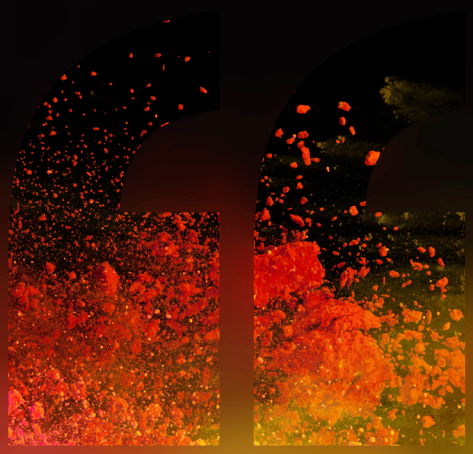
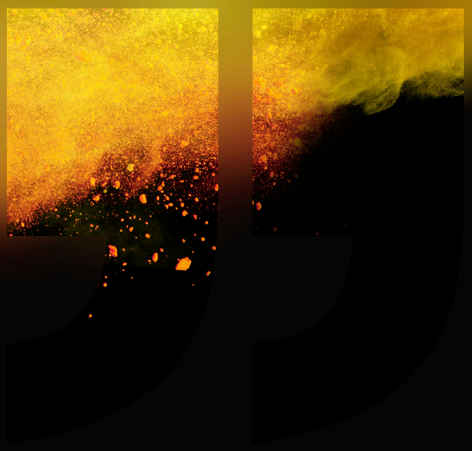
CLIFFORD
CHANCE



THE FUTURE OF AI REGULATION IN EUROPE AND ITS GLOBAL IMPACT



— THOUGHT LEADERSHIP

MAY 2021

THE FUTURE OF AI REGULATION IN EUROPE AND ITS GLOBAL IMPACT

On 21 April 2021, the European Commission finally released the long-awaited proposal for a Regulation on AI (AI Act), a cornerstone of its AI package. With the AI Act, the EU is confirming its role and ambition as a pioneer in the regulation of tech. We consider what this means for businesses, and also offer perspectives from around the world.

The AI Act is the first of its kind, setting out harmonised rules for AI systems in the EU. It attempts to strike a difficult balance between two key objectives: promoting innovation and harnessing the benefits of AI, on the one hand; and addressing key risks and fears AI gives rise to, on the other. In so doing, it seeks to address some of the main concerns levelled at a general, horizontal framework, favouring a risk-based approach and taking account of specific sectoral issues.

At a glance

Key takeaways of the proposed AI Act

- The first-ever harmonised legal framework on AI
- Far-reaching rules with an ambition to set global standards
- A risk-based approach around four risk categories
- A ban on particularly harmful practices creating unacceptable risks
- A set of essential requirements and obligations for high-risk AI, with a special focus on data and data sets
- Specific transparency rules for specific AI systems
- Specific mechanisms to address sectoral concerns
- Fines of up to 6% of total global annual turnover
- A possible entry into force in the second half of 2022, with full application at the earliest in the second half of 2024
- A new public consultation to stay involved
- One key milestone in a wider AI and digital strategy for Europe

Perspectives from around the world

- United Kingdom
- United States
- Asia Pacific

Whilst largely focusing on high-risk AI systems, it also bans some particularly harmful practices, and provides specific requirements for other systems deemed to present more limited risks but nonetheless requiring increased transparency. It also encourages voluntary compliance, beyond high-risk AI.

It provides for strong governance and enforcement mechanisms, including the creation of a European Artificial Intelligence Board and significant sanctions.

At this stage, it is only a proposal and there is a long road ahead. Yet the AI Act represents a revolution in the field of AI, and a landmark in defining a harmonised regulatory framework for the EU with the potential for setting global standards.

The AI Act is a critical part of a wider and very ambitious strategy in Europe on AI, and on tech more generally. Proposals for further legislation are expected in the months to come, and other key texts in the tech space are already being discussed in the Parliament and Council. They include the proposals for a Digital Markets Act and a Digital Services Act as well as for a Data Governance Act. All are game-changers. And when viewed together, this is the biggest shake-up ever of European rules in the tech sector, and the effects will be felt for years to come.

What is AI?

There is no universally accepted definition of AI.

Like the European Commission's White Paper on AI, the AI Act recognises the need for a 'future-proof' definition: one that strikes the right balance between flexibility, to be able to account for the ever-accelerating pace of technological progress, and a definition that is sufficiently precise to provide the necessary legal certainty. Beyond, it aims to keep the definition 'technology neutral', and it focuses not on AI as such, but on AI systems.

The AI Act contains a quite simple – and pretty broad – definition of an AI system (or artificial intelligence system), focusing on software and the approaches and techniques used to develop that software. It also contains a mechanism for the Commission to update the list in light of market and technological developments.

More specifically, an AI system is defined as "software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives,

generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with". The list of techniques and approaches includes machine-learning approaches, logic and knowledge-based approaches as well as statistical approaches.

As those who saw the previous leaked draft of the Regulation may note, the definition has been scaled back. Notably, there is no longer any reference to automation within the definition itself.

GDPR-style extraterritorial scope?

The rules set out in the AI Act are not limited to EU-based operators. Far from it. Purportedly to ensure effective protection of citizens in the EU, the new rules have far-reaching effects, and would basically apply where an AI system is placed on the EU market, or its use affects people located in the EU.

More specifically, the AI Act applies to:

- Providers placing or putting AI systems into service on the EU market, regardless of where they are established;
- Users of AI systems located in the EU; and
- Non-EU providers and users of AI systems, where the output produced by the AI system is used in the EU.

The third limb ensures a very broad scope for the new rules and is likely to be a source of questions.

There would also be the need for providers outside the EU to designate an authorised representative in the EU, when an importer cannot be identified.

The new rules would in principle apply to public authorities, agencies and bodies, including Union institutions, agencies and bodies subject to specific rules, including different fines. However, there is a specific exclusion for public authorities in third countries or international organisations using AI systems in the framework of international agreements for law enforcement and judicial co-operation.

Covering the entire AI value chain

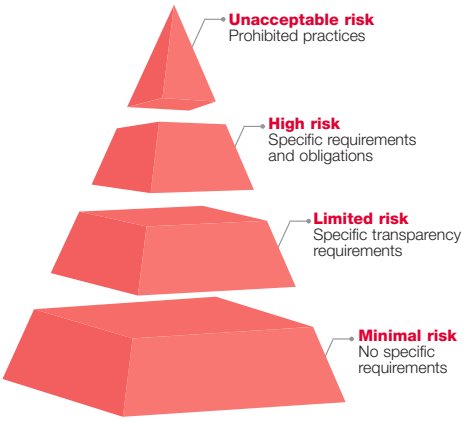
Although the focus is on the provider and the user of the AI system, there are obligations for parties involved across the entire AI value chain, from providers, manufacturers and authorised representatives to importers and distributors through to users – and relevant third parties.

Most are defined. This is the case for the provider – the person that develops or has developed an AI system with a view to placing it on the market or putting it into service under its own name or trademark. It is also the case of the authorised representative, importer, distributor and user. Regarding users, use in the course of a personal non-professional activity is expressly excluded.

On the other hand, the notion of third party does not appear to have been defined, leaving this open to interpretation. Nevertheless, the recitals shed some light on this notion. It would for instance seem aimed at covering third parties involved in the sale and supply of software or pre-trained models and data, and network services providers.

The AI Act includes specific measures, and relaxes certain requirements, for 'small-scale providers' and start-ups.

Categories of AI systems



The European Commission's risk-based approach is structured around four categories of AI systems. Three of the four are regulated under the AI Act.

> **This proposed EU AI regulation is a world first, and is likely to be a game-changer. Global organisations will be concerned about the worldwide reach of these rules.**
>
> —**DESSI SAVOVA**
> **Partner, Commercial & Tech**

The fourth, dubbed 'minimal risk' and which would include such things as AI-enabled video games or spam filters, is apparently not. According to the European Commission, this category would in fact cover the great majority of AI systems.

That said, the AI Act generally also encourages the voluntary application of its rules to AI systems other than high-risk systems.

A ban on unacceptable AI practices?

As part of its risk-based approach, the AI Act prohibits certain practices as a matter of principle, or authorises them subject to specific conditions. These are practices deemed to create unacceptable risks, contravening core Union values. They include:

- **Manipulative AI practices:** AI systems deploying subliminal techniques that are beyond a person's consciousness or exploiting vulnerabilities of a specific group of persons, in each case to materially distort a person's behaviour in a manner likely to cause physical or psychological harm;
- **Social scoring by public authorities** in certain circumstances where it leads to detrimental or unfavourable treatment; or
- **The use of 'real-time' remote biometric identification systems in publicly accessible spaces for law enforcement**, except in circumstances tied to specific use cases (such as the targeted search for potential victims including missing children and the prevention of terrorist attacks) and subject to specific conditions. Notably, each individual use would require a prior authorisation.

There are questions on the effectiveness of these restrictions, given their limited nature and applicable conditions and exceptions.

These provisions also need to be considered in light of other legislation, including the GDPR and its provisions on automated processing / profiling.

The central notion of high-risk AI

The main focus is on this category of AI systems, the second from the top in the risk pyramid. The AI Act expressly identifies the types of AI systems that are considered high-risk.

The first category comprises AI systems to be used as safety components of some (or that themselves are) products covered by Old Approach Sectoral Legislation or NLF Sectoral Legislation (for instance, in the aviation, automotive or healthcare sectors) identified in the AI Act, where such products (or the AI system itself if it is the product) are subject to a third-party conformity assessment under that legislation.

The second category relates to 'stand-alone' AI systems. For example, it includes AI systems intended to be used for:

- 'Real-time' and 'post' remote biometric identification of natural persons (e.g., facial recognition). More generally, and given the risks, remote biometric identification systems are subject to specific and stricter requirements;
- Determining access to education or assessing students in educational and vocational training institutions;
- Recruitment or selection purposes, e.g., for filtering applications or evaluating candidates, or for making decisions in terms of promotion or termination of work relationships. This is a topic that is also relevant for companies that are active in the 'gig' economy. There is an ongoing debate about the role and impact of technology towards employees compared with its effects on self-employed people and people providing services through platforms;
- Evaluating eligibility to, granting, reducing, revoking or reclaiming public assistance benefits and services;
- Evaluating natural persons' creditworthiness or establishing their credit score.

It also includes AI systems intended to be used as safety components for the

management and operation of certain critical infrastructure, i.e. road traffic and the supply of water, gas, heating and electricity.

High-risk AI: Looking to the future

To be able to address future developments, there is a procedure to update the list of high-risk AI systems.

The first key condition to be able to add an AI system to the existing list is that it comes within one of the eight areas that are expressly identified. The second is that it represents a risk of harm to health and safety or adverse impact on fundamental rights that is equivalent to or greater than the risk posed by the systems that are already listed. The text proceeds to identify criteria to be taken into consideration by the European Commission.

Specific rules for high-risk AI

Specific requirements apply to high-risk AI systems:

- **Risk management system:** a risk management system must be established and maintained, and it must consist of a process requiring regular, systematic updating. Key steps would include identification and analysis of risks and adoption of suitable risk management measures. In implementing the risk management system, specific consideration must be given to the potential impact on children.
- **Data and data governance:** these aspects appear key and have received special treatment, being subject to the highest level of fines. Requirements are included on the training of models with data and data sets, including to ensure the quality of data sets and address possible biases. The data sets must be relevant, representative, free of errors and complete. One question here is to what extent it is feasible, in practice, to have fully error-free data sets.

The AI Act allows providers to process 'special categories of data' as referred to in the GDPR and other related EU legislation. This refers to particularly sensitive data such as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and genetic data or data concerning health. And its processing is generally prohibited except in very limited circumstances. Here, the processing is authorised to the extent strictly necessary for bias monitoring, detection and correction, and is subject to appropriate safeguards.

Interestingly, the data and data governance requirements themselves do not appear to include an explicit requirement that the data sets not incorporate biases, or to actually correct biases. The position differs from what was envisaged in the previous (leaked) draft. It notably contained a requirement for high quality data sets to ensure that the AI system "does not incorporate any intentional or unintentional biases, which may become the source of discriminatory impacts prohibited by Union and Member State law once the high-risk AI system is used according to its intended purpose".

- **Documentary requirements and record-keeping**: this notably covers the technical documentation to be established, maintained and updated, logging capabilities and traceability. On logging capabilities, additional requirements are included for systems intended to be used for biometric identification.
- **Transparency and provision of information to users**: high-risk AI systems must be accompanied by instructions for use, containing "concise, complete, correct and clear information that is relevant, accessible and comprehensible". The information must include the capabilities and limitations of performance of the AI system, changes that have been pre-determined, expected lifetime,

For the first time, the proposed EU AI rules explicitly require human oversight for high-risk AI systems. That will require companies working with high-risk AI to implement appropriate measures to ensure that people prevent or minimise potential risks. Organisations will have to provide for a 'kill switch' to instantly interrupt high-risk AI.

—**THOMAS VOLAND**
Partner, Corporate

and necessary maintenance and care measures. The information is all the more important as users have a duty to use the system in accordance with the instructions.

- **Human oversight**: the regulation proposes explicit human oversight. As a starting point, high-risk AI systems must be designed and developed in a manner enabling effective human oversight. Two main types of measures are identified: those 'by design', in that they are built into the systems; and those that are identified by the provider and suitable for implementation by the user. Measures are aimed at enabling the person exercising the oversight to for instance, and as appropriate, monitor the system's operation, interpret its output and intervene or even interrupt its operation. There are specific measures for AI systems to be used for biometric identification.
- **Accuracy, robustness and cyber security**: requirements include resilience to errors, faults or inconsistencies and to attempts by unauthorised third parties to alter use or performance by exploiting system vulnerabilities. Provisions are included to address the specific issues of bias and 'feedback loops', as well as 'data poisoning'.

Specific obligations for operators of high-risk AI and other related parties

The provider

First and foremost, the AI Act sets out obligations for the provider. They include responsibility for ensuring that the high-risk AI system complies with the requirements above and undergoes the relevant conformity assessment procedure, drawing up the EU declaration of conformity and affixing the CE marking. The provider is also responsible for having a post-market monitoring system in place, and for taking necessary corrective actions and informing relevant authorities in the event of non-compliance.

Dedicated guidance to facilitate providers' compliance with the obligations to report serious incidents or malfunctioning is to be issued within 12 months following the entry into force of the AI Act.

Other 'operators'

Specific obligations are set out for other operators and actors, including importers and distributors. For their part, users for instance must use the AI system in accordance with the instructions. In addition, if the user controls the 'input data', it must ensure that data is relevant in view of the intended purpose.

Allocation of roles and responsibilities – flow-down

Beyond defining specific obligations for each category of actor, the AI Act clarifies in what circumstances the manufacturer of the product takes responsibility for compliance of the AI system, when an authorised representative must be appointed by the provider and when other actors of the AI value chain, including third parties, are to be considered as provider. This is the case, for instance, where they put a high-risk AI system on the EU market under their name, or where they modify the intended purpose or make a substantial modification. This means that white-labelling arrangements and any bespoke 'off the shelf' systems will need to be carefully assessed and monitored.

The AI Act also seeks to ensure that actors throughout the chain take responsibility. For instance, the importer is required to ensure the appropriate conformity assessment has been carried out by the provider and the appropriate technical documentation has been drawn up. The distributor must ensure that the provider and the importer have complied with applicable obligations. The importer and the distributor are required to not place a high-risk AI system on the market where they consider that it does not comply with certain requirements. Both must also ensure that while a high-risk AI system is under their responsibility, storage or transport conditions do not

jeopardise its compliance. Users likewise have monitoring obligations and a duty to inform the provider or distributor when they have reasons to consider that use in accordance with the instructions may result in the AI system presenting certain risks or when they identify a serious incident or malfunctioning.

Key questions will also arise regarding the contractual framing of the parties' respective roles and responsibilities, including related warranties, liability and indemnities. The scope and effect of these provisions may also depend on specific rules that may be developed regarding the liability regime for (certain) AI systems.

Conformity assessments for high-risk AI

A key requirement for high-risk AI systems is that they be subject to a conformity assessment prior to placing on the market or putting into service.

As a general rule, and putting aside high-risk AI systems to which the NLF Sectoral Legislation applies or those put on the market or into service by credit institutions and to which specific regulations apply (see below), the AI Act appears to favour conformity assessments carried out by the provider under its own responsibility. A notable exception relates to the conformity assessment of AI systems intended to be used for the remote biometric identification of natural persons, where specific rules apply.

The conformity assessment procedures include specific provisions regarding the need to carry out new assessments each time the high-risk AI system is substantially modified. One specificity, in the context of AI, relates to systems that continue to learn. On this, it seems that changes to the high-risk AI system and its performance that have been pre-determined by the provider at the time of the initial conformity assessment would in principle not be considered as substantial modifications.

There are specific derogations from the conformity assessment procedure. They allow market surveillance authorities to authorise, on a temporary basis and subject to conditions, the placing on the market or putting into service of specific high-risk AI systems "for exceptional reasons of public security or the protection of life and health of persons, environmental protection and the protection of key industrial and infrastructural assets".

The registration of high-risk AI systems

The AI Act provides for the creation of an EU database for 'stand-alone' high-risk AI systems (in principle, not those covered by certain specific sectoral legislation referred to in the AI Act).

Providers of those high-risk AI systems would be required to register them in the database with a pre-defined list of information, e.g.: identification of the provider and of the AI system, description of the intended purpose of the AI system, copy of the certificate issued by the relevant notified body (if applicable), copy of the declaration of conformity and electronic instructions for use. The information in the database would be publicly accessible, and the Commission would be the controller of the database.

Specific transparency for 'limited risk' AI

Certain AI systems are subject to specific transparency obligations.

One key ethical concern often raised in relation to AI is the need to ensure that people are aware when interacting with an AI system. Each of the 2019 Ethics Guidelines for Trustworthy AI, the 2020 Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self-assessment and the European Parliament's 2020 resolution on a framework for ethical aspects of AI touches on this question. The AI Act follows suit. It requires providers to ensure that systems are designed and developed in such a manner that individuals are informed when they are interacting with an AI system (e.g., a chatbot), unless this is obvious.

The AI Act also imposes additional information obligations on users. This is the case in relation to 'deep fake' content, where users must reveal that the content has been artificially generated / manipulated. Likewise, where natural persons are exposed to emotion recognition or biometric categorisation systems, they must be informed of the operation of the system.

There are exceptions however, in particular for certain AI systems authorised by law for the purposes of crime detection, prevention and/or prosecution.

The interplay with other regimes

- **Sectoral issues:** The AI Act seeks to address certain specific sectoral issues and concerns, including in light of existing legislation.
- **Interplay with other laws more generally:** The AI Act needs to be considered in conjunction with other laws. It cannot be perceived in isolation. For example, the AI Act recognises that classifying and regulating an AI system as high-risk does not mean that it is necessarily lawful under other EU law or national law. That means, for instance, that compliance with rules like the GDPR will need to continue and be interpreted alongside these rules.

An excluded, limited or partial application to certain AI systems

No application to military-purpose systems

The AI Act does not apply to AI systems that are developed or used exclusively for military purposes.

A very limited application to certain types of AI systems

Importantly, the AI Act seeks to address the question of the interplay with existing sectoral legislation.

For some AI systems, the AI Act would be of very limited application, at least direct application. This is the case of high-risk AI systems that are safety components of (or that themselves are) products or systems covered by specific listed sectoral legislation in the fields of civil aviation, motor vehicles, two- or three-wheel vehicles and quadricycles, agricultural and forestry vehicles, rail systems and marine equipment (referred to in this note as Old Approach Sectoral Legislation). More specifically, only the provisions of the AI Act related to its evaluation and review process (Article 84) are said to apply. There is uncertainty on what exactly this means.

On the other hand, through other provisions the AI Act expressly amends the Old Approach Sectoral Legislation, to ensure that key requirements for high-risk AI systems set out in the AI Act shall be "taken into account" when adopting relevant delegated or implementing acts (or other relevant measures / documents) under that legislation. Accordingly, whilst the AI Act would be of very limited direct application, it would make its way into the Old Approach Sectoral Legislation.

Avoiding additional burden for other AI systems?

The AI Act addresses questions of interplay with other listed sectoral legislation, i.e. 'Union-harmonised legislation based on the New Legislative Framework' (NLF Sectoral Legislation). This covers, amongst other things, medical devices, toys, lifts and radio equipment, as well as machinery for which a Proposal for a Regulation was also announced on 21 April 2021. For instance, and to avoid duplications and additional burden, the conformity assessment procedure required under that specific sectoral legislation would in principle be followed. The key requirements for high-risk AI under the AI Act would apply and be part of the assessment, and certain other conformity assessment aspects under the AI Act would also apply. Likewise, a single set of technical documentation would be drawn up, containing the information set out in the AI Act and the information required under the specific sectoral legislation.

In addition, there are specificities throughout the AI Act regarding requirements for credit / financial institutions in light of existing legislation, e.g., in relation to conformity assessments, monitoring and the notification of serious incidents. This will not be relevant for all financial institutions, but those that are within scope will begin considering the interplay between their CRD IV governance frameworks and the AI Act, particularly as this is an area that such firms will want to ensure makes its way into the final versions of the Regulation. Whether these proposed limited derogations survive to the final proposal – and the extent of them – remains to be seen. However, this will be an area for relevant firms to monitor and consider how their existing CRD compliance efforts will synchronise with the scope and requirements of the new rules.

Specific time frame for certain large-scale IT systems

There are specific provisions regarding the application of the AI Act to AI systems that are components of certain large-scale IT systems in the area of freedom, security and justice (e.g., Schengen Information System, Visa Information System, Eurodac). In principle, the AI Act would not apply to those systems where placed on the market or put into service before the date that falls 12 months after the date of full application of the AI Act. However, there are exceptions.

Governance – the creation of a European Artificial Intelligence Board

The harmonised implementation of the AI Act would be ensured at the EU level by a newly established European Artificial Intelligence Board. This would be comprised of the national supervisory authorities and the European Data Protection Supervisor, and be chaired by the Commission. It would notably provide advice and assistance to the Commission, including issuing opinions and recommendations on technical specifications and issues of standardisation and the preparation of guidance documents.

The AI Act also details the role and powers of different national authorities, including national competent authorities, notifying authorities, national supervisory authorities and market surveillance authorities.

Sandboxes

Proposed measures in support of innovation include regulatory sandboxes, under the direct supervision of competent authorities, to facilitate the development, testing and validation of AI systems. Modalities and conditions of operation are to be set out in implementing acts. There are specific measures aimed at helping small-scale providers and start-ups, including giving them priority access if they satisfy eligibility conditions.

Also, the AI Act enables the processing, for the purposes of developing and testing AI systems in the sandboxes, of personal data collected for other processes. However, there are conditions attached. Moreover, this is said to be without prejudice to EU or national legislation that excludes processing for purposes other than those explicitly set out in that legislation. It is uncertain, for instance, how exactly the option under the AI Act relates to and interacts with the restrictions in the GDPR on purpose limitation.

Post-market monitoring, sharing of information on incidents and market surveillance

The AI Act contains detailed provisions to address the post-market environment. Providers of high-risk AI systems are, for example, required to have a post-market monitoring system, itself based on a post-market monitoring plan. The Commission is expected to adopt an implementing act to detail what that plan is to look like.

Providers of high-risk AI systems must report serious incidents and malfunctions to competent market surveillance authorities against aggressive timelines – and no more than 15 days from having become aware of them. Here too, additional guidance is to be developed by the Commission, and issued within 12 months of the entry into force of the Regulation.

Provisions on enforcement and market surveillance also include specific procedures where a Member State determines that, although an AI system is compliant with applicable requirements, it poses a risk in terms of health and safety, protection of fundamental rights or other public interest protection.

> **This is not the end game. For anyone wanting to influence Europe's direction of travel on AI, the hard work starts now. The European Parliament and Member States will spend the next 18 months to two years debating the proposal. They could make significant changes before they finally adopt the new Regulation.**
>
> —**GAIL ORTON**
> **Head of EU Public Policy**

Sanctions – GDPR or antitrust-like fines

Very significant fines are contemplated to ensure effective implementation.

For the most serious non-compliances, administrative fines can reach the higher of EUR 30,000,000 and 6% of total global annual turnover. This applies to prohibited AI practices, as well as to any non-compliance with the data and data governance requirements for high-risk AI systems.

For non-compliance of the AI system with any other requirement or obligation, administrative fines of up to the higher of EUR 20,000,000 and 4% of total global annual turnover apply. Specific fines apply to the supply of incorrect, incomplete or misleading information to relevant bodies/ authorities following a request (up to EUR 10,000,000 or 2% of total global annual turnover, whichever is the higher).

Member States are responsible for laying down the rules on penalties, including administrative fines, and for ensuring they are implemented. Penalties must be effective, proportionate and dissuasive. With respect to a Member State's public authorities and bodies, that Member State would determine to what extent administrative fines could apply. Administrative fines would be imposed by national courts or other bodies in the relevant Member State, as applicable, depending on its legal system.

Different fines and different rules apply for Union institutions, agencies and bodies, and the European Data Protection Supervisor is empowered to impose those fines.

The AI Act generally does not, on the other hand, deal with the question of damages and indemnification.

The road ahead – the beginning of the process

It is early days for the AI Act and there is a long road ahead before it becomes EU law. The AI Act will now be passed to the European Parliament and Council of the EU for adoption under the ordinary legislative process (formerly known as 'co-decision'). Both the Parliament and Member States must jointly agree the final wording of the legislation before it can be formally adopted. Interestingly, the European Commission has launched another public consultation, this time on the AI Act. The feedback received will be shared with the European Parliament and Council so that it can be taken into account in the legislative process. The AI Act was opened for feedback for a minimum of eight weeks from 26 April 2021, with the deadline for submissions set at 5 July 2021 (at the date of this note). Dates may further change.

This provides yet another opportunity for interested parties to have their say and contribute to the legislative debate.

The timing of the legislative process is difficult to predict but the earliest we could expect a final text to be agreed and adopted by the Parliament and Council is 18-24 months from now (end of 2022 or first half of 2023), with a further period of 24 months before it would become fully applicable. The decision to propose a Regulation rather than a Directive means the new rules will be directly applicable and avoids the additional time that would have been required for national implementation.

In any event, it would be a while before these new rules kick in.

We should also assume that the proposal will undergo substantial changes as part of the legislative process. The regulation of AI is a controversial and thorny question, with complex issues to be managed and conflicting interests to be balanced. Concerns and criticism are already being voiced, whether as regards

“The proposed AI Act marks a turning-point in the regulation of AI. And it's only the start. It is one crucial part within a wider framework being assessed and designed in Europe for the regulation of AI, and tech more generally.”

—**ALEXANDER KENNEDY**
Counsel, Commercial & Tech

shortfalls and loopholes in terms of addressing risks and protecting fundamental rights, or in terms of the restrictions, burden and cost for businesses.

The Parliament has already undertaken significant work on the issues, having adopted a number of documents on AI including on a framework for ethical aspects, a civil liability regime for AI and intellectual property rights for the development of AI. However, several of those aspects would in principle be addressed through separate legal instruments to come, rather than through the AI Act itself.

A phased application

The new rules would generally apply from 24 months after entry into force of the AI Act.

By exception, some provisions would begin to apply earlier. This is the case of those on notifying authorities and notified bodies, as well as on the European Artificial Intelligence Board and national competent authorities. They would apply from three months following entry into force. The point here is that the infrastructure regarding governance and the conformity assessment system should be operational before the date of full application. The provisions on penalties would start to apply from 12 months following entry into force of the AI Act. The rationale is to enable the Member States to define the applicable rules, notify the Commission and ensure they are properly and effectively implemented by the time the AI Act applies in full.

Also, the AI Act addresses the important question of AI systems put on the market or into service before the AI Act starts applying in full. Putting aside the specific case of large-scale IT systems in the fields of freedom, security and justice mentioned above, the AI Act would apply only in case of significant changes in design or intended purpose from the date of full application of the AI Act.

A wider regulatory framework expected for AI

Any discussion of AI involves key questions around safety and liability, and whether the existing regulatory framework can address the new challenges and risks created by AI. The AI Act has not resolved all of these questions.

The review of the Co-ordinated Plan on AI, the second pillar of the Commission's AI package announced on 21 April 2021, provides very useful insight on what can be expected. In addition to the AI Act, the European Commission will be proposing:

- In 2021 and beyond, necessary revisions of existing sectoral safety legislation. This has already started with the Proposal for a Regulation on machinery products. Other examples include the General Product Safety Directive, with the Commission apparently intending to adopt a proposal for its revision during Q2 2021.
- In 2022, measures to adapt the liability framework to the specific challenges of new technologies and AI (other available information refers to Q4 2021 – Q1 2022). This may include revising the Product Liability Directive, as well as a legislative proposal regarding the liability regime for certain AI systems.

Likewise, the AI Act does not address other key aspects related to AI, for instance specific challenges in terms of intellectual property rights. The need to ensure that the IP framework is fit for the digital age and address any changes deemed necessary to the existing legal framework, is something that is picked up by the IP Action Plan announced by the European Commission at the end of 2020. Naturally, the impact of the use of AI is a key part of that discussion.

The four policy objectives of the Co-ordinated Plan on Artificial Intelligence 2021 Review

- **Enabling the development and uptake of AI in the EU:** includes key initiatives around data sharing and computing infrastructure
- **AI excellence, "from the lab to the market":** includes funding networks of excellence centres, setting up the European Partnership on AI, Data and Robotics, and consolidating the European AI-on-demand platform
- **AI for good: Ensuring that "AI works for people and is a force for good in society":** includes initiatives to foster talent and develop skills, and a policy framework to ensure trust in AI systems. Beyond legislative proposals, action areas include the promotion of the Assessment List for trustworthy AI (ALTAI)
- **Strategic leadership in 'high-impact sectors':** the focus is on seven sectoral action areas, i.e. (i) climate and the environment, (ii) health, (iii) robotics, (iv) the public sector, (v) law enforcement, migration and asylum, (vi) mobility, and (vii) sustainable agriculture.

Implementing AI governance and compliance should be a priority for all Boards. The proposed EU AI Act shows that global corporates need to keep pace with both legislative change and sectoral legislation. The reputational and financial consequences of failing to do so are material.

—**KATE SCOTT**
Partner, Litigation & Dispute Resolution

The US is approaching AI as they have other technology, emphasising transparency and explainability, as well as outputs. We can expect US regulators to continue to bring enforcement actions in this area.

—**MEGAN GORDON**
Partner, Litigation & Dispute Resolution

PERSPECTIVES FROM AROUND THE WORLD

As with other EU initiatives, the proposal may have knock-on effects in other jurisdictions that are considering how to design and implement their own regulatory regimes for AI. In any event, the AI Act will be closely followed by governments, policymakers and regulatory bodies globally. And non-EU companies will also need to consider what authorities in their jurisdictions have to say about AI.

The UK

Although the UK's position on AI matters post-Brexit is still evolving, the UK has clearly indicated that it aims to be a world leader in AI. The UK has retained the GDPR, one of the only regulations around the world that deals directly with automated decision-making, and therefore AI, in domestic law. In May 2020, the UK's data protection regulator, the ICO, released detailed guidance on explaining decisions made with AI. This provides important clarity for businesses on how to meet the requirements set out in the UK GDPR. The UK House of Lords has also warned that a solely self-regulatory approach, based on organisations producing their own ethical AI codes of conduct, risks a lack of uniformity and enforceability. In March 2021, the UK Department for Digital, Culture, Media and Sport announced its Ten Tech Priorities. The priorities include helping to set the rules of engagement for AI use and leading the global debate on AI and governance. They have been released in advance of the UK's National AI Strategy, which will be finalised in 2021 and will bring together the policy and regulatory recommendations made to the UK government on how to ensure safe and resilient development of AI. In the meantime, we expect the UK to continue working closely with competition, privacy, financial services and other sector regulators to produce meaningful guidance for companies working with AI, and to see continued enforcement relying on existing legal requirements and ethical expectations. The UK, EU and other global AI players will also need to align and find areas of harmony in order to further boost innovation.

The US

The Federal Trade Commission (FTC), the general consumer protection regulator in the US, has asserted that it would be closely monitoring companies' use of AI. In particular, the Commission has highlighted concern over AI intended to be used for or that has the effect of discriminating against a protected class, such as by race or gender. To this end, the FTC has set out guidance for businesses to adopt when deploying AI functions, including principles embodied in the AI Act such as transparency and monitoring. US banking regulators are also seeking comment on the use of AI by financial institutions, suggesting further guidance may be forthcoming.

APAC

Generally, and with the exception of the PRC, APAC jurisdictions have explored AI initiatives and provided high-level guidance but there has yet to be an enforcement regime in place or underway.

The PRC

Within APAC, the PRC is leading to look into AI regulations, releasing the long-term action plan 'New Generation Artificial Intelligence Development Plan' in 2017 with specific goals in the regulatory regime of AI up to 2030, alongside the existing legal framework such as the Cybersecurity Law which governs the use and processing of personal information. The AI Act will certainly provide helpful referential value for China to fine-tune its goals and milestones in terms of its AI regulatory regime.

Other key APAC jurisdictions

- **Singapore:** There is no centralised AI regulation (or even one being tabled). Instead, there are several different issued guidelines dealing with AI which, while not meant to be prescriptive, are supposed to assist organisations with implementing AI responsibly – the key guideline being the PDPC's Artificial Intelligence Governance Framework, followed by the MAS's FEAT (which shares broadly the same principles). Naturally, that means that there are no penalties specifically for misuse of AI either – although there can be under other legislation such as the PDPA, provided they apply.
- **Hong Kong:** Similar to Singapore, there are currently no laws/regulations in Hong Kong that are specific to AI (with the exception of measures adopted to ban certain AI products which may affect personal safety such as self-driving AI). Local regulatory bodies have released high-level guidance on AI and AI products, including the Hong Kong Monetary Authority's High-level Principles on AI, and the SFC's Guidelines on Online Distribution and Advisory Platforms. Any regulation of AI is largely dependent on existing regulations for specific institutions such as FI, or existing legislation that may apply to specific aspects of the use of technology/data such as the Personal Data (Privacy) Ordinance.
- **Japan:** There is currently a lack of thematic guidance on specific applications of AI in Japan, although there are high-level considerations relating to AI in its updated AML guidelines (that AI output should be explainable and interpretable). AI regulation is largely undertaken via individual enforcement actions by the FSA (Financial Services Agency) based on the existing regulatory framework against potential misuse (e.g. suspension order against a registered firm lending its name to non-registered firms developing investment programmes).
- **Australia:** The ASIC (Australian Securities and Investments Commission) has rolled out a detailed ASIC Regulatory Guide which provides guidance that aims to assist industry with understanding ASIC's approach to regulating digital advice, requiring regulated entities to put in adequate resources and to have appropriate monitoring and testing.

The proposed AI Act may provide a useful starting point for other jurisdictions in deciding how best to implement AI regulatory regimes of their own. This may be all the more relevant for jurisdictions such as Singapore, where the current governance framework appears based on similar core principles and approach: transparency, accuracy and the necessity for human oversight, along with a risk-sensitive approach.

—**IRIS MOK**
Senior Associate, Litigation & Dispute Resolution

AUTHORS

Dessislava Savova
Partner
Paris
T: +33 1 4405 5483
E: dessislava.savova@cliffordchance.com

Gail Orton
Head of EU Public Policy
Paris/Brussels
T: +33 1 4405 2429
E: gail.orton@cliffordchance.com

Alexander Kennedy
Counsel
Paris
T: +33 1 4405 5184
E: alexander.kennedy@cliffordchance.com

Herbert Swaniker
Lawyer
London
T: +44 207006 6215
E: herbert.swaniker@cliffordchance.com

Thomas Voland
Partner
Dusseldorf
T: +49 211 4355 5642
E: thomas.voland@cliffordchance.com

Sanne Blankestijn
Associate
Amsterdam
T: +31 20 711 9131
E: sanne.blankestijn@cliffordchance.com

CONTACTS

Düsseldorf

Claudia Milbradt
Partner
Düsseldorf
T: +49 211 4355 5962
E: claudia.milbradt@cliffordchance.com

Hong Kong

Brian Harley
Consultant
Hong Kong
T: +852 2826 2412
E: brian.harley@cliffordchance.com

Iris Mok
Senior Associate
Hong Kong
T: +852 2826 3585
E: Iris.Mok@cliffordchance.com

Singapore

Paul Landless
Partner
Singapore
T: +65 6410 2235
E: paul.landless@cliffordchance.com

Xide Low
Senior Associate
Singapore
T: +65 6506 2783
E: xide.low@cliffordchance.com

UK

Monica Freely
Senior Associate
London
T: +44 207006 2322
E: monica.freely@cliffordchance.com

Arnav Joshi
Senior Associate
London
T: +44 207006 1303
E: arnav.joshi@cliffordchance.com

Jonathan Kewley
Partner
London
T: +44 207006 3629
E: jonathan.kewley@cliffordchance.com

Stephen Reese
Partner
London
T: +44 207006 2810
E: stephen.reese@cliffordchance.com

Kate Scott
Partner
London
T: +44 207006 4442
E: kate.scott@cliffordchance.com

Leigh Smith
Senior Associate
London
T: +44 207006 6235
E: leigh.smith@cliffordchance.com

Phillip Souta
Head of UK Public Policy
London
T: +44 207006 1097
E: phillip.souta@cliffordchance.com

US

Megan Gordon
Partner
Washington DC
T: +1 202 912 5021
E: megan.gordon@cliffordchance.com

Daniel Silver
Partner
New York
T: +1 212 878 4919
E: daniel.silver@cliffordchance.com

Alex Sisto
Associate
New York
T: +1 212 878 4990
E: alex.sisto@cliffordchance.com

Brian Yin
Associate
New York
T: +1 212 878 4980
E: brian.yin@cliffordchance.com

Warsaw

Anna Biała
Counsel
Warsaw
T: +48 22429 9692
E: anna.biala@cliffordchance.com

CLIFFORD

CHANCE

www.cliffordchance.com

Clifford Chance, Avenue Louise 65, Box 2, 1050
Brussels, Belgium

2105-000178