FROM MINIMAL RISK TO PROHIBITED PRACTICES: THE AI ACT RISK SPECTRUM FOR AI SYSTEMS

Join us as we uncover the latest insights into the European Union's (the '**EU**') ground-breaking Artificial Intelligence Act, in the wake of the leak of its most recent consolidated version on 26 January 2024 [i]. We delve herein into the core objectives, risk-based categorisation, and key provisions of this text, originally proposed by the European Commission on 21 April 2021 and now nearing adoption (the '**AI Act**').

Starting with its primary objective, the AI Act aims to enhance the functioning of the internal market by establishing a uniform legal framework for the development, marketing, and use of artificial intelligence systems (the '**AI systems**') within the EU. This framework is to be applied in accordance with EU values, to ensure a high level of protection of health, safety and fundamental rights enshrined in the Charter of Fundamental Rights of the EU.

The AI Act introduces a risk-based approach for AI systems, similar to the GDPR's data protection rules. This approach distinguishes three AI systems, based on the risk posed by their usage: Low or Minimal Risk AI Systems, High-Risk AI Systems, and Prohibited (or unacceptable) AI Systems. Occasionally, a fourth level is also mentioned in some papers published online: the 'transparency risk' or 'limited risk'.

This risk differentiation stands out from Recital (14) of the AI Act, which currently states the following:

"It is therefore necessary to prohibit certain unacceptable artificial intelligence practices, to lay down requirements for high-risk AI systems and obligations for the relevant operators, and to lay down transparency obligations for certain AI systems".

Below is a table detailing the three risk levels of AI systems, along with examples of AI systems for each risk level, and listing some requirements and obligations associated with each of those levels.

	Low or Minimal Risk AI Systems (Not referred to *per se* by the AI Act but in EC's Explanatory Memorandum, p. 12)	High-Risk AI Systems (Articles 6 to 51 AI Act)	Prohibited AI Systems (Article 5 AI Act)
Description	AI systems are considered low or minimal risk AI systems whenever they create a low or minimal risk to individuals with regards to the impact they have on the health, safety, and fundamental rights of persons in the EU. Depending on a certain number of criteria, this may include AI systems that do not materially influence decision-making or do not substantially harm legal interests. These AI systems are largely unregulated by the AI Act and may freely be used. The AI Act contains no provision	AI systems are considered high-risk AI systems, and subject to specific requirements, whenever they have a significant harmful impact on the health, safety, and fundamental rights of persons in the EU. High-risk AI systems include those systems that are used: – as **remote biometric identification** systems, **or** for biometric categorisation (assigning people to specific categories based on their biometric data), **or** for emotion recognition; – as safety components in the management and operation of **critical infrastructures**, **road**	AI systems are considered prohibited AI systems whenever they can provide novel and powerful tools for manipulative, exploitative and social control practices, contradicting EU values of respect for human dignity, freedom, equality, democracy, the rule of law, as well as fundamental rights. Prohibited AI systems include those systems: – that deploy **subliminal techniques** beyond a person's consciousness or that deploy purposefully manipulative or deceptive

	specifically concerning the broad category of low or minimal risk AI systems. Low or minimal risk AI systems include those systems that are used for the following purposes: - Video games bots; - Spam filters; - Some current chatbots, - Some current domestic virtual assistants; - AI-enhanced educational tools; - AI for recommendations. Nevertheless, certain low or minimal risk AI systems may be subject to specific obligations (e.g., some chatbots). See below.	**traffic** and the supply of water, gas, heating, and electricity; – to determine access to **educational and vocational training** institutions, **or** to evaluate learning outcomes, **or** to assess the appropriate level of education of a person, **or** for monitoring and detecting prohibited behaviour of students during tests in the context of education and vocational training institutions; – for **recruitment or HR selection of persons**, **or** to make decisions affecting work-related relationships, **or** to allocate tasks based on behaviour or personal characteristics, **or** to monitor performance/behaviour in such relationships; – to **evaluate creditworthiness**, **or** to establish credit scores, **or** to establish priorities in the dispatching of emergency first response services, **or** to perform risk assessments and pricing in relation to people for life and health insurance purposes; – by public authorities, to evaluate a person's **eligibility for essential public** assistance benefits and services; – by law enforcement authorities, to assess the **risk of a person for offending or becoming a potential victim** of criminal offences, **or** to serve as a polygraph and similar tools, **or** to detect the emotional state of a person, **or** to evaluate the reliability of evidence during an investigation/prosecution of criminal offences, **or** to predict criminal offences based on people profiling, **or** for profiling people during the detection, investigation, or prosecution of criminal offences;	techniques, with the objective to or the effect of distorting a person's or a group of peoples' behaviour by impairing a person's ability to make an informed decision; – that **exploit vulnerabilities** of a person or a specific group of people due to their age, disability or a specific social or economic situation; – that **categorise a person 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; – for **evaluation or classification of a person** or group of people over a certain period, based on their social behaviour or on their personal/personality characteristics (**social credit scoring**); – used for **'real time' remote biometric identification** in publicly accessible spaces by authorities, for the purpose of law enforcement (unless such use is strictly necessary for certain objectives listed by the AI Act); – used for practices where such use of artificial intelligence infringes other EU law.

		– by public authorities, to serve as a polygraph and similar tools; – by public authorities, to assess a **risk posed by a person entering in the territory of an EU Member State**, **or** to examine applications for asylum/visa/residence permits, **or** for the purpose of detecting, recognising, or identifying people (**border control**); – by a judicial authority, **to interpret facts or the law**, and to apply the law to a set of facts; and – for **influencing the outcome of an election** or referendum or peoples' voting behaviour.	
Possible examples	**Siri (Apple, Inc.)** – **What it does:** Siri is a voice-controlled virtual assistant. It is designed to respond to voice commands and perform tasks such as answering questions, setting reminders, sending messages, and controlling smart devices. – **Why it may be low risk:** Siri primarily assists users with voice-based tasks and information retrieval. While it can perform various functions, it typically does not make decisions that have a significant impact on individuals' lives. **Grammarly (Grammarly, Inc.)** – **What it does:** Grammarly is a grammar and spell-checking tool that provides suggestions for writing. – **Why it may be low risk:** Grammarly is limited to	**IBM Watson for Oncology (International Business Machines Corporation)** – **What it does:** IBM Watson assists oncologists in diagnosing cancer, recommending personalised treatment options, and providing insights into cancer care. – **Why it may be high-risk:** IBM Watson may be considered a high-risk AI system due to its role in cancer diagnosis and treatment. Inaccuracies or errors in its recommendations, including in in the dispatching of emergency services, could have severe consequences for cancer patients. **Clearview AI (Clearview AI, Inc.)** – **What it does:** Clearview AI offers facial recognition often used by law enforcement agencies and organisations. – **Why it may be high-risk:** Clearview AI is classified as a	**Sesame Credit (Alibaba Group)** – **What it does:** Sesame Credit is a social credit scoring system in the People's Republic of China. It uses a wide range of data to assess and rate the trustworthiness of individuals. – **Why it may be prohibited:** Sesame Credit raises concerns due to its use of personal and sensitive data to generate scores based on individuals' social behaviour over a certain period. This practice has the potential for profound impacts and could lead to discrimination (an EU fundamental right). **Deepfake Generators for Impersonation of a deceased companion**

	providing writing assistance and does not influence any critical or high-stake decisions.	high-risk AI system due to its use in remote biometric identification with potential for abuse and misuse, which can lead to infringement of personal freedoms and fundamental rights.	– **What it does:** it creates realistic videos and audio that impersonate a deceased loved one. – **Why it may be Prohibited:** High potential to exploit vulnerabilities of a specific group of people due to their age.
Obligations	Certain AI systems and general-purpose models (see paragraphs under this table), which also may include low or minimal risk AI systems, are subject to transparency obligations (Art. 52 AI Act). Providers and deployers of these AI systems must therefore inform individuals whenever: – the AI system is intended to directly interact with people, and it may not be obvious that they are interacting with such AI systems from the point of view of someone reasonably well-informed, observant, and circumspect; – the AI system is used for emotion recognition; – the AI system is used for biometric categorisation (assigning people to specific categories based on their biometric data, relating to sex, age, hair colour, eye colour, tattoos, behavioural or personality traits, language, religion, membership of a national minority, sexual or political orientation); and – the AI system generates or manipulates image, audio or video content that resembles existing persons, places, or events and would	High-risk AI systems can only be placed on the EU market or put into service if they comply with mandatory requirements that ensure, *inter alia*, that they do not pose unacceptable risks to important EU public interests. High-risk AI systems must comply with the following requirements: – have an implemented, documented, and maintained risk management system; – be tested to ensure that it performs consistently with its intended purpose and that it is compliant with applicable requirements; – be developed based on training, validation and testing data sets that meet the quality criteria; – have technical documentation drawn up before that system is placed on the market or put into service, which must be kept up-to date (transparency); – allow for the automatic recording of events ('logs'); – be designed and developed to ensure that its operation is sufficiently transparent to achieve compliance with user/provider obligations and to enable its appropriate use; – be accompanied by user instructions in a digital format or that include concise, complete, correct, and clear information (transparency);	Placing prohibited AI systems on the market, putting them into service or using them is an unacceptable practice that is fully prohibited by the AI Act. An EU Member State may however decide to provide for the possibility to authorise the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement within certain limits and conditions.

	falsely appear to a person to be authentic ('deep fakes').	– be designed and developed to be overseen by natural persons; – be designed and developed to achieve an appropriate level of accuracy, robustness, and cybersecurity and perform consistently in those respects; – be resilient to errors, faults, or inconsistencies, and to unauthorised attempts to alter its use, outputs, or performance by exploiting the system vulnerabilities; and – be developed to eliminate or reduce the risk of biased outputs influencing input for future operations ('feedback loops'). Furthermore, obligations applicable to 'certain AI systems' and listed at the end of the column on 'low or minimal risk AI systems', may equally be applicable to high-risk AI systems. The requirements and obligations applicable to high-risk AI systems are without prejudice to the obligations applicable to the providers, deployers and other potential operators of high-risk AI systems (e.g., compliance with the registration obligations).	

The AI Act also briefly touches upon the so-called general-purpose AI systems.

These AI systems are based on or integrate a general-purpose AI model with the capability of serving a variety of purposes (Article 3(44e) AI Act; Recital (60d) AI Act). However, the AI Act contains no specific requirement or obligation for general-purpose AI systems. Instead, it focuses on general-purpose AI models, which serve as a foundation of these general-purpose AI systems. This may include some of OpenAI's ChatGPT models.

A general-purpose AI model may be placed on the market in various ways, including through libraries, application programming interfaces (APIs) or as a direct download (Recital (60a) AI Act). They allow for flexible generation of content (such as text, audio, images, or video) and can readily accommodate a wide range of tasks (Recital (60c) AI Act).

General-purpose AI models are essential components of some AI systems, but they do not constitute AI systems on their own – notably because they lack further components to be considered as such, for example, a user interface (Recital (60a) AI Act). Therefore, contrary to

what some papers may suggest, they are not inherently an AI system, nor do they fall in one of the existing three risk categories of AI systems.

Providers of general-purpose AI models are nevertheless subject to specific requirements and obligations (Article 52c AI Act), including draw up technical documentation, a policy to respect EU copyright law, and a detailed summary about the content used for training. Furthermore, since general-purpose AI models may be integrated or form part of many different AI systems (including high-risk AI systems), they may pose a systemic risk. In such cases where the AI model meets the criteria to be classified as having a systemic risk, providers are subject to additional obligations (Articles 52d and 52e AI Act).

When the provider of a general-purpose AI model integrates their model into their own AI system, the obligations provided for general-purpose AI models may apply in addition to those for AI systems (Recital (60a) AI Act).

In conclusion, the EU's AI Act represents a significant step forward in the regulation of AI systems. Its goal is to bring the rules for the development, marketing, and use of these systems into uniformity within the EU while maintaining a high level of protection for health, safety, and fundamental rights of EU citizens.

It also presents new opportunities and challenges, for which MOLITOR’s Media, Data, Technology, and IP team can offer its comprehensive expertise. On the one hand, we can assist clients in understanding and complying with the AI Act, particularly with high-risk AI systems and transparency obligations. On the other hand, we can assist you in either exercising your personal data rights or complying with the GDPR's obligations relating to personal data in the AI field. This includes the drafting of terms and conditions for the deployment and usage of AI systems, as well as privacy policies and data processing agreements.

Please contact us should you require our assistance in complying with and navigating the complexities of AI regulations.

[i] Consolidated version dated 26 January 2024 of the Artificial Intelligence Act

Experts :

Virginie LIEBERMANN

COUNSEL

Avocat à la Cour, Member of the Luxembourg Bar, 2008

Ruben MENDES

SENIOR ASSOCIATE

Avocat à la Cour, Member of the Luxembourg Bar, 2016

Caroline GAL

ASSOCIATE