SLAUGHTER AND MAY/ CRAVATH

# EU AI ACT TO ENTER INTO FORCE

JULY 2024

## / INTRODUCTION

The EU's AI Act will come into force on 1 August 2024. Cited by the Commission as the 'world's first comprehensive AI law', The Act has caught the attention of organisations across the globe with its focus on responsible innovation, wide extra-territorial reach, high fines and prohibition on certain types of AI which pose an unacceptable risk.

In this briefing we highlight some of the key aspects of the EU AI Act ("the Act"), focussing on ten key questions. We will also look at what practical steps organisations can take now to comply with the Act, and how the Act compares with the approach to AI regulation being taken in other jurisdictions like the UK and US.

**Note:** while the Act is relatively detailed, more information on how it will work in practice will be provided throughout the transition period, through secondary legislation, harmonised standards and guidance.

## / CONTENT

# 1. WHAT IS THE AIM OF THE ACT?

The Act lays down a uniform legal framework for the development, marketing and use of artificial intelligence in line with EU values. It is a Regulation, meaning it will have direct effect in EU Member States.

The Commission states that the Act aims to foster responsible innovation in Europe – "[by] guaranteeing the safety and fundamental rights of people and businesses it will support the development, deployment and take-up of trustworthy AI in Europe."

As well as laying down rules around the development and use of AI, the Act contains provisions designed to promote innovation, including sandboxes and rules to ease the regulatory burden for SMEs.

# 2. WHAT DOES THE ACT COVER?

### I. AI Systems

While EU legislation in the technology space has tended to be technology neutral, the Act is specifically designed to regulate "AI Systems". Defining AI Systems has, however, proved to be challenging, with the original Commission proposal being widely criticised for being too broad. The agreed definition aligns with both the approach proposed by the OECD and the Biden administration's Executive Order on Artificial Intelligence. It defines an AI System as:

*// a machine-based system 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. //*

Examples of AI Systems include: machine learning models such as autonomous driving systems; natural language processing such as chatbots, voice assistants and machine translation; computer vision systems such as facial recognition and medical imaging; and robotic process automation systems such as data entry systems and customer service bots.

There are also specific rules for general-purpose AI ("GPAI") models, which are defined separately from AI Systems as AI models that display significant generality, are capable of competently performing a wide range of distinct tasks and that can be integrated into a variety of downstream systems or applications. For more information on GPAI models, see question 7 below.

### II. Exemptions

While the Act is far reaching, some areas are out of its scope. It does not, for example, apply to areas outside the scope of EU law (e.g. it should not affect Member States' competences in national security) and there are a number of exemptions listed, in areas such as military/defence, R&D and third country public authority use. It does not apply to any research, testing (other than in real world conditions) or development activity which takes place prior to the AI System being placed on the market or put into service, and users are also not caught if they are using AI purely for personal use.

The Act also provides an exemption for AI Systems released under free and open-source licences, unless those AI Systems trigger the criteria for prohibited or high-risk AI, or AI requiring additional transparency obligations.

Finally, the majority of the Act does not apply to operators of high-risk AI Systems (for more information on high-risk AI Systems see question 5 below) that have been put on the market or into service before 2 August 2026 (i.e. two years from the date the Act entered into force – its general date of application) unless significant changes are made to their design (see questions 6 and 10 for more detail).

# 3. WHO IS CAUGHT BY THE ACT'S OBLIGATIONS?

The Act covers a wide range of organisations in the AI supply chain, including:

- **Providers** - organisations that develop and/or supply an AI System or GPAI model, or that have an AI System or GPAI model developed, and place it on the market or put it into service under their own name or trademark (whether for payment or free of charge).
- **Deployers** - organisations that use an AI System, where that use is under the deployer's authority (except if for personal/non-professional use).
- Other members of the supply chain, including **Product Manufacturers** (who incorporate an AI System into their product design and thereby place an AI System on the market or into service with their product, under their own name or trademark), **Importers** and **Distributors**.

Most of the Act's obligations apply to either Providers, who must effectively design and provide safe AI, or Deployers, who must use AI in a responsible and safe way.

# 4. DOES THE ACT HAVE EXTRA-TERRITORIAL REACH?

Yes.

First, the Act covers Providers – wherever based – who place AI Systems or GPAI models on the market in the EU or put them into service in the EU. US or UK organisations would therefore be subject to the Act if (among other things) they sell tools or services using AI in the EU.

Providers of high-risk AI Systems who are subject to the Act but not based in the EU must appoint an Authorised Representative who is located in the EU. The recitals state that this Authorised Representative:

*// plays a pivotal role in ensuring the compliance of the high-risk AI Systems placed on the market or put into service in the Union by those Providers who are not established in the Union and in serving as their contact person established in the Union. //*

Second, the Act covers non-EU Providers and Deployers where the outputs produced by their AI Systems are used in the EU. This may be difficult to determine in practice and organisations will therefore need to consider how they will monitor where the outputs from their systems are being used.

# 5. HOW DOES THE ACT'S RISK-BASED APPROACH WORK?

The Act takes a risk-based approach to regulation. It defines four categories of risk and imposes separate obligations on Providers of GPAI models (as defined in question 2 above; see also question 7 for more information).

The obligations an organisation will face differ depending on both the role that organisation plays in the AI supply chain and the type of AI System involved.

The risk categories are set out below.

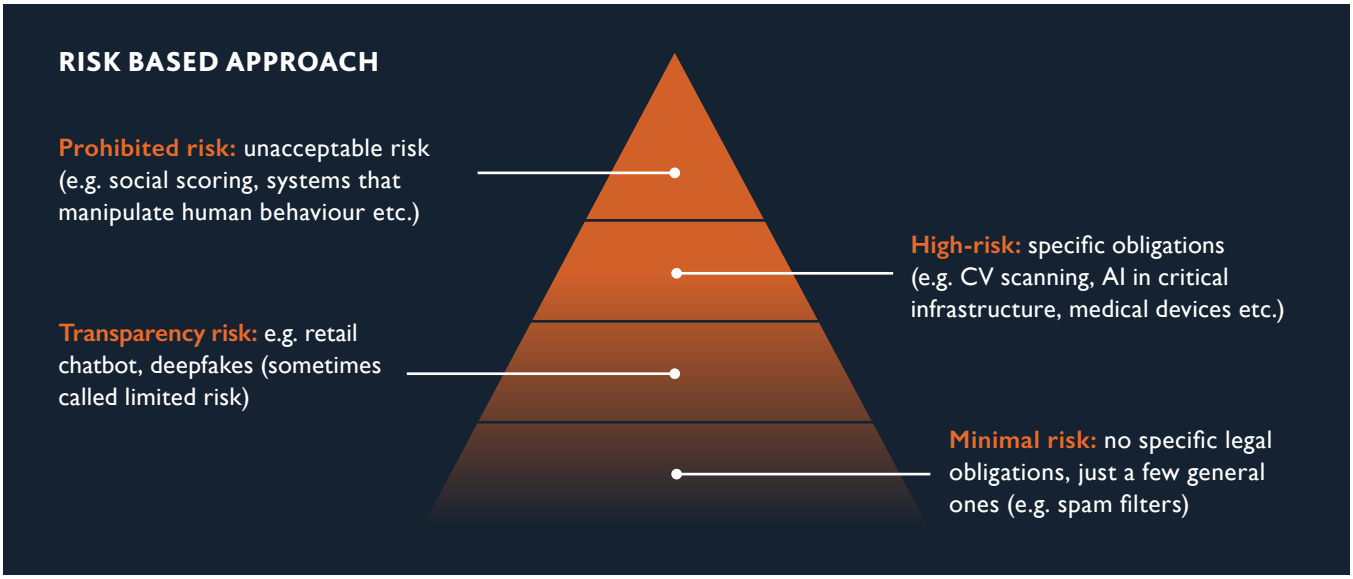
### I. Prohibited AI practices:

These have an unacceptable level of risk and include things like social scoring or an AI System which: deploys subliminal or deceptive techniques to distort behaviour and cause a harmful decision to be made; creates or expands facial recognition databases; or infers emotions in the workplace or in schools/universities. There are also certain uses relating to biometrics that are prohibited, including real-time biometric ID systems in public (although use is allowed in limited circumstances).

### II. High-risk AI:

These AI Systems are highly regulated. They trigger requirements around risk mitigation, documentation, human oversight, fundamental rights impact assessments and conformity testing. Applicable AI Systems include those:

- intended to be used as safety components in products (or which are themselves products) falling under the EU's product safety legislation (listed in Annex I) and which are required to undergo a third-party conformity assessment before being placed on the market (e.g. toys, aviation, cars, medical devices, lifts etc.); or
- which fall within a designated list set out in Annex III of the Act. The list includes: (i) certain (permitted) biometric use; (ii) critical infrastructure; (iii) education and vocational training; (iv) employment (e.g. in recruitment), worker management and access to self-employment; (v) essential private and public services and benefits (e.g. AI Systems used in accessing healthcare, credit scoring and pricing of life and health insurance); (vi) certain law enforcement uses (e.g. to evaluate the reliability of evidence in investigating or prosecuting criminal offences); (vii) migration, asylum and border



control management; and (viii) administration of justice and democratic processes. To trigger the requirements of this category, an AI System must also pose a significant risk of harm to the health, safety or fundamental rights of people. This includes where profiling occurs but does not include systems which carry out narrow procedural tasks, improve the result of a previously completed human activity, detect decision-making patterns or perform certain preparatory tasks.

The Commission will, after consulting with the European AI Board, provide guidance containing examples of use cases which are, and are not, high-risk. It also has the right under the Act to add or modify the use cases listed in Annex III (through delegated acts) and to add to or amend the provisions specifying what does not constitute significant risk of harm. (See question 6 for more information).

As mentioned above, high-risk AI Systems that have been put on the market or into service before 2 August 2026 are exempt from the majority of the Act (including the rules relating to high-risk AI Systems) unless significant changes are made to their design. The exemption does not apply to public sector use cases (although there is a longer transition period in such cases) or where an AI System is used on certain large-scale union IT systems. There is no similar exemption for the rules around prohibited AI, which will still apply.

### III. Transparency Risk AI:

The Act sets out types of AI Systems which, by their nature, present particular transparency risk and therefore require additional transparency and information disclosure obligations (specific to that particular type of AI). These AI Systems are sometimes called "limited risk" AI, although the Act does not use that phrase. Some of the obligations relate to Providers and some relate to Deployers.

The Provider transparency obligations cover:

- **AI Systems intended to interact directly with people (such as chatbots):** Providers must design and develop such systems so that users are informed (unless it is obvious to a reasonably informed person) that they are interacting with an AI System; and
- **AI Systems generating synthetic audio, image, video or text content:** Providers must ensure outputs are watermarked or otherwise marked in a machine-readable format and are detectable as artificially generated/manipulated. Providers must also ensure such technology is robust, interoperable and reliable.

The Deployer transparency obligations cover:

- **Emotion recognition or biometric categorisation AI Systems:** Deployers must inform the people exposed about the operation of the AI System and process any data in line with specified EU Regulations and Directives;
- **Deepfakes:** Deployers must disclose that content has been artificially generated or manipulated; and
- **AI systems generating or manipulating text published to inform the public on matters of public interest:** Deployers must disclose such text as AI generated or manipulated, unless there has been human review or editorial control and a person (natural/legal) holds editorial responsibility.

### IV. Minimal risk AI:

No specific new rules apply if you are using minimal risk AI Systems which perform simple automation tasks without direct interaction with a human (e.g. spam filters). The Commission has stated that "the vast majority" of AI Systems will fall into this category. The Act does, however, impose some general rules which apply to everyone in scope, for example around AI literacy and regulatory co-operation.

## 6. WHAT RULES APPLY TO HIGH-RISK AI?

High-risk AI Systems are subject to a range of detailed compliance requirements which apply depending on what role, or roles, an organisation plays within the AI value chain.

The majority of the obligations fall on Providers and Deployers, with Providers subject to the most far-reaching obligations. Importers and Distributors are subject to specific checks before placing high-risk AI Systems on the EU market.

Transparency obligations and AI literacy requirements (as discussed above) could also apply, depending on the nature of the AI System involved.

Key technical compliance requirements for high-risk AI include:

- a comprehensive risk management system;
- an obligation to ensure data used to train, validate or test the AI System are relevant, representative and to the best extent possible, free of errors and complete;
- maintenance of thorough technical documentation;
- ensuring the AI System is capable of record-keeping and keeping an event log; and
- obligations as to transparency, human oversight and the accuracy, robustness and cybersecurity of the AI System.

Providers must ensure that their high-risk AI Systems comply with these requirements, and Authorised Representatives, Distributors and Importers also have obligations in relation to them (e.g. to maintain compliance).

Further Provider compliance obligations include:

- AI System registration and record keeping requirements;
- completion of conformity assessments;

- implementation of a quality management system;
- establishment of monitoring systems to gather information from Deployers; and
- cooperation with relevant authorities.

Organisations should be aware that Distributors, Importers, Deployers or other third parties will be considered Providers where they: (i) put their name/trademark on the system (parties can still contractually allocate the attendant obligations); (ii) make a substantial modification to a high-risk AI System and it remains high-risk; or (iii) modify the purpose of a non-high-risk system which makes it high-risk.

Product Manufacturers may also be considered Providers if a high-risk AI System is a safety component of a product listed in Section A of Annex I of the Act (including machinery, toys, lifts etc.) and the high-risk system is (i) placed on the market together with the product under the name or trademark of the product manufacturer; or (ii) put into service under the name or trademark of the Product Manufacturer after the product has been placed on the market.

Compliance obligations for Deployers of high-risk AI Systems include:

- implementation of appropriate technical and organisational measures to ensure use is consistent with instructions;
- appointment of suitably competent individuals in human oversight roles;
- verification of input data to ensure relevance to intended purpose;
- carrying out a fundamental rights impact assessment (for certain public bodies and private entities providing public services, e.g. operators of AI Systems which evaluate creditworthiness, or are used in risk assessment for pricing life and health insurance); and
- AI System monitoring, record-keeping and reporting as necessary to Providers, Distributors and authorities.

# 7. WHAT RULES APPLY TO GENERAL PURPOSE AI?

GPAI models are AI models that display significant generality, are capable of competently performing a wide range of distinct tasks and that can be integrated into a variety of downstream systems or applications, as noted in question 2 above. Typically, GPAI models will be trained on large amounts of data using self-supervision at scale. AI models used in R&D and prototyping for pre-market release are excluded. An AI system which is based on a GPAI model and which has the capability to serve a variety of purposes is a GPAI System.

Regulating GPAI models has been one of the most controversial aspects of the Act, with Members States such as Germany and Italy initially opposing stricter regulation and France attempting to block the regulation in its entirety. Agreement was finally reached on rules for both GPAI models generally and GPAI models with systemic risk, both of which will be enforced and monitored by the AI Office at the EU, rather than Member State, level.

Providers of GPAI models must:

- draw up and keep updated technical documentation of the model (including on training and testing process and results of evaluation etc). Annex XI sets out a minimum list of technical information to be maintained and to be provided, upon request, to the AI Office and national competent authorities;
- draw up, keep updated and make available information and documentation to Providers of AI Systems that will integrate the GPAI model into their model, enabling such Providers to understand its capabilities and limitations and to comply with their obligations. Annex XII contains a minimum list of such information;
- put a policy in place to comply with EU copyright (and related rights) law, particularly the Directive on Copyright in the Digital Single Market;
- make a summary of the content used for training the GPAI model publicly available (following the AI Office template); and
- cooperate with the Commission and national competent authorities.

There are additional rules for Providers of GPAI models with systemic risk. These include GPAI models that:

- have high impact capabilities (i.e. where cumulative computing power used for training is greater than the agreed threshold – currently FLOPs greater than 10^25); or
- the Commission, or a scientific panel, has decided have equivalent high impact capabilities.

Providers of GPAI models that meet the systemic risk criteria should notify the Commission without delay, and within two weeks of the criteria being met.

Providers may object to their GPAI model being classified as having systemic risk. During the notification process, Providers may present the Commission with arguments to demonstrate that the at-issue GPAI model does not present risk due to its specific characteristics. The Commission will assess and ultimately publish a list of all GPAI models it deems to have systemic risk (without prejudice to the need to respect IP or confidential business information). At this stage, Providers may object, and the Commission may decide to reassess.

For GPAI models that meet the systemic risk threshold, Providers must carry out additional actions to:

- perform model evaluation in line with standardised protocols, including conducting adversarial testing to identify and mitigate risks;

- assess and mitigate possible systemic risks;
- track, document and report (to the AI Office and national competent authorities where relevant) serious incidents and possible corrective measures to address them; and
- ensure adequate levels of cybersecurity (including for the model's physical infrastructure).

## 8. WHAT ARE THE ACT'S OTHER MEASURES?

Central to the Commission's aim of fostering innovation, the Act proposes that Member States and the European Data Protection Supervisor (on behalf of Union institutions) set up coordinated AI regulatory sandboxes across the EU. These sandboxes promote innovation by providing a controlled environment where Providers can develop, train, test and validate AI Systems for a period before being placed on the market. National competent authorities will be obliged to submit annual reports to the AI Office providing information on the sandbox progress and results which will be available to the public.

The Act also acknowledges the challenges that Small and Medium-sized Enterprises ("SMEs") might face in complying with the new regulations. Some key considerations made for SMEs under the Act include Member States offering initiatives such as: priority access to sandboxes, training on how to apply the Act to SMEs, communication channels for advice and responses to queries about implementation and proportional reductions in fees for Conformity Assessments for certain high-risk AI Systems.

## 9. ENFORCEMENT AND FINES: WHAT HAPPENS IF YOU DON'T COMPLY?

The scale of the Act's fines have caught the headlines. In-scope organisations face fines of (the higher of) €35 million or 7% of global annual turnover in the previous financial year for violations of the prohibited AI practice rules, €15 million or 3% for violations of the Act's obligations (including high-risk compliance obligations, fundamental rights impact assessment and transparency obligations) and €7.5 million or 1.5% for the supply of incorrect information.

Fines for SMEs and start-ups are capped at the lower of the percentages or amounts applicable to each category of violation.

Enforcement of the Act is carried out through a two-layer governance framework at both European Commission level (through the AI Office – supported by a scientific panel of experts - and the AI Board) and at national (Member State) level.

With the exception of rules for GPAI, which (as mentioned above) are enforced by the AI Office at the EU, the majority of enforcement will be carried out at the national level. Each Member State will appoint one notifying authority and at least one market surveillance authority. National market surveillance authorities will undertake most compliance investigations and enforcement actions. This approach aims to ensure harmonised implementation while allowing Member States flexibility to designate competent bodies to carry out effective implementation.

## 10. TIMINGS: WHEN WILL THE ACT APPLY?

Political agreement was reached in December 2023, although more work was needed to finalise the details, and final votes were required by the European institutions. The final votes took place in March (for the European Parliament) and May (for the Council).

The Act then comes into force on 1 August 2024, 20 days after being published in the Official Journal of the EU. It will generally apply on 2 August 2026, after a 2-year transition period (subject to certain exceptions).

Important transition period deadlines include:

- **2 February 2025** (six months after entry into force): prohibited AI practices will be banned and general provisions (e.g. regarding AI literacy) apply;
- **2 May 2025** (nine months after entry into force): codes of practice developed by industry in participation with Member States (through the AI Board) and AI Office to be completed;
- **2 August 2025** (one year after entry into force): rules on GPAI and penalties take effect, and Member States must have appointed their notifying authorities and bodies;
- **2 August 2026** (two years after entry into force): the Act becomes applicable across the EU;
- **2 August 2027** (three years after entry into force): the Annex I high-risk AI System rules apply, and the GPAI rules take effect for GPAI placed on the market prior to the end of the first year of the Act;
- **2 August 2030** (six years after entry into force): the high-risk AI System rules apply to high-risk AI Systems in use by public authorities, where such high-risk AI systems were put on the market before 2 August 2026; and
- **31 December 2030:** the Act applies to AI Systems which are components of the large-scale IT systems established by the legal acts set out in Annex X (which includes a list of EU acts in the areas of freedom, security and justice such as the Schengen Information System).

Please see below our AI Act Timeline.

# PRACTICAL STEPS FOR ORGANISATIONS

Organisations should take steps now to comply with the Act. Some rules will come into force in early 2025 and products and services which will be put onto the market when the Act is in full force are being designed and developed now. Organisations will want to devise such products and services with compliance in mind.

Organisations should ask themselves:

## Do I know what AI I am using?

The first step is to understand what AI you are using in your organisation and whether it falls within the definition of an AI System or GPAI model under the Act.

## Am I in scope of the AI Act?

For each AI System, determine:

- Does an exemption apply?
- Are you within the Act's territorial reach?

If you are a UK or US based organisation, you may still be in scope if you sell into the EU, or the output of your AI System is used in the EU.

## If I am in scope, what role do I play?

For each AI System, determine:

- Are you a Provider, Deployer, Distributor, Importer, Product Manufacturer or Authorised Representative?

## Which risk category does my AI fall into?

The Act takes a risk-based approach and obligations differ depending on the type of AI you use (e.g. is it prohibited, high, limited or minimal risk or is it a GPAI model?) as well as the role you play (e.g. Provider transparency obligations are different from Deployer transparency obligations).

## Am I making changes to an existing AI System?

Modifying an AI System that is already on the market could have substantial consequences under the Act.

For example, in relation to high-risk AI Systems:

- There are certain exemptions which apply for high-risk AI Systems that have been placed on the market before 2 August 2026 (i.e. the general date of application of the Act), but these exemptions fall away where there are significant changes to a high-risk AI System's design.
- If a Distributor, Importer, Deployer or other third party makes a substantial modification to an existing high-risk AI System they may then be treated as a Provider of that system, and subject to the obligations of a Provider under the Act. This will also be the case if they brand the AI System as their own (i.e. put their name or trademark on it).

Changes in use could also bring an AI System into the high risk or prohibited categories, so such use changes should be monitored.

## Am I monitoring developments in this space and using the resources available?

There will be a whole host of AI guidance, standards and codes of conduct to aid compliance which we will be monitoring. In addition, the EU Commission has proposed an AI Pact aimed at assisting EU and non-EU organisations in planning ahead for compliance and encouraging early adoption of the Act's measures. The AI Office will play a facilitator role organising workshops and gathering insights into best practices and challenges faced. The AI Office will also report and publish participants' "declarations of engagement" showing concrete actions (planned or underway) that organisations are taking to meet the Act's requirements. Technology is also rapidly evolving in this area, such that organisations will need to monitor advancements as the Act's requirements enter into force to ensure implementation of best practices. Today's best practices might be outdated and insufficient in two years.

## Do I need to include AI-specific provisions in my contracts?

While general contractual provisions around compliance with law, performance, liability, IP etc. may provide some protections against AI risk, now is the time to consider whether you need to include any AI-specific protections in new contractual arrangements, and whether you need to review and amend any existing contracts. For non-EU organisations, protections may include geographic limitations on usage and outputs, among other items.

## Is my AI Governance ready?

More generally, now is also the time to ensure that you have appropriate AI governance in place. While AI Act compliance is important – something underpinned by the large, GDPR busting fines provided for under the Act , there are a whole range of AI related risks that are not covered by the Act. A good governance process which helps you set your risk appetite, keep track of your AI use and bring together all relevant stakeholders to identify, manage and monitor the associated risks, can help ensure that AI is developed and/or deployed in your organisation in a responsible way.

# THE US AND UK APPROACHES TO AI REGULATION

Governments around the world are considering how to regulate AI. While others are not currently taking the EU's approach of introducing a comprehensive, cross-cutting, technology specific AI law, many legislators and regulators are introducing new rules and guidance in this space. Here we review the approaches being taken in the UK and US.

## US APPROACH TO AI

### OVERVIEW

On October 30, 2023, President Biden signed an Executive Order aimed at promoting the responsible development and deployment of AI. The Executive Order broadly directs over 20 federal agencies to take action to regulate AI and establishes an interagency AI council. While this briefing focuses on federal law and the Executive Order, states have also passed laws (e.g. Colorado), or are looking to pass laws (e.g. California), to regulate AI.

### REGULATORY APPROACH

The Executive Order tasks over 20 federal agencies with regulating various aspects of AI. Among other requirements:

- **National Institute of Standards and Technology:** Establish guidelines relating to AI, including for risk management and secure development practices.
- **Department of Commerce:** Establish guidelines for developing trustworthy AI systems, and require companies that develop or intend to develop dual-use AI foundation models (one type of GPAI model) as well as Infrastructure as a Service providers to report on certain information and activities to the Federal Government.
- **Department of the Treasury:** Publish a public report on best practices for financial institutions to manage AI specific cybersecurity risks.
- **Federal Trade Commission:** Consider enforcement with respect to AI and consumer protection.
- **Department of Labor:** Provide guidance relating to non discrimination in hiring involving AI.
- **U.S. Patent and Trademark Office:** Provide guidance surrounding intellectual property issues raised by AI.

### WHITE HOUSE AI COUNCIL

An interagency council of major federal agencies has been established to oversee implementation of AI related policies and to encourage effective implementation of the Executive Order.

### TIMING

The Executive Order's implementation deadlines range from 30 to 540 days. More obligations applicable to private entities are likely to be developed as federal agencies implement the Executive Order's directives.

## UK APPROACH TO AI

### OVERVIEW

On March 29, 2023 the UK Government published its "Pro-Innovation approach to AI regulation" White Paper. It set out a sector-specific approach to AI regulation, underpinned by five cross-sectoral principles and a set of centralised functions such as a sandbox and centralised risk function. On February 6, 2024, the (now previous) Government published its response to the consultation it launched alongside the White Paper. This confirmed that the UK is moving forward with this proposed AI Framework, although new binding rules may also now be on the horizon for the most advanced general purpose AI systems. The King's Speech on 17 July confirmed that the new Labour Government is looking to introduce these GPAI rules, although no commitment was made on when a bill would be introduced (see blog for more information).

### AI PRINCIPLES

All UK regulators must have regard to five cross-sectoral AI principles, although the principles are not currently on a statutory footing. They are: (i) safety, security and robustness; (ii) appropriate transparency and explainability; (iii) fairness; (iv) accountability and governance; and (v) contestability and redress.

### REGULATORY APPROACH

The AI Framework considers that context is key and that sector regulators are best placed to understand, and proportionally regulate, AI in their sectors. Some regulators are also already very active in this space. For example, the Information Commissioner's Office (the UK's data regulator) has published AI specific guidance for over ten years and has already issued AI related enforcement actions. In addition:

- key UK regulators have published how they are responding to AI risks and opportunities (following a request to do so by the UK Government); and
- the Digital Regulation Cooperation Forum, made up of the data, financial, competition and communications regulators, is taking a role in helping to co-ordinate the regulatory approach to AI.

### DSIT

Within UK Government, the Department of Science, Innovation and Technology (DSIT) is taking the lead on AI regulation, and centralised functions (such as a centralised risk function and the AI Safety Institute) sit within DSIT. It is also considering IP issues, alongside other government agencies.

# AI ACT TIMELINE

**1 AUGUST 2024**

Act enters into force

**2 FEBRUARY 2025**

+ six months

Prohibited AI provisions apply

**2 MAY 2025**

+ nine months

Guidance published

**2 AUGUST 2025**

+ one year

GPAI and penalties rules apply, MS must appoint competent authorities

**2 AUGUST 2026**

+ two years

Act applies generally

**2 AUGUST 2027**

+ three years

Annex I high-risk provisions apply, existing GPAI models must comply

**2 AUGUST 2030**

+ six years

Certain high-risk AI Systems used by public authorities must comply

# YOUR AI ADVISORS

Our firms share an international strategy that promotes collaboration, with leading legal experts in jurisdictions our clients are operating in, over the opening of satellite offices in multiple countries. Through this type of collaboration, our AI and Digital legal specialists at Slaughter and May and Cravath are working jointly to support our respective clients with AI compliance, AI governance and AI transactions in the US, EU, UK and beyond.

## SLAUGHTER AND MAY

Slaughter and May is a leading international law firm, recognised throughout the business community for our exceptional legal service, commercial awareness, and commitment to clients. We are known for our ability to find innovative solutions to the most complex of legal problems on an international scale.

**ROB SUMROY**
Partner
+44 (0)20 7090 4032
rob.sumroy@slaughterandmay.com

**LAURA HOUSTON**
Partner
+44 (0)20 7090 4230
laura.houston@slaughterandmay.com

**NATALIE DONOVAN**
PSL Counsel
+44 (0)20 7090 4058
natalie.donovan@slaughterandmay.com

*With thanks to associate Kathryn Martin Cussons.*

## CRAVATH

Cravath, Swaine & Moore LLP has been known as one of the premier U.S. law firms for over two centuries. Each of the Firm's practices is highly regarded, and Cravath lawyers are recognized for their commitment to the representation of their clients' interests in the US and throughout the world.

**DAVID J. KAPPOS**
Partner
+1-212-474-1168
dkappos@cravath.com

**SASHA ROSENTHAL-LARREA**
Partner
+1-212-474-1967
srosenthal-larrea@cravath.com

**EVAN NORRIS**
Partner
+1-212-474-1524
enorris@cravath.com

*With thanks to associates Dean M. Nickles and Carys J. Webb.*