (GDPR)[4], ensuring that data protection and privacy rights are upheld in the context of AI system deployment.

In summary, the AI Act's material and territorial scope is designed to ensure that all relevant stakeholders, regardless of their location, are accountable for the safe and ethical deployment of AI systems or general-purpose AI models within the EU. By establishing a comprehensive regulation with broad territorial scope like the GDPR, the act aims to advance a trustworthy and human-centric approach to AI, balancing the need for innovation with the protection of fundamental rights and public interests.

2. AI LITERACY

The AI Act emphasises the importance of AI literacy[5] among providers and deployers of AI systems. Providers and deployers are required to take measures to ensure a sufficient level of AI literacy among their staff and other persons dealing with the operation and use of AI systems on their behalf.[6] This includes considering the technical knowledge, experience, education, and training of the individuals involved, as well as the context in which the AI systems are to be used

[4] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[5] Article 3(56) AI Act: "'AI literacy' means skills, knowledge and understanding that allow providers, deployers and affected persons, taking into account their respective rights and obligations in the context of this Regulation, to make an informed deployment of AI systems, as well as to gain awareness about the opportunities and risks of AI and possible harm it can cause;".

[6] Article 4 AI Act.

and the persons or groups of persons on whom the AI systems are to be used.

The act aims to equip individuals with the necessary skills and understanding to effectively and responsibly engage with AI technologies by promoting AI literacy. AI literacy encompasses a broad range of competencies, including the ability to understand and interpret AI outputs, recognise the limitations and potential biases of AI systems, and make informed decisions based on AI-generated insights.

Providers and deployers must ensure that their staff are well-versed in these areas to maximise the benefits of AI while minimising risks. This involves providing ongoing training and education programmes that keep pace with the rapid advancements in AI technology. Requiring a culture of continuous learning and adaptation is crucial to maintaining a high level of AI literacy within organisations. The specific use cases and applications of AI systems can vary significantly, and the required level of literacy may differ accordingly. For instance, individuals working with AI systems in healthcare may need specialised knowledge related to medical data and ethical considerations, while those in the financial sector may require expertise in algorithmic trading, credit scoring practices and regulatory compliance. By tailoring AI literacy initiatives to the specific needs of different sectors and use cases, providers and deployers can ensure that their staff are adequately prepared to handle the unique challenges and opportunities presented by AI technologies.

The AI Act also highlights the role of AI literacy in promoting public trust and acceptance of AI technologies. By ensuring that individuals are knowledgeable about AI and its implications, the act aims to build a foundation of trust that is essential for the widespread adoption of AI systems. This trust is particularly important in sectors where AI has a direct impact on individuals' lives, such as healthcare, education, and law enforcement. AI literacy initiatives can help mitigate fears and misconceptions about AI, paving the way for its responsible and ethical use by supporting transparency and understanding. Likewise, the AI Act encourages collaboration between various stakeholders, including industry, academia, and civil society, to develop and implement AI literacy programmes. This collaborative approach ensures that AI literacy initiatives are comprehensive and inclusive, addressing the diverse needs and perspectives of different communities. A sustainable AI literacy framework, able to adapt to the evolving landscape of AI technology, can be created by leveraging the expertise and resources of multiple stakeholders.

AI literacy is a critical component of the AI Act even though it was added late in the legislative process. It reflects the EU's commitment to fostering a knowledgeable and responsible AI ecosystem. By equipping individuals with the necessary skills and understanding, the act aims to maximise the benefits of AI while minimising its risks. Through ongoing education, tailored training programmes, and collaborative efforts, AI literacy will remain a priority in the development and deployment of AI technologies within any type of organisation.

3. PROHIBITED AI PRACTICES

From February 2025, the AI Act prohibits placing on the market, putting into service and using certain AI practices or AI systems that are deemed to pose unacceptable risks to fundamental rights, safety, and public interests.[7]

[7] Article 5 AI Act. Note that 'making available on the market' means the supply of an AI system or a general-purpose AI model for distribution or use on the EU market in the course of a commercial activity, whether in return for payment or free of charge. According to Article 3(9) AI Act, the placing on the market of an AI system is 'the first making available of an AI system […] on the Union market'. 'Making available' is defined in Article 3(9) AI Act as the supply of the system for distribution or use on the Union market in the course of a commercial activity, whether in return for payment or free of charge. 'Putting into service' means the supply of an AI system for first use

Harmful manipulation and deception. These prohibited practices include AI systems that deploy subliminal techniques, which are designed to manipulate an individual's subconscious, to materially distort a person's behaviour in a manner that causes or is likely to cause physical or psychological harm. This involves embedding hidden messages within media content that are below the threshold of conscious perception, such as flashing certain incentivising messages for a fraction of a second during what in first instance seems an informative video. This can influence viewers' behaviour without their awareness, and can lead them to make purchases they wouldn't have otherwise considered. Such practices are considered highly manipulative and can undermine an individual's autonomy and decision-making capacity. By prohibiting these techniques, the AI Act aims to protect individuals from covert and potentially harmful influences.

Exploitation of vulnerabilities. Another prohibited practice involves AI systems that exploit vulnerabilities of specific groups of persons due to their age, physical or mental disability, in a manner that causes or is likely to cause physical or psychological harm. For example, AI algorithms can analyse online behaviour to target children with advertisements for products that may not be suitable for their age. This can include promoting unhealthy foods, age-inappropriate content, or addictive games. This provision is designed to safeguard vulnerable populations from being targeted and manipulated by AI systems that take advantage of their specific physical characteristics. By addressing these concerns, the AI Act seeks to ensure that AI technologies are used ethically and do not exacerbate existing inequalities or discrimination.

Social scoring. The AI Act also prohibits the use of AI systems for the evaluation or classification of the trustworthiness of natural persons based on their social behaviour or known or predicted personal or personality characteristics, leading to detrimental or unfavourable treatment. In some countries, AI systems are used to detect welfare fraud by analysing large datasets to identify patterns of behaviour deemed suspicious. For example, the Netherlands implemented an automated system risk indication (SyRI) application to identify potential welfare fraud. However, the profiling algorithm was found to disproportionately target low-income neighbourhoods and minority groups for fraud investigations, leading to discrimination. Such practices, often referred to as social scoring, result in unjust and discriminatory outcomes, affecting individuals' access to services, opportunities, and rights.[8] By banning social scoring, the AI Act aims to prevent the misuse of AI for surveillance and control purposes, thereby protecting individuals' privacy and dignity.

Other prohibited practices under the AI Act include:

- **Individual criminal offence risk assessment and prediction**. Ban on AI systems predicting criminal behaviour based solely on profiling or personality traits, except when supporting human assessment based on objective facts.
- **Untargeted scraping to develop facial recognition databases**. Prohibition on AI systems creating or expanding facial recognition databases through untargeted

directly to the deployer or for own use in the EU for its intended purpose (Article 3(11) AI Act). The 'use' should be interpreted "in a broad manner covering the use or deployment of the system an any moment of its lifecycle after having been placed on the market or put into service," according to the Commission Guidelines on prohibited artificial intelligence practices (https://ec.europa.eu/newsroom/dae/redirection/document/112367).

[8] ECLI:NL:RBDHA:2020:1878, The Hague District Court, C-09-550982-HA ZA 18-388; The court has decided that SyRI as a legal instrument by the Dutch government to detect various forms of fraud, including social benefits, allowances, and taxes fraud does not comply with Article 8 of the European Convention on Human Rights (ECHR), which protects the right to respect for private and family life, home and correspondence.

scraping of images from the internet or CCTV footage.

- **Emotion recognition**. Ban on AI systems inferring emotions in workplaces and educational institutions, except for medical or safety reasons.
- **Biometric categorisation**. Prohibition on AI systems categorising individuals based on biometric data to infer sensitive attributes like race, political opinions, or sexual orientation, except for lawful law enforcement purposes.
- **Real-time remote biometric identification**. Additionally, the AI Act restricts the use of AI systems for real-time remote biometric identification (RBI) in publicly accessible spaces for law enforcement purposes, except under specific conditions and with appropriate safeguards. RBI, such as facial recognition, can have significant implications for privacy and civil liberties. The act mandates that such technologies should only be used in exceptional circumstances[9], with strict oversight and safeguards to prevent abuse and ensure compliance with fundamental rights. By setting these limitations, the AI Act aims to balance the potential benefits of biometric identification for security purposes with the need to protect individuals' rights and freedoms.

The prohibition of these AI practices reflects the EU's commitment to upholding fundamental rights and ensuring that AI technologies are used in a manner that respects human dignity and autonomy. The AI Act seeks to create a safe and ethical environment for the development and deployment of AI systems by identifying and banning practices that pose significant risks. This approach not only protects individuals from harm but also fosters public trust in AI technologies, which is essential for their widespread adoption and acceptance.

Moreover, the AI Act's focus on prohibiting manipulative and exploitative practices highlights the importance of ethical considerations in AI development. By setting clear boundaries on what is acceptable, the act encourages providers and deployers to prioritise ethical principles in their AI initiatives. This emphasis on ethics is crucial in ensuring that AI technologies contribute positively to society and do not perpetuate harmful behaviours or biases.

In addition to the specific prohibitions outlined in the act, the AI Act also encourages ongoing monitoring and assessment of AI practices to identify emerging risks and address them proactively. This dynamic approach ensures that the regulatory framework remains relevant and effective in the face of rapid technological advancements. The AI Act aims to stay ahead of potential threats and safeguard the public interest by continuously evaluating and updating the list of prohibited practices.

The AI Act's prohibition of certain AI practices underscores the EU's commitment to protecting fundamental rights and promoting ethical AI development. The act aims to create a safe and trustworthy AI ecosystem that benefits all individuals and society as a whole by banning manipulative, exploitative, and discriminatory practices. Through ongoing monitoring and ethical considerations, the AI Act yet seeks to ensure that AI technologies are used responsibly and contribute positively to the advancement of society.

[9] Article 5(1)(h) AI Act refers to the following specific circumstances: (i) the targeted search for specific victims of abduction, trafficking in human beings or sexual exploitation of human beings, as well as the search for missing persons; (ii) the prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or a genuine and present or genuine and foreseeable threat of a terrorist attack; (iii) the localisation or identification of a person suspected of having committed a criminal offence, for the purpose of conducting a criminal investigation or prosecution or executing a criminal penalty for offences referred to in Annex II AI Act and punishable in the EU member state concerned by a custodial sentence or a detention order for a maximum period of at least four years.

4. HIGH-RISK AI SYSTEMS

High-risk AI systems are subject to specific requirements and obligations under the AI Act.[10] These systems are classified as high risk if they meet certain criteria, such as being intended to be used as a safety component of a product or being themselves products covered by the EU harmonisation legislation listed in Annex I of the AI Act. High-risk AI systems also include those listed in Annex III of the AI Act, which covers areas of biometric identification, critical infrastructure, education, employment, essential private and public services, law enforcement, migration, asylum, border control management, and administration of justice and democratic processes.

The classification of high-risk AI systems is based on the potential impact these systems can have on individuals' rights, safety, and well-being. An AI system listed in Annex III is not to be considered high risk where it does not pose a significant risk of harm to the health, safety or fundamental rights of natural persons, including by not materially influencing the outcome of decision making (e.g. where no adverse impacts on physical, psychological health or financial interests are likely to occur).[11]

4.1 Requirements for high-risk AI systems for providers

The AI Act outlines several requirements[12] that providers of high-risk AI systems must comply with to ensure their safe and ethical deployment, including the following:

Risk management system. One of the key requirements under the AI Act is the establishment of a risk management system for providers of high-risk AI systems. They must establish, implement, document, and maintain a risk management system throughout the entire lifecycle of the high-risk AI system. The risk management system should identify, analyse, estimate, evaluate, and address known and reasonably foreseeable risks to health, safety, and fundamental rights. Implementing a robust risk management system, enables providers to proactively mitigate potential risks and ensure that their AI systems operate safely and ethically.

Data and data governance. Another critical requirement for high-risk AI systems is data and data governance. High-risk AI systems that use techniques involving the training of AI models with data must be developed based on training, validation, and testing data sets that meet quality criteria. These data sets should be subject to appropriate data governance and management practices. Ensuring the quality and integrity of data used in AI systems is essential to prevent biases, inaccuracies, and other issues that could compromise the system's performance and fairness.

Technical documentation and record-keeping. Providers of high-risk AI systems are also required to draw up and keep up-to-date technical documentation before placing the high-risk AI system on the market or putting it into service. This documentation should demonstrate compliance with the requirements and provide necessary information for national competent authorities and notified bodies to assess compliance. By maintaining comprehensive technical documentation, providers can ensure transparency and accountability in the development and deployment of high-risk AI systems. To ensure a level of traceability of the functioning of a high-risk AI system that is appropriate to the intended purpose of the system, logging capabilities must enable the

[10] Chapter III AI Act – High Risk AI Systems; Article 6 AI Act.

[11] See examples in recital 53 AI Act: "[…] where the AI system is intended to perform a narrow procedural task, such as an AI system that transforms unstructured data into structured data, an AI system that classifies incoming documents into categories; an AI system that is used to detect duplicates among a large number of applications; or an AI system detecting deviations in decision-making patterns."

[12] Chapter III, Section 2 AI Act – Requirements for high-risk AI systems.

recording of events relevant for specific events, data and situations.[13]

Transparent information. Transparency and the provision of information are also a crucial compliance element for high-risk AI systems. These systems must be accompanied by instructions for use in an appropriate digital format, including concise, complete, correct, and clear information relevant to deployers. This information should enable deployers to understand the system's capabilities, limitations, and potential risks, allowing them to use an AI system responsibly and effectively.

Human oversight. Human oversight is another essential requirement for high-risk AI systems. Providers must ensure that high-risk AI systems are designed to enable human oversight, allowing natural persons to understand the system's capacities and limitations, monitor its operation, interpret its output, and intervene or interrupt the system if necessary. Through provisions on human oversight, the AI Act aims to prevent over-reliance on AI systems and ensure that human judgment and intervention remain integral to decision-making processes where natural persons can be severely affected.

Accuracy, robustness and cybersecurity. High-risk AI systems must be robust, accurate, and secure. Providers must implement measures to ensure the performance and reliability of these systems, as well as to mitigate risks to health, safety, and fundamental rights. This includes addressing potential cybersecurity threats and vulnerabilities that could compromise the system's integrity and functionality. By adhering to these requirements, providers can ensure that high-risk AI systems operate safely and effectively, minimising potential harms and maximising their benefits.

Quality management system. Finally, providers of high-risk AI systems must establish a documented quality management system (QMS) to ensure compliance with the AI Act. This system should include strategies for regulatory compliance, design and development procedures, quality control, testing and validation processes, technical specifications, data management systems, risk management, post-market monitoring, incident reporting, communication handling, record-keeping, resource management, and an accountability framework. The implementation should be proportional to the provider's size but must maintain the required level of protection and compliance as prescribed by the act. Providers which are already subject to sectoral EU law or financial institutions with internal governance requirements may integrate these aspects into their existing systems or be deemed to be fulfilling these requirements by complying with the rules on internal governance arrangements or processes pursuant to the relevant EU financial services law.

4.2 Requirements for high-risk AI systems for deployers

Deployers of high-risk AI systems are mandated to adhere to a comprehensive set of requirements to ensure compliance with the AI Act.[14] An overview of the key obligations is provided hereunder.

Firstly, deployers must implement appropriate technical and organisational measures to use high-risk AI systems in accordance with the instructions for use provided by the system's provider. They are required to assign human oversight to competent, trained, and authorised natural persons, ensuring these individuals have the necessary support to perform their oversight duties effectively.

Deployers must also ensure that input data is relevant and sufficiently representative for the intended purpose of the high-risk AI system, particularly when they exercise control over such data. Continuous monitoring of the AI system's operation is an essential element of compliance,

[13] See Article 12(2) AI Act.

[14] Article 26 AI Act.

and deployers must inform providers of any identified risks or serious incidents without undue delay, suspending the AI system's use where risks become too high. Additionally, deployers are required to maintain logs automatically generated by the high-risk AI system for a period appropriate to the system's intended purpose, with a minimum duration of six months, unless otherwise specified by applicable EU or national law.

Prior to deploying a high-risk AI system in the workplace, deployers who are employers must inform workers' representatives and affected workers about the system's use, adhering to relevant EU and national laws and practices. Furthermore, deployers must use the information provided by deployers to fulfil their obligation to conduct a data protection impact assessment as required under the GDPR or Directive (EU) 2016/680.[15]

In the context of law enforcement, deployers must seek authorisation from a judicial or administrative authority for the use of post-remote biometric identification systems, except for initial identification of potential suspects based on objective and verifiable facts directly linked to the offence. Deployers must also inform natural persons that they are subject to the use of high-risk AI systems, particularly in law enforcement contexts, in accordance with Directive (EU) 2016/680. Lastly, deployers are required to cooperate with relevant competent authorities in any actions taken to implement the AI Act.

These stringent requirements for deployers aim to ensure the responsible deployment and oversight of high-risk AI systems, safeguarding fundamental rights and public interests. In practice, this means that deployers must be vigilant in their use of AI systems, ensuring that they are used ethically and in compliance with all relevant regulations. They must also be proactive in identifying and mitigating any potential risks associated with the AI systems, ensuring that any issues are promptly addressed to prevent harm. This comprehensive approach helps to build trust in AI technologies and ensures that their deployment contributes positively to society.

5. TRANSPARENCY OBLIGATIONS

The transparency obligations outlined in the AI Act are designed to ensure that AI systems are developed and deployed in a manner that respects fundamental rights and promotes public trust. By requiring providers and deployers to inform natural persons about their interaction with AI systems, the act aims to prevent deception and misuse of AI technologies. The detailed documentation and logging requirements for high-risk AI systems further enhance accountability and facilitate oversight.

To support the effective implementation of the transparency obligations, the AI Act establishes the European Artificial Intelligence Office (AI Office). The AI Office is responsible for overseeing the compliance of AI systems with the transparency requirements and providing guidance to providers and deployers.

The AI Office also plays a key role in facilitating cooperation and information sharing among national authorities, industry stakeholders, and civil society organisations. It is tasked with developing templates and best practices for transparency documentation and ensuring that these resources are accessible to all relevant parties. These measures collectively contribute to the responsible and trustworthy use of AI systems in the EU.

[15] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

5.1 Providers Transparency

Informing natural persons. The AI Act imposes transparency obligations on providers of AI systems to ensure that natural persons are informed about their interaction with AI systems. These obligations are crucial for maintaining trust and ensuring that individuals are aware of when they are engaging with AI technologies. The transparency obligations are designed to cover various aspects of AI system interactions, including the nature of the interaction, the origin of the content, and the processing of personal data.

Providers must ensure that AI systems intended to interact directly with natural persons are designed and developed in a way that informs the natural persons concerned that they are interacting with an AI system, unless this is obvious from the context. This requirement is particularly important for AI systems that may not be immediately recognisable as such, ensuring that users are not misled or deceived. The AI Act emphasises that the notification should be clear and understandable, considering the characteristics of the target audience, including vulnerable groups such as children or persons with disabilities.

Stakeholder involvement. The AI Act recognises the importance of stakeholder involvement in the development and deployment of AI systems. It encourages providers to engage with relevant stakeholders, including civil society organisations, industry representatives, and experts, to ensure that the systems are designed and used in a manner that respects fundamental rights and promotes public trust. The act also emphasises the need for transparency in the decision-making processes related to AI systems, including the criteria used for system design, development, and deployment.

Logging and record-keeping. The AI Act also mandates that providers of high-risk AI systems must implement robust logging and record-keeping practices. These practices are essential for ensuring traceability and accountability in the event of an incident or malfunction. The logs should include information about the system's operation, including the input data, the processing steps, and the output generated. This information is crucial for investigating and addressing any issues that may arise during the system's deployment. Providers must ensure that the logs are securely stored and protected against unauthorised access or tampering.

Codes of conduct. Furthermore, the AI Act includes provisions for the development of voluntary codes of conduct for AI systems that are not classified as high risk. These codes of conduct are intended to promote the adoption of transparency and accountability measures across the AI industry. Providers of non-high-risk AI systems are encouraged to adhere to these codes of conduct to demonstrate their commitment to ethical AI practices. The AI Office is responsible for *supporting* the development and distribution of these codes of conduct and for monitoring their implementation.

Stricter obligations for high-risk AI systems. Notably, the AI Act outlines specific transparency obligations for high-risk AI systems. High-risk AI systems are subject to stricter transparency requirements to ensure that their deployment does not result in harm or discrimination. Providers of high-risk AI systems must ensure that their systems are accompanied by detailed documentation that includes information about the system's capabilities, limitations, and potential risks. This documentation should be made available to deployers and relevant authorities to facilitate oversight and accountability.

AI Marking. Providers of AI systems generating synthetic audio, image, video, or text content must make certain that the outputs are marked in a machine-readable format and detectable as artificially generated or manipulated. This measure is intended to prevent the spread of misinformation and to ensure that users can distinguish between real and synthetic content.

The AI Act specifies that the marking should be robust and resistant to tampering, ensuring that the artificial nature of the content remains detectable even if the content is altered or shared across different platforms. This measure will of course require continuous development as tampering possibilities advance with technological advancements.

5.2 Deployers Transparency

Informing natural persons, codes of conduct, stakeholder involvement and high-risk AI transparency obligations, which apply for providers are also relevant for deployers of AI systems. Additionally, the following transparency obligations apply specifically for deployers.

Use in accordance with provider's instructions. Deployers are responsible for ensuring that the high-risk AI systems are used in accordance with the instructions provided by the providers. Furthermore, deployers must monitor the system's performance and report any incidents or malfunctions to the relevant authorities. Deployers are also required to conduct regular assessments of the system's impact on fundamental rights and take appropriate measures to mitigate any identified risks. This includes implementing human oversight measures to ensure that the system's outputs are interpreted and used correctly.

Emotion recognition and biometric categorisation. Deployers of emotion recognition systems or biometric categorisation systems must inform natural persons exposed to these systems about their operation and process personal data in accordance with applicable data protection laws. The AI Act mandates that this information should include details about the purpose of the system, the types of data being collected, and how the data will be used. Additionally, deployers must ensure that the systems are designed to respect privacy and data protection principles, such as data minimisation and purpose limitation. Be reminded that biometric categorisation systems that are based on natural persons' biometric data, such as an individual person's face or fingerprint, to deduce or infer an individuals' political opinions, trade union membership, religious or philosophical beliefs, race, sex life or sexual orientation are prohibited.[16]

Employers. Before putting into service or using a high-risk AI system at the workplace, deployers who are employers must inform workers' representatives and the affected workers that they will be subject to the use of the high-risk AI system. This information should be provided, where applicable, in accordance with the rules and procedures laid down in EU and national law and practice on information of workers and their representatives.[17]

Deep fakes. Deployers of AI systems that generate or manipulate image, audio, or video content constituting a deep fake must disclose that the content has been artificially generated or manipulated. This disclosure is essential to prevent the misuse of deep fake technology for malicious purposes, such as spreading false information or impersonating individuals. The AI Act requires that the disclosure be made in a

[16] Article 5(1)(g) AI Act.

[17] See in this context also a clarification of this requirement provided in recital (57) of the AI Act: "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, should also be classified as high-risk, since those systems may have an appreciable impact on future career prospects, livelihoods of those persons and workers' rights. Relevant work-related contractual relationships should, in a meaningful manner, involve employees and persons providing services through platforms as referred to in the Commission Work Programme 2021. Throughout the recruitment process and in the evaluation, promotion, or retention of persons in work-related contractual relationships, such systems may perpetuate historical patterns of discrimination, for example against women, certain age groups, persons with disabilities, or persons of certain racial or ethnic origins or sexual orientation. AI systems used to monitor the performance and behaviour of such persons may also undermine their fundamental rights to data protection and privacy."

manner that is clear and easily understandable, ensuring that viewers are aware of the artificial nature of the content. The information for natural persons concerned must be provided in a clear and distinguishable manner at the latest at the time of the first interaction or exposure. The provided information should also conform to the applicable accessibility requirements. This means that the information must be accessible to all individuals, including those with disabilities, and should be provided in a format that is easy to understand. The AI Act highlights the importance of using plain language and avoiding technical jargon to ensure that the information is comprehensible to a broad audience. Additionally, the information should be available in multiple languages custom for EU countries where the AI system is being used, as appropriate, to cater to the diverse population of the EU.

6. GENERAL-PURPOSE AI MODELS

General-purpose AI models, including large generative AI models, present unique innovation opportunities, but also some challenges. These models are typically trained on large amounts of data through various methods such as self-supervised, unsupervised, or reinforcement learning. They can be placed on the market in various ways, including through (computer programme) libraries, application programming interfaces (APIs), as direct downloads, or as physical copies. These models may be further modified or fine-tuned into new models. Although AI models are essential components of AI systems, they do not constitute AI systems on their own. AI models require the addition of further components, such as a user interface, to become AI systems.

The AI Act provides specific rules for general-purpose AI models, including those that pose systemic risks.[18] Systemic risks result from particularly high capabilities: a general-purpose AI model should be considered to present systemic risks if it has high-impact capabilities or significant impact on the internal market due to its reach. High-impact capabilities in general-purpose AI models mean capabilities that match or exceed the capabilities recorded in the most advanced general-purpose AI models.[19] The full range of capabilities in a model and associated risks can only be understood after it has been placed on the market or when deployers interact with the model. Consequently, adequate risk mitigation measure can only be introduced following the interaction with these general-purpose AI models, which presents a risk on its own. For this reason, where a general-purpose AI model meets these conditions, the provider must notify the EU Commission without delay and in any event within two weeks after that requirement is met or it becomes known that it will be met. That notification must include the information necessary to demonstrate that the relevant requirement classifying general-purpose AI model as general-purpose AI model with systemic risk has been met. Also, the Commission may on its own decide to designate an AI model as an AI model with systemic risk, if it becomes aware of a general-purpose AI model presenting systemic risks of which it has not been notified.

6.1 Measuring Model Capabilities for Systemic Risk Classification

A general-purpose AI model shall be classified as a general-purpose AI model with *systemic risk* if it has high impact capabilities. These are evaluated on the basis of appropriate technical tools and methodologies, including indicators and benchmarks.

Moreover, according to the state of the art at the time of entry into force of the AI Act, the

[18] Article 3(65) AI Act: "'systemic risk' means a risk that is specific to the high-impact capabilities of general-purpose AI models, having 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;".

[19] Article 3(64) AI Act.

cumulative amount of computation used for the training of the general-purpose AI model measured in floating point operations[20] is one of the relevant estimates for model capabilities. The cumulative amount of computation used for training includes the computation across the activities and methods that are intended to enhance the capabilities of the model prior to deployment, such as pre-training, synthetic data generation, and fine-tuning. Therefore, an initial threshold of floating point operations is set under the AI Act, which, if met by a general-purpose AI model, leads to a *presumption* that the model is to be considered a general-purpose AI model with systemic risks.[21] This threshold can be adjusted over time to reflect technological and industrial changes, such as algorithmic improvements or increased hardware efficiency, and should be supplemented with benchmarks and indicators for model capability.

To enable provisioning of the relevant further information, the AI Office will engage with the scientific community, industry, civil society, and other experts. Thresholds, as well as tools and benchmarks for the assessment of high-impact capabilities, are strong predictors of generality, its capabilities, and associated systemic risk of general-purpose AI models. They consider the way the model will be placed on the market or the number of users it may affect. The AI Act provides specific rules for general-purpose AI models, including those that pose systemic risks.

6.2 Technical and Organisational Measures

Providers of general-purpose AI models are required to in any event undertake the following technical and organisational measures, as well as those described in chapter 9 – Governance, Risk Management and Responsible AI of this article, in achieving compliance with the AI Act.

- **Technical documentation**. Providers are required to prepare and maintain comprehensive and current technical documentation for their AI models. This documentation must cover various aspects, including a general description of the model, its intended tasks, and the types of AI systems it can be integrated into. It should also detail acceptable use policies, release date, distribution methods, architecture, number of parameters, and the modality and format of inputs and outputs. Additionally, the documentation must include the model's licence, a detailed description of its elements and development process, design specifications, optimisation goals, and information on the data used for training, testing, and validation. Furthermore, it should specify the computational resources employed and the known or estimated energy consumption of the model.
- **Information and documentation for deployers**. Providers should make relevant information and documentation available to AI system deployers who intend to integrate the general-purpose AI model. This information should provide a clear understanding of the model's capabilities and limitations to ensure compliance with AI Act obligations. It should include a general description of the model, acceptable use policies, release date, distribution methods, and interaction details with hardware or software not part of the model. Additionally, it should cover versions of relevant software,

[20] Article 3(67) AI Act: "'floating-point operation' means any mathematical operation or assignment involving floating-point numbers, which are a subset of the real numbers typically represented on computers by an integer of fixed precision scaled by an integer exponent of a fixed base;". Floating-point numbers are used in computing to represent very large or very small numbers that cannot be accurately represented as simple integers. They are essential in various scientific calculations, simulations, and AI algorithms where precision and range are crucial.

[21] Article 51(2) AI Act: "A general-purpose AI model shall be presumed to have high impact capabilities pursuant to paragraph 1, point (a), when the cumulative amount of computation used for its training measured in floating point operations is greater than 10^{25}.".

architecture, number of parameters, modality and format of inputs and outputs, the model's licence, and a description of the model elements and development process. Information on the data used for training, testing, and validation, including type, provenance, and curation methodologies, should also be provided.

- **Copyright law compliance**. Providers are required to establish a policy to comply with EU copyright and related rights laws, including identifying and adhering to rights held by rightsholders. Providers are also required to create and publicly share a summary of the content used to train the AI model. This summary should be comprehensive enough to enable parties with legitimate interests, including copyright holders, to enforce their rights under EU law, simultaneously protecting trade secrets and confidential business information. The summary should also list the main data collections or sets, such as large private or public databases or archives, and provide a narrative explanation of other data sources utilised.
- **Summary of training content**. Finally, providers should prepare and make publicly available a detailed summary of the content used for training the AI model. This summary should include information on the type and provenance of data, curation methodologies applied, and any other relevant details that enhance transparency about the training process. This will facilitate parties with legitimate interests, including copyright holders, in exercising and enforcing their rights under EU law.

7. INNOVATION AND AI REGULATORY SANDBOXES

In addition to these primary objectives, the AI Act also emphasises the importance of ethical AI development.[22] The act requires AI systems to be designed and used in a manner that respects fundamental rights and EU values, such as human dignity, privacy, and non-discrimination. The regulatory sandboxes play an important role in ensuring that AI technologies adhere to these ethical standards by providing a space for thorough testing and evaluation.

The AI regulatory sandboxes[23] provide a controlled experimentation and testing environment to ensure compliance with the AI Act and other relevant laws. These sandboxes allow developers to experiment with AI technologies in a safe space, where they can identify and mitigate potential risks before deploying their systems in the real world. This controlled setting helps in refining AI models and improving their robustness and reliability.

The sandboxes also improve the oversight and understanding of AI opportunities, emerging risks, and impacts, facilitating regulatory learning for authorities and undertakings. By operating within the regulatory sandbox, developers and regulators can work closely to understand the implications of AI technologies, ensuring that they comply with existing laws and regulations. This collaboration helps in creating a clear legal framework that supports innovation while protecting public interests.

The AI regulatory sandboxes encourage cooperation and sharing of best practices among authorities, standardisation organisations, notified bodies, testing and experimentation facilities, research labs, and other stakeholders.

[22] See recital 27 AI Act: "While the risk-based approach is the basis for a proportionate and effective set of binding rules, it is important to recall the 2019 Ethics guidelines for trustworthy AI developed by the independent AI HLEG appointed by the Commission. In those guidelines, the AI HLEG developed seven non-binding ethical principles for AI which are intended to help ensure that AI is trustworthy and ethically sound. The seven principles include human agency and oversight; technical robustness and safety; privacy and data governance; transparency; diversity, non-discrimination and fairness; societal and environmental well-being and accountability.".

[23] Article 57 AI Act.

The sandboxes serve as a platform for various stakeholders to collaborate, share knowledge, and develop standardised practices for AI development. This cooperation is crucial for building a cohesive AI ecosystem that promotes trust and transparency in the EU.

The AI regulatory sandboxes also aim to remove barriers for SMEs, including start-ups, and accelerate access to markets. Moreover, the sandboxes provide SMEs with the resources and support they need to bring their AI innovations to market more quickly. By reducing regulatory hurdles and offering a supportive environment, the AI Act aims to level the playing field for smaller enterprises, fostering a more diverse and competitive AI market.

8. CODES OF CONDUCT AND GUIDELINES

The AI Act encourages the development of codes of conduct and guidelines to facilitate the proper application of the regulation. The European Artificial Intelligence Board (the Board) and the AI Office will in cooperation with EU member states support the drawing up of codes of conduct, which may cover:

- **Voluntary application of requirements**. Fostering the voluntary application of some or all requirements set out in the AI Act to AI systems other than high-risk AI systems. This includes encouraging providers and deployers to adopt best practices and standards that align with the ethical principles for trustworthy AI.
- **Ethical guidelines**. Promoting the application of EU ethical guidelines for trustworthy AI. These guidelines emphasise the importance of human-centric AI, which serves as a tool for people with the ultimate aim of increasing human well-being. The guidelines also stress the need for AI systems to be transparent, accountable, and non-discriminatory, ensuring they align with EU values and fundamental rights.
- **Environmental sustainability**. Assessing and minimising the impact of AI systems on environmental sustainability. This involves developing AI systems in a sustainable and environmentally friendly manner, monitoring and assessing their long-term impacts on society and democracy, and ensuring that AI development aligns with the European Declaration on Digital Rights and Principles for the Digital Decade.[24]
- **AI literacy**. Promoting AI literacy among persons dealing with the development, operation, and use of AI. The Board and the AI Office will – together with the EU member states – support initiatives to enhance public awareness and understanding of the benefits, risks, safeguards, rights, and obligations related to AI systems. This includes facilitating the drawing up of voluntary codes of conduct to advance AI literacy and improve working conditions, ultimately sustaining the innovation path of trustworthy AI in the EU.
- **Inclusive and diverse design**. Facilitating the inclusive and diverse design of AI systems, including the establishment of diverse

[24] European Commission, Policy and Legislation, *European Declaration on Digital Rights and Principles,* 15 December 2022, https://digital-strategy.ec.europa.eu/en/library/european-declaration-digital-rights-and-principles. The European Declaration on Digital Rights and Principles outlines the EU's commitment to a human-centric digital transformation. The promotion and implementation of the declaration is a shared political commitment and responsibility of the EU and its member states within their respective competences and in full compliance with EU law. It emphasises the protection of human rights, democracy, and inclusion in the digital age, ensuring that offline rights are upheld online. [Cont.] The declaration promotes ethical principles, digital skills, and access to digital public services while safeguarding privacy, security, and sustainability. It calls for solidarity and inclusion, fair working conditions, freedom of choice in digital interactions, and the protection of children and young people online. Additionally, it advocates for a sustainable digital environment and the responsible use of technology to address climate change. The declaration serves as a guiding framework for policymakers, businesses, and international partners, aiming to foster a fair, inclusive, and resilient digital society in the EU.

development teams and stakeholder participation. This ensures that AI systems are developed with attention to vulnerable persons and accessibility for persons with disabilities, promoting equality and non-discrimination. The involvement of relevant stakeholders such as business, civil society organisations, academia, research organisations, trade unions, and consumer protection organisations is crucial in the design and development of AI systems.

9. GOVERNANCE, RISK MANAGEMENT AND RESPONSIBLE AI

Setting up AI Governance and implementing a centralised risk assessment framework is crucial for managing AI risks. This involves establishing criteria for risk management and ensuring that the right stakeholders, including legal, compliance, and technical teams, are involved in the decision-making process. This also includes forming AI governance committees or boards that are responsible for setting policies, monitoring compliance, and ensuring the ethical use of AI. These structures provide oversight and accountability, helping to align AI projects with organisational goals and regulatory requirements.

Centralised risk assessment, clear policies, guidelines, AI literacy and AI solution ownership helps in identifying potential risks early in the process and in developing strategies to prevent and mitigate them. It is equally essential to allow for decentralised deployment of AI technologies. This means empowering business units to innovate and deploy AI solutions while adhering to the centralised legal, risk and compliance management criteria. This approach balances the business's need for innovation with the necessity of risk control by its internal legal, risk and compliance departments, and supported by external experts where needed.

Creating sandboxes and using synthetic data for testing AI models can significantly reduce risks. Sandboxes provide a controlled environment where AI models can be tested without impacting live systems or data. Using synthetic data ensures that sensitive or proprietary information is not exposed during the testing phase. Careful design of AI use cases is another important control. This involves identifying clear objectives, understanding the potential risks and benefits, and ensuring that the AI system is designed to meet specific business needs. Appropriate use case design helps in minimising unintended consequences and maximising the value derived from AI technologies.

Providing training and raising awareness among employees about AI risks and best (data protection) compliance practices is essential and a mandatory requirement under the AI Act. This includes educating staff on how to use AI responsibly, understanding the limitations of AI systems, and recognising potential ethical and legal implications. Well-informed and knowledgeable employees give their companies a head-start as they are better equipped to adequately prevent, manage and mitigate AI risks.

Developing and enforcing ethical guidelines for responsible AI use is utterly important. These guidelines should cover aspects such as fairness, transparency, accountability, and privacy. Adhering to pre-established ethical principles helps in building trust with stakeholders and ensuring that AI technologies are used in a socially responsible manner.

Finally, implementing operational controls such as regular audits, monitoring, and reporting mechanisms can help in maintaining the integrity and performance of AI systems. These controls ensure that AI models are functioning as intended and that any deviations or issues are promptly identified and addressed.

10. PENALTIES

The penalties framework in the AI Act is designed to address various levels of non-compliance,

ensuring that all entities, regardless of their size, adhere to the established rules and principles.

Non-compliance with the AI practices prohibited under Article 5 of the AI Act can result in administrative fines up to EUR 35 million or 7% of the offender's total worldwide annual turnover, whichever is higher.[25] This significant financial penalty underscores the seriousness with which EU legislators view prohibited AI practices and serves as a strong deterrent against such violations.

Other infringements related to operators or notified bodies, excluding those under Article 5, can incur fines up to EUR 15 million or 3% of the total worldwide annual turnover. Providing incorrect, incomplete, or misleading information to authorities can lead to fines up to EUR 7.5 million or 1% of the total worldwide annual turnover.

For SMEs, including start-ups, fines are capped at the lower of the specified percentages or amounts. When determining fines, authorities must consider the nature, gravity, and duration of the infringement, the operator's size and market share, and any mitigating or aggravating factors. The penalties must be effective, proportionate and dissuasive but they need to take into account the interests of SMEs, including start-ups, and their economic viability. Cooperation with authorities and the degree of responsibility and technical measures taken by the operator[26] are also relevant factors.

Furthermore, the AI Act specifies penalties for non-compliance with specific requirements or obligations set forth in the regulation. In these cases, administrative fines can be as high as EUR 750,000. While this amount is lower than the fines for prohibited practices and other provisions, it still represents a substantial financial burden for many entities, particularly SMEs and start-ups.

In addition to financial penalties, the AI Act also includes other enforcement measures to ensure compliance. These measures may include orders to cease operations, mandatory corrective actions, and increased monitoring and reporting requirements. By implementing a range of enforcement measures, the AI Act aims to create a robust compliance environment that encourages adherence to the regulation while also providing flexibility in addressing different types of non-compliance.

EU member states must define the extent to which administrative fines can be imposed on public authorities and bodies. The imposition of fines may be carried out by national courts or other competent bodies, ensuring equivalent effects across the EU. The exercise of these powers must adhere to procedural safeguards, including judicial remedies and due process. EU member states must annually report fines issued and any related legal proceedings to the Commission.

The AI Act also emphasises the importance of transparency and accountability in the enforcement process. EU member states are required to publish information about penalties and enforcement actions, providing a clear and public record of non-compliance and the corresponding consequences. This transparency serves as an additional deterrent against violations and reinforces the overall integrity of the regulation.

11. GRADUAL APPLICATION

The AI Act came into force on 1 August 2024 but many of its key obligations only start to apply from 2025. Further application is as follows:

[25] Article 99(3) AI Act.

[26] Article 3(8) AI Act. "Operator" means a provider, product manufacturer, deployer, authorised representative, importer or distributor of an AI system or general-purpose AI model.

- Prohibited practices and AI literacy obligations apply from 2 February 2025;
- General-purpose AI models, governance, confidentiality obligations and penalty framework start to apply from 2 August 2025;
- The other provisions, excluding high-risk AI system proviso in article 6(1), apply from 2 August 2026;[27]
- Article 6(1) AI Act and the corresponding obligations apply from 2 August 2027;[28]
- The evaluation of the AI Act and reporting about its effectiveness, including the functioning of the AI Office, take place from 2 August 2028;[29]
- Providers and deployers of high-risk AI systems that are to be used by public authorities must have taken the necessary steps to comply with the requirements and obligations of the AI Act by 2 August 2030;
- Finally, AI systems that are components of the large-scale IT systems listed in Annex X of the AI Act and placed on the market or put into service before 2 August 2027 must be brought into compliance with this Regulation by 31 December 2030.[30]

12. CONCLUSION

The EU AI Act represents a landmark regulatory framework aimed at harmonising the development, deployment, and use of AI systems within the European Union. By establishing comprehensive rules and obligations for AI system providers and deployers as well as other actors in the AI value chain, the act seeks to ensure the safety, transparency, and ethical deployment of AI technologies.

Key takeaways are the prohibition of certain AI practices deemed to pose unacceptable risks, the emphasis on AI literacy and public trust, the stringent requirements for high-risk AI systems, the comprehensive material and territorial scope, the importance of transparency obligations, the specific rules for general-purpose AI models, the role of AI regulatory sandboxes, and the development of codes of conduct and guidelines. The act's material and territorial scope is designed to hold all relevant stakeholders accountable, regardless of their geographical location, thereby preventing regulatory arbitrage and promoting a level playing field.

Moreover, the AI Act underscores the importance of continuous monitoring and assessment of AI practices to address emerging risks proactively. The establishment of the AI Office and the development of voluntary codes of conduct further enhance the regulatory framework's robustness. The act also introduces significant penalties for non-compliance, ensuring that entities adhere to the established guidelines and principles. By fostering a trustworthy and human-centric approach to AI, the EU AI Act aims to balance the need for innovation with the protection of fundamental rights and public interests, ultimately contributing to the responsible and ethical advancement of AI technologies in the EU and beyond.

AI technologies and their associated risks continuously evolve. Because AI is expected to transform all technology in the coming decades, it is important to adopt a mindset of continuous improvement, advancing responsible AI development and use. This involves regularly reviewing and updating governance and operational controls to keep pace with technological advancements and emerging risks. Through an understanding of the act, following the legal developments and taking the steps described in this article, businesses can effectively prevent, manage and mitigate AI risks beyond regulatory requirements, ensuring the safe and ethical development and deployment of AI technologies.

[27] Article 113 AI Act.

[28] Article 113(c) AI Act.

[29] Article 112 (2) AI Act.

[30] Article 111(1) AI Act.

CMS Law-Now™

Your free online legal information service.

A subscription service for legal articles on a variety of topics delivered by email.
cms-lawnow.com

CMS locations:

Aberdeen, Abu Dhabi, Amsterdam, Antwerp, Barcelona, Beijing, Belgrade, Bergen, Berlin, Bogotá, Bratislava, Brisbane, Bristol, Brussels, Bucharest, Budapest, Casablanca, Cologne, Cúcuta, Dubai, Dublin, Duesseldorf, Edinburgh, Frankfurt, Funchal, Geneva, Glasgow, Gothenburg, Hamburg, Hong Kong, Istanbul, Johannesburg, Kyiv, Leipzig, Lima, Lisbon, Liverpool, Ljubljana, London, Luanda, Luxembourg, Lyon, Madrid, Manchester, Maputo, Mexico City, Milan, Mombasa, Monaco, Munich, Muscat, Nairobi, Oslo, Paris, Podgorica, Poznan, Prague, Reading, Rio de Janeiro, Riyadh, Rome, Santiago de Chile, São Paulo, Sarajevo, Shanghai, Sheffield, Singapore, Skopje, Sofia, Stavanger, Stockholm, Strasbourg, Stuttgart, Tel Aviv, Tirana, Vienna, Warsaw, Zagreb and Zurich.
