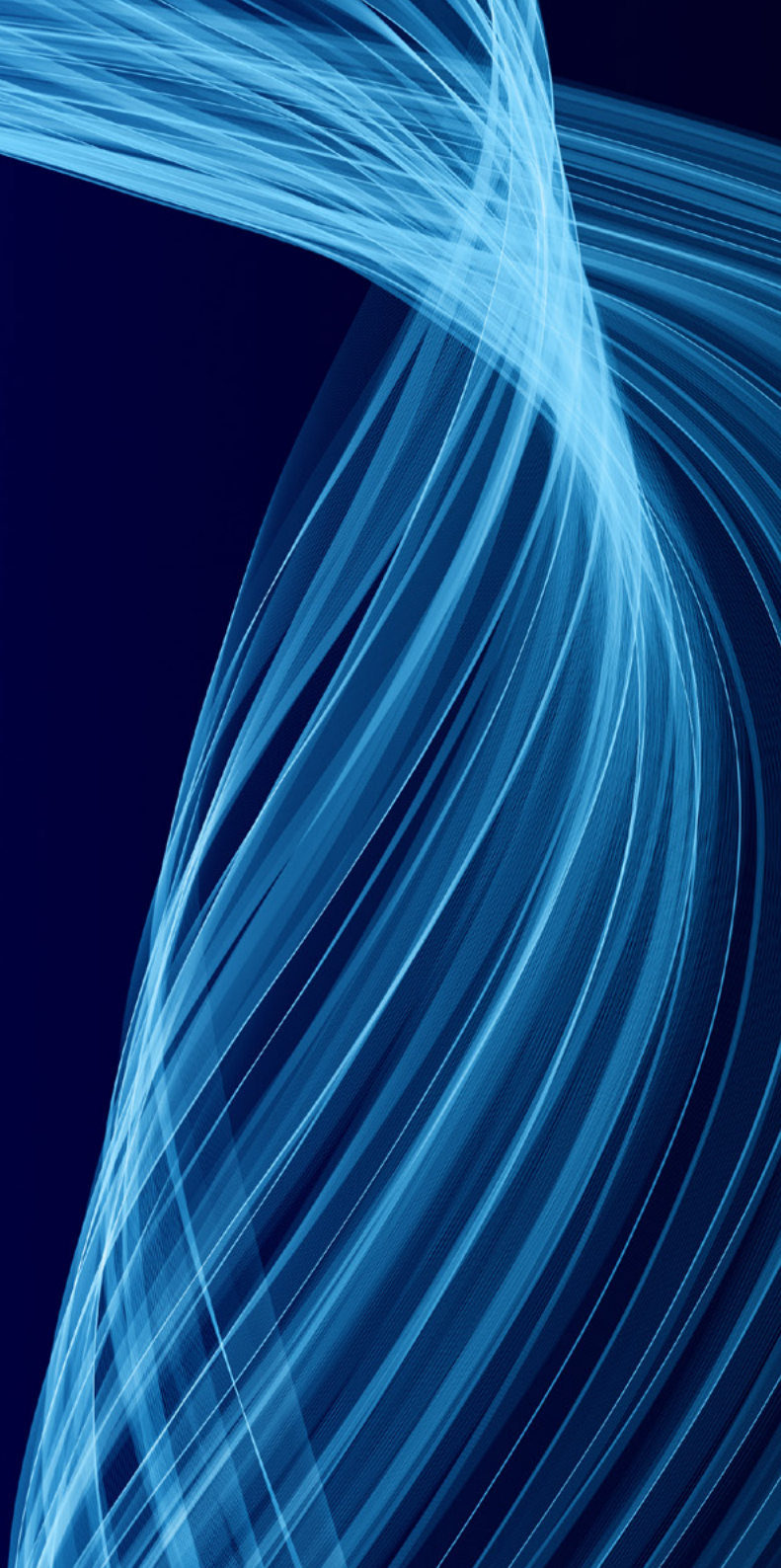
Deciphering the EU AI Act

Practical steps for navigating the landmark AI legal framework shaping Europe's digital future



LathamTECH

LATHAM&WATKINS

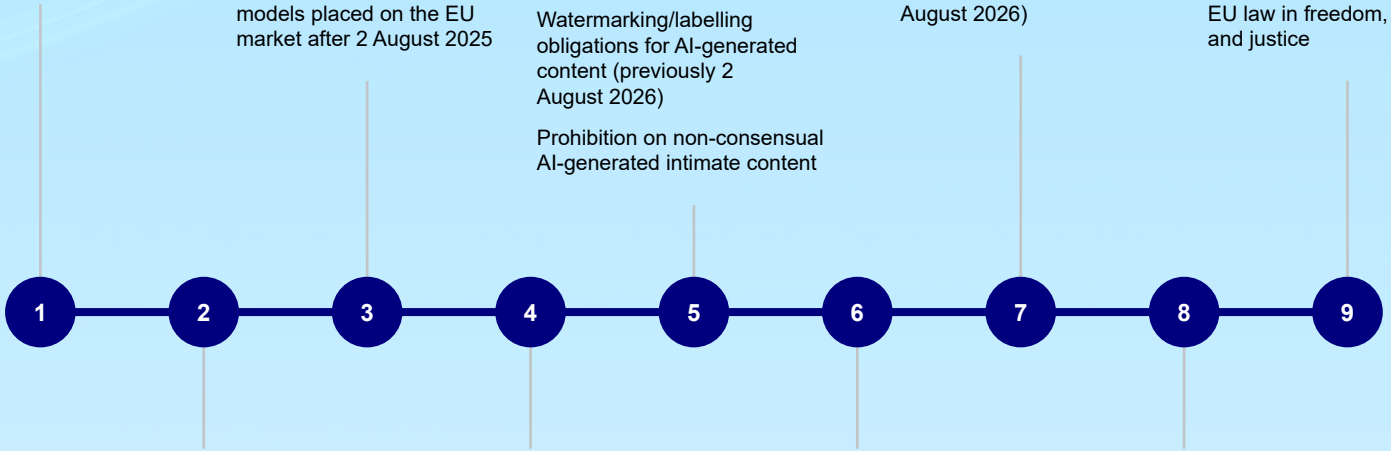
The EU AI Act (the Act) comprehensively regulates the development and deployment of AI along the AI value chain. The Act forms part of a wider landscape of EU technology and data regulation — including the GDPR, Revised Product Liability Directive, Digital Services Act, Data Act — which presents both significant opportunities and complex compliance challenges.

The scope of the Act is broad and extends beyond the borders of the EU. The Act applies to companies providing or using AI in the EU, regardless of where the company is established. The Act establishes a risk-based framework of requirements for AI systems, including a ban on certain AI practices considered the most harmful to individuals, extensive requirements for AI systems categorised as high-risk, and transparency obligations for providers and deployers of certain AI systems that generate or modify media content. A specific regime applies to general-purpose AI (GPAI) models, with additional obligations imposed on providers of GPAI models with systemic risk. Whilst the Act sets out a complex and detailed regime, there are core requirements including robust protection of individual rights, actively managed risk assessments, effective transparency, and adaptable governance.

The Act becomes applicable in a phased implementation, including transition periods for GPAI models and high-risk AI in regulated products. The AI Act Omnibus extends compliance deadlines for high-risk AI systems and introduces new rules on AI-generated intimate content.

This report leverages Latham's experience advising on the AI ecosystem to help companies navigate different aspects of the Act, equipping them with key takeaways and practical steps to stay ahead of an ever-evolving AI regulatory landscape.

AI Act: Timeline for Implementation



Entry Into Force
1 August 2024

The Act entered into force

Prohibited AI
2 February 2025

Prohibition on unacceptable risk AI systems

AI literacy obligations

GPAI
2 August 2025

Obligations on providers of general-purpose AI (GPAI) models placed on the EU market after 2 August 2025

General Transparency
2 August 2026

Transparency obligations for certain AI systems

Watermarking/labelling and Prohibition on AI-Generated Intimate Content
2 December 2026

Watermarking/labelling obligations for AI-generated content (previously 2 August 2026)

Prohibition on non-consensual AI-generated intimate content

Existing GPAI
2 August 2027

Obligations on providers of GPAI models already on the EU market before 2 August 2025

High-Risk AI
2 December 2027

Obligations on high-risk AI systems (previously 2 August 2026)

AI in Regulated Products
2 August 2028

Obligations on high-risk AI systems in regulated products (previously 2 August 2027)

Larger IT Systems
31 December 2030

Compliance for AI systems in large-scale IT systems under EU law in freedom, security, and justice

AI Act Scope

KEY POINTS

ARTICLES 2, 3, 25, 113

In force from:
2 February 2025

Applicable to:
Providers and deployers of AI systems; importers and distributors of AI systems; providers of GPAI models

Guidance:
Commission Guidelines on the Definition of AI System (AI System Definition Guidelines)

AI Systems

The definition of an AI system under the Act is broad and includes six main elements:

- a machine-based system designed to operate with varying levels of autonomy — the AI System Definition Guidelines state this element requires an AI system to operate with some degree of independence from human involvement or intervention;
- that may exhibit adaptiveness after deployment;
- and that, for explicit or implicit objectives;
- infers, from the input it receives, how to generate outputs — the AI System Definition Guidelines seek to address the fact that systems may have capacity to make inferences but not otherwise meet the threshold for an AI system regulated by the Act (e.g., linear or logistic regression methods that solely improve or accelerate computational performance or mathematical optimisation, and simple predictions systems that do not go beyond basic data processing or demonstrate autonomy or adaptiveness);
- such as predictions, content, recommendations, or decisions;
- that can influence physical or virtual environments.

AI Act Scope

The Act provides for several exclusions, including: AI systems used solely for scientific research; testing and development of AI systems before being placed on the market; and certain open-source AI systems (though open-source AI systems constituting a prohibited AI practice, high-risk AI system, or an AI system under Article 50 — chatbots, generative AI systems, deepfake tools (See Transparency) — are not excluded from the scope of the Act).

GPAI Models

(See GPAI Models)

Providers, Deployers, Importers, Distributors

The Act applies to participants along the AI value chain, including those established or located outside the EU in certain circumstances:

- Provider (EU or non-EU): Develops and supplies an AI system on the EU market or the output of the AI system is used in the EU
- Deployer (EU): Uses AI in the context of its business
- Deployer (non-EU): The output of the AI system is used in the EU in the context of its business
- Importer (EU): Supplies an AI system of a non-EU provider on the EU market
- Distributor (EU): Supplies an AI system on the EU market without being a provider or importer
- Provider of a GPAI model (EU or non-EU): Supplies a GPAI model on the EU market

Non-EU established providers of high-risk AI systems and non-EU established providers of GPAI models are required to appoint an EU representative.

A deployer, importer, or distributor of a high-risk AI system will be treated as the provider of the AI system (and required to comply with the provider's obligations) if that deployer, importer, or distributor substantially modifies, or modifies the intended purpose of, the AI system (such that it remains or becomes a high-risk AI system) or applies its own branding to the AI system (see High-Risk AI Systems).

AI Act Scope

PRACTICAL STEPS

- Map AI systems and use cases, and assess whether each system falls within the scope of the Act and, if so, what risk category it falls into. This is a potentially complex exercise in practice, in light of the broad concept of AI system adopted by the Act and the equally broadly defined risk categories featuring various exclusions (see Prohibited AI Practices; High-Risk AI Systems; and Transparency).
- Determine your organisation's role in relation to each AI system (e.g., provider, deployer, etc.) in the context of the wider AI value chain.
- Regularly review and document all mapping and assessments, as part of wider AI governance processes.

AI Literacy

KEY POINTS

ARTICLE 4

In force from:
2 February 2025

Applicable to:
Providers and deployers of AI systems

Penalties:
No direct penalties; potential for civil liability (e.g., if use of AI systems by personnel who have not been adequately trained causes harm to consumers, business partners, or other third parties)

Guidance
Commission AI Literacy - Questions & Answers; Commission Living Repository of AI Literacy

Providers and deployers must ensure that personnel working with AI have a sufficient understanding of AI, taking into account technical experience and the context in which AI will be used.

PRACTICAL STEPS

- Design and implement AI literacy resources adapted to the internal audience. Non-technical personnel working extensively with AI in higher risk uses (e.g., impactful decision-making about individuals, health and safety, etc.) are likely to require more extensive training than IT teams using AI-powered project management tools for internal workflows. The Act is not prescriptive, and AI literacy can be achieved in a number of ways (through live training, on-demand online training, and layered resources).
- Regularly review and document AI literacy programmes and resources in a regulator-ready format.

Related Insights: Upcoming EU AI Act Obligations: Mandatory Training and Prohibited Practices

Prohibited AI Practices

KEY POINTS

ARTICLE 5

In force from:
2 February 2025; prohibition on non-consensual AI-generated intimate content in force from 2 December 2026

Applicable to:
Providers, deployers, importers, and distributors of AI systems

Guidance:
Commission Guidelines on prohibited artificial intelligence practices (Prohibited AI Guidelines)

Penalties:
Fines of up to the greater of €35 million or 7% of total worldwide annual turnover per violation, and potentially other penalties under national frameworks (see Supervision and Enforcement). National market surveillance authorities enforce the penalties regime, which came into effect on 2 August 2025.

The Act sets out an exhaustive list of prohibited AI practices. This list is not static; the Commission will review the prohibited practices annually and can propose amendments. Under the Act, providing or deploying an AI system for any of the following purposes or uses is prohibited:

- Emotion inference in the workplace or educational institutions (other than for medical or safety reasons)
  - The Prohibited AI Guidelines explain that this prohibition applies to AI systems that identify emotion as well as those that infer emotion. The Prohibited AI Guidelines also narrow the scope of this prohibition in practice by clarifying that the ban is limited to inferences based on biometric data (rather than, for example, sentiment analysis based on keywords or tone in text). The Prohibited AI Guidelines confirm that "emotion recognition systems"[1] falling outside this prohibition could still qualify as high-risk AI systems (see High-Risk AI Systems).

1 Defined in the Act as AI systems for the purpose of identifying and inferring emotions or intentions of natural persons on the basis of their biometric data.

Prohibited AI Practices

- Using subliminal, manipulative, or deceptive techniques to manipulate human behaviour and circumvent their free will in a manner likely to cause significant harm
  - The Prohibited AI Guidelines suggest that this prohibition applies to learned manipulative behaviours, regardless of the intention behind the development and deployment of the AI system.
- Exploiting individual vulnerabilities due to age, disability, or social or economic situation, in order to manipulate individuals in a manner likely to cause significant harm
- Biometric categorisation of individuals to deduce or infer their race, political views, religious or philosophical beliefs, sex life or sexual orientation, or trade union membership
- Untargeted or bulk scraping of facial images from the internet or CCTV footage to create facial recognition databases
- Social scoring based on social behaviour or personal characteristics resulting in detrimental treatment of individuals.
- Real-time biometric identification in public spaces for law enforcement purposes, subject to certain exemptions
- Profiling for the purposes of predictive policing
- Generating or manipulating sexually explicit or intimate images, video, or audio without explicit consent, or generating child sexual abuse material. This prohibition is introduced by the AI Act Omnibus, applicable from 2 December 2026.

PRACTICAL STEPS

- Map AI systems and use cases, and identify uses that could potentially fall within the prohibited categories (as part of a wider AI system mapping and risk categorisation process, as relevant). The prohibited AI use cases are relatively narrow but not precisely defined in the Act and may therefore require a nuanced analysis to determine their application in practice. The Prohibited AI Guidelines provide a degree of clarification on the scope of each prohibited AI practice, though context-specific analysis would still be required.
- Regularly review AI system categorisations to capture any AI practices that may have evolved into a prohibited practice (e.g., learned manipulative behaviours) and additions by the Commission to the prohibited practices list; document all mapping and assessments.

Related Insights: Upcoming EU AI Act Obligations: Mandatory Training and Prohibited Practices
AI Act Update: EU Resolves to Change Rules and Extend Deadlines

High-Risk AI Systems

KEY POINTS

ARTICLES 6-49 AND 71-73; ANNEXES I, III-IX

In force from:

2 December 2027. The high-risk AI system requirements apply from 2 December 2027 for AI systems categorised as high-risk use cases under Annex III of the Act; providers of AI systems in regulated products categorised as high-risk under Annex I of the Act have until 2 August 2028 to bring AI systems into compliance. These compliance deadlines were extended by the AI Act Omnibus from 2 August 2026 (high-risk use cases under Annex III) and 2 August 2027 (AI systems in regulated products under Annex I) respectively.

Applicable to:

Providers, deployers, importers, and distributors of high-risk AI systems

Penalties:

Fines of up to the greater of €15million or 3% of total worldwide annual turnover per violation, and potentially other penalties under national frameworks (see Supervision and Enforcement). National market surveillance authorities enforce the penalties regime, which came into effect on 2 August 2025.

Guidance:

Commission consultation on guidelines on high-risk AI systems

Commission draft guidance and template for incident reporting

Classification as a High-Risk AI System

The Act establishes two categories of high-risk AI system.

1. Product safety: AI systems that are products, or safety components of products, regulated by certain EU product safety laws (as listed in Annex I, and including vehicle, machinery, and toy safety rules) and required to undergo third-party conformance assessments.
2. High-risk use cases: AI systems that are used for certain applications as listed in Annex III of the Act (which may be amended by the Commission to reflect advances in AI technology and deployment), unless exempt (see below):
   - Certain employment and workers management uses including recruitment, employment termination, and performance evaluation

High-Risk AI Systems

High-risk use cases continued

- Emotion recognition
- Remote biometric identification and biometric categorisation
- Access to essential private and public services, including evaluating eligibility for public assistance, evaluating creditworthiness and credit scoring, and health insurance pricing
- Safety components in the management and operation of critical infrastructures
- Certain educational or vocational training uses, including determining access, evaluating outcomes, and monitoring behaviour during exams
- Various public authority use cases related to: law enforcement; migration, asylum and border control; the justice system; and democratic processes

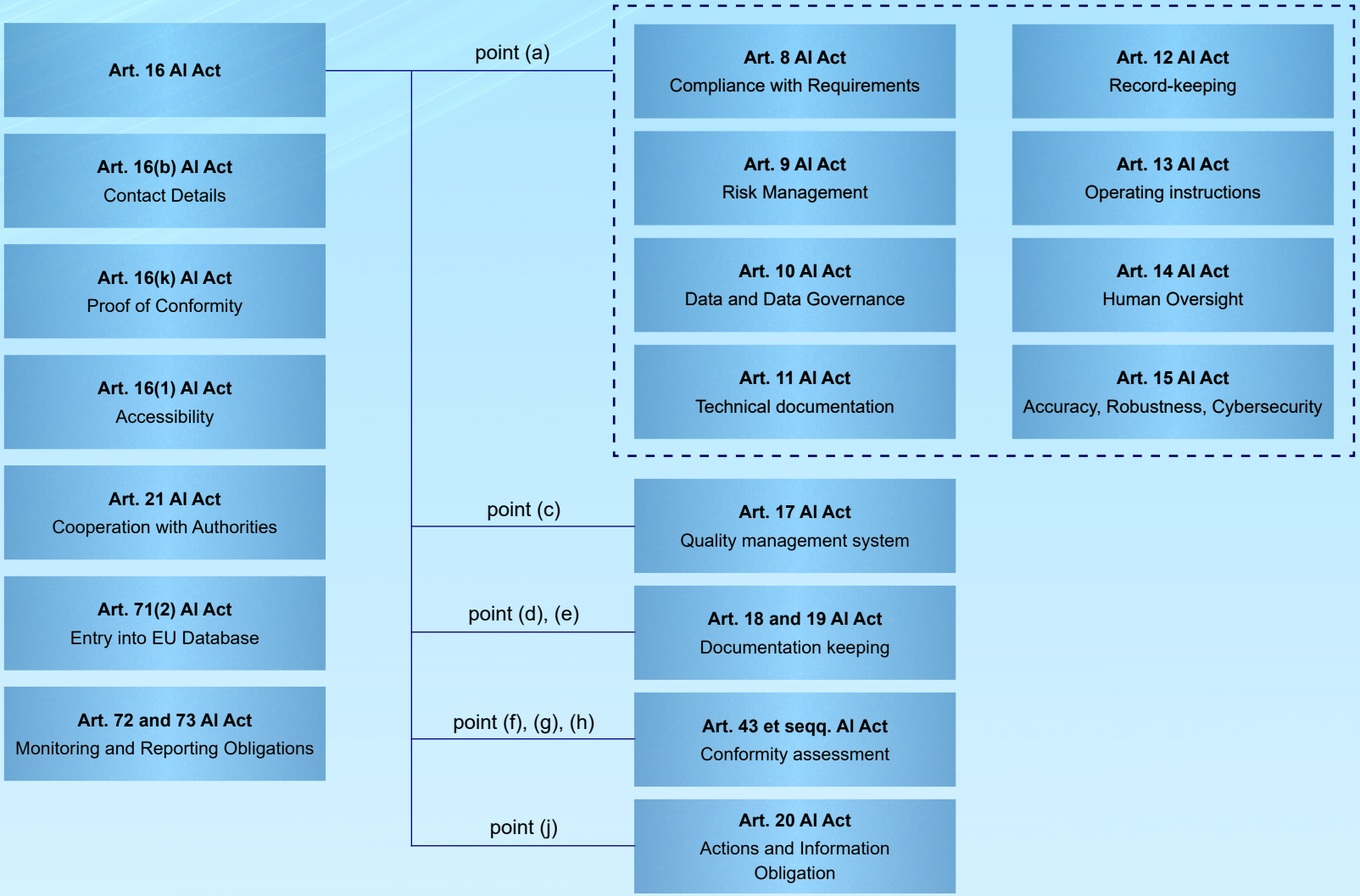
The Act excludes from the high-risk AI system category those AI systems listed in Annex III that meet one of the following criteria, on the basis that such systems do not pose a significant risk of harm to individuals:

- performs a narrow procedural task;
- improves the result of a previously completed human activity;
- detects decision-making patterns or deviations and is not meant to replace or influence the previously completed human assessment (without proper human review); or
- performs a preparatory task to an assessment relevant for the purposes of the use cases listed in Annex III.

AI systems cannot benefit from this exclusion if the system profiles individuals.

High-Risk AI Systems

Obligations on Providers of High-Risk AI Systems



High-Risk AI Systems

Providers of high-risk AI systems must comply with a range of obligations, including:

Risk Management

Providers are required to implement a comprehensive risk management system, which must be continuously applied throughout the system's life cycle and regularly reviewed and updated. Several EU data and digital laws include requirements for effective risk assessments — including the Digital Services Act, General Data Protection Regulation, Network and Information Systems Directive, and the Cyber Resilience Act — necessitating a consistent approach to assessing core risks across services, technologies, and user bases.

Data and Data Governance

High-risk AI systems must meet minimum data quality and management standards for training, validation, and testing, emphasising the critical role of effective data governance for providers of high-risk AI systems.

Human Oversight

High-risk AI systems must be designed to allow for effective human oversight, which must be carried out by individuals with appropriate skills and authority, and reflect the system's risks, level of autonomy, and context of use.

Accuracy, Robustness, and Cybersecurity

High-risk AI systems must be designed for appropriate levels of accuracy, robustness, and cybersecurity throughout their life cycle. For example, systems must: be resilient to errors, faults, or inconsistencies; be protected against attempts to exploit system vulnerabilities; minimise the risk of biased outputs (relevant to systems that continue to learn once on the market).

Instructions for Use

Providers of high-risk AI systems are required to provide deployers of their systems with concise, complete, and accurate instructions for the use of the system, to enable them to appropriately interpret and use the AI system and its outputs. The Act mandates the minimum information providers must include on these instructions, such as the system's features and capabilities, accuracy levels and metrics, and human oversight measures.

Quality Management System

Providers of high-risk AI systems are required to establish and document a comprehensive quality management system to ensure compliance with the Act, covering aspects such as regulatory compliance, design and development procedures, quality control, data management, and risk management. Providers that are already subject to sector-specific quality management obligations may integrate these AI-specific aspects into their existing quality management processes.

Corrective Actions

If a provider of a high-risk AI system finds or suspects that the system does not comply with the Act, the provider must immediately remedy the issue or withdraw, disable, or recall the AI system. If a high-risk AI system poses a risk to an individual's health, safety, or fundamental rights, the provider is required to inform the relevant market surveillance authorities.

High-Risk AI Systems

Conformity Assessments and Post-Market Monitoring

The Act establishes a comprehensive conformity assessment and certification regime for high-risk AI systems. This regime includes the release of EU-harmonised standards and common specifications for high-risk AI systems. Systems meeting such standards will be presumed to comply with the Act, which will be of significant practical relevance to providers. Before placing high-risk AI systems on the market, providers must carry out an internal conformity assessment process. The internal assessment processes must verify that the AI system (including its design and development process), the provider's quality management system, and the post-market monitoring process are compliant.

Conformance assessments are an ongoing requirement; providers must complete a new conformity assessment if the AI system is substantially modified (though pre-determined continuous learning once the system has been deployed does not require a new assessment). Providers of remote biometric identification and biometric categorisation AI systems (falling under point 1 of Annex III) are required to undergo a third-party assessment process carried out by the national notified bodies (see Supervision and Enforcement) in certain circumstances (e.g., if the provider has not fully applied relevant harmonised conformity standards or common specifications). If a third-party assessment is not required, such biometric AI system providers may complete an internal assessment process.

Following the conformity assessment, providers are required to issue a written, machine-readable EU declaration of conformity for the high-risk AI system and retain it for 10 years, to be made available to the national authorities. Providers should also label the AI system with the EU-recognised CE marking to visibly confirm compliance with the Act. Providers of high-risk AI systems subject to conformity assessment, declaration, and CE marking requirements under other relevant EU laws must issue a single declaration and CE label covering all applicable requirements.

After placing a high-risk AI system on the market, providers must conduct post-market monitoring to evaluate ongoing compliance with the Act, proportionate to the specific nature and risks of the AI system. Providers must immediately report any serious incidents identified through monitoring to the relevant national market surveillance authorities. Serious incidents are defined in the Act, and include death or serious harm to health, violation of fundamental rights, and serious disruption to critical infrastructure.

Technical Documentation

Providers are required to implement and maintain comprehensive technical documentation, to be made available to national authorities and notifying authorities.

High-Risk AI Systems

Record-Keeping

High-risk AI systems must feature event-logging functionality to capture events relevant to risk assessments, post-market monitoring, and operational oversight. Providers must keep these logs for at least six months.

Documentation

Providers of high-risk AI systems must retain certain documentation for 10 years after the system is placed on the market, to ensure such documentation is available to national authorities, including required: technical documentation; quality management system documentation; and declarations of conformity.

Registration

Providers of high-risk AI systems are required to register themselves and their AI systems in the high-risk AI system EU database, to be established by the Commission.

Cooperation With Authorities

Providers of high-risk AI systems are required to cooperate with relevant supervisory authorities (see Supervision and Enforcement), including providing information and documentation to demonstrate compliance with the Act.

Obligations on Deployers of High-Risk AI Systems

Operational Measures:

- Implement appropriate technical and organisational measures to ensure that use of high-risk AI systems is in accordance with the provider's instructions.
- Ensure input data is representative, qualitative, and relevant for the AI system's intended purpose.
- Suspend use if the high-risk AI system poses a risk or does not perform as intended.

Control and Risk-Management:

- Where applicable, carry out, document, and maintain a fundamental rights impact assessment in relation to the AI system.
- Assign competent individuals to oversee the functioning of the AI system and implement the human oversight measures indicated by the providers.
- Monitor the AI system for risks, anomalies, and unexpected performance.

Training and Support:

- Provide necessary training and support for those overseeing the system to ensure they have the necessary competence and authority to carry out their role.

Documentation:

- Maintain logs of the AI system's operations for at least six months.

High-Risk AI Systems

Notification and Transparency:

- Notify the provider and relevant national authorities in case of risks to the health, safety, or fundamental rights of individuals or a serious incident.
- Inform the provider of the AI system of any relevant operational circumstances that arise, as instructed by the provider.
- Inform individuals that may be affected by the output of the AI system about the use of the system.

Cooperation:

- Cooperate with EU and national authorities.

A deployer of a high-risk AI system will be treated as the provider of the AI system (and required to comply with the provider's obligations) if that deployer substantially modifies the AI system (such that it remains or becomes a high-risk AI system) or applies its own branding to the AI system (see AI Act Scope).

PRACTICAL STEPS

- Map AI systems and use cases and identify uses that could potentially fall within the high-risk categories (as part of a wider AI system mapping and risk categorisation process, as relevant). The determination of high-risk AI uses is a potentially complex exercise in practice in particular due to the various exclusions applicable. AI system providers may wish to consider whether they can modify their potentially high-risk AI systems in order to benefit from such exclusions, and therefore avoid the high-risk category obligations.
- Determine your organisation's role in relation to each high-risk AI system (e.g., provider, deployer, etc.) in the context of the wider AI value chain, paying particular attention to situations in which a deployer may be treated as a provider (i.e., white labelled or modified AI systems).
- Regularly review AI system categorisations to capture any AI practices that may have evolved into high-risk AI system uses.
- Develop and document a compliance approach for each applicable set of high-risk AI system obligations (e.g., as a provider or a deployer). Compliance with several of these obligations, particularly those applicable to AI system providers, may require alignment with similar obligations in other EU regulations such as transparency, risk assessments, and cybersecurity. Compliance approaches should also be aligned with any applicable sector-specific legislation and leverage related testing, reporting, post-market monitoring, transparency, and documentation requirements.

Related Insights: EU AI Act: Obligations for Deployers of High-Risk AI Systems
AI Act Update: EU Resolves to Change Rules and Extend Deadlines
European Commission Publishes Draft Guidance on Reporting Serious AI Incidents

GPAI Models

KEY POINTS

ARTICLES 51-56, ANNEXES XI-XIII

In force from:

The GPAI model requirements apply from 2 August 2025 for new models placed on the market after this date; providers of GPAI models already on the market before 2 August 2025 have until 2 August 2027 to bring models into compliance.

Applicable to:

Providers of GPAI models

Penalties:

Fines of up to the greater of €15 million or 3% of total worldwide annual turnover per violation and potentially other penalties including corrective measures (see Supervision and Enforcement). The AI Office enforces the penalties regime, which will apply from 2 August 2026.

Guidance:

Commission template for reporting serious incidents involving GPAI with systemic risk

Commission Guidelines on the scope of obligations for providers of general-purpose AI models under the AI Act; Commission Template for the Public Summary of Training Content; GPAI Code of Practice

The Act imposes several requirements on providers of GPAI models. A GPAI model is defined as:

"an AI model, including where such an AI model is trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable of competently performing a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications, except AI models that are used for research, development or prototyping activities before they are released on the market", with a focus on the generality of the model (capturing, for example, large language models).

The Act regulates GPAI models separately from any AI systems into which a model may be integrated (a downstream system) and both sets of requirements under the Act — for GPAI models and AI systems — apply in parallel.

GPAI Models

The obligations on providers of GPAI models include:

- Making publicly available a sufficiently detailed summary of the GPAI model's training data in the mandatory form provided by the AI Office.
- Making available to providers of downstream AI systems that integrate the GPAI model relevant and up-to-date information, including mandatory minimum information set out in the Act, to enable those providers to understand the capabilities and limitations of the GPAI model and comply with their obligations under the Act.
- Implementing a policy to comply with EU law on copyright and related rights, including complying with rightholders' opt-outs from the inclusion of their copyright protected material in GPAI model training data sets (pursuant to the Directive on Copyright in the Digital Single Market), noting that the territorial scope of this requirement — particularly whether it applies to models developed outside the EU — remains the subject of significant controversy.
- Maintaining technical documentation, including mandatory minimum information set out in the Act, to be made available to the AI Office and national authorities.

Additional obligations apply to providers of GPAI models with systemic risk, defined in the Act as models with "high-impact capabilities", which is presumed if the cumulative training compute of the model exceeds 10^25 FLOPs. In addition to the obligations applicable to all GPAI model providers, providers of GPAI models with systemic risk must:

- Perform model evaluations including adversarial testing of the model
- Assess and mitigate systemic risks arising from the development and use of the model
- Notify the AI Office and national authorities of serious incidents relating to the model
- Ensure cybersecurity measures for the model and associated physical infrastructure

The GPAI Code of Practice, published by the AI Office and endorsed by the Commission and the AI Board, is a voluntary tool intended to help providers of GPAI models demonstrate compliance with their obligations under the Act. The Code of Practice is divided into three chapters: transparency; copyright; and safety and security. Signatories to the Code of Practice commit to a range of measures and standards aligning with the GPAI model requirements in the Act. The Code of Practice is not mandatory, though providers of GPAI models that do not sign up to the Code of Practice are required to demonstrate compliance via other means.

GPAI Models

PRACTICAL STEPS

- Map AI models and assess whether each model falls within the scope of the GPAI models requirements under the Act.
- Assess in-scope GPAI models against systemic risk thresholds to identify models potentially subject to additional obligations applicable to models with system risk.
- Develop and document a compliance approach to meet the Act's GPAI model requirements, including consideration of signing up to the GPAI Code of Practice (in whole or in part) or relying on alternative means to demonstrate compliance.
- Regularly review mapping and assessments of AI models, particularly as the systemic risk thresholds may be periodically amended by the Commission; document AI model mapping and risk assessments as part of wider AI governance processes.

Related Insights: EU AI Act: GPAI Model Obligations in Force and Final GPAI Code of Practice in Place

Transparency

KEY POINTS

ARTICLES 13, 50, 53

In force from:

2 August 2026 for AI systems, other than provider obligations for generative AI systems which apply from 2 December 2026; 2 August 2025 for GPAI models

Applicable to:

Providers and deployers of certain AI systems; providers of GPAI models

Penalties:

For relevant AI systems, fines of up to the greater of €15 million or 3% of total worldwide annual turnover per violation, and potentially other penalties under national frameworks (see Supervision and Enforcement). National market surveillance authorities enforce the penalties regime for transparency requirements, which came into effect on 2 August 2025.

For GPAI models, fines of up to the greater of €15 million or 3% of total worldwide annual turnover per violation and potentially other penalties including corrective measures (see Supervision and Enforcement). The AI Office enforces the penalties regime for GPAI models, which will apply from 2 August 2026.

Guidance:

Commission Template for the Public Summary of Training Content; GPAI Code of Practice; Draft Code of Practice on marking and labelling of AI-generated content

The Act mandates transparency obligations for providers and deployers of various types of AI systems and for providers of GPAI models.

Transparency obligations for providers and deployers of certain AI systems (subject to exemptions):

Provider Obligations

Interactive AI systems (e.g., chatbots)

- Providers of AI systems that interact directly with individuals must design and develop the AI system to inform the individual that they are interacting with an AI system (unless obvious).

Transparency

Generative AI systems

- Providers of generative AI systems must label outputs as artificially generated or manipulated in a machine-readable and detectable format. Certain exceptions apply, such as for AI systems that perform an assistive function for standard editing or do not substantially alter the input data provided by the deployer. The AI Act Omnibus delays the application of this obligation from 2 August 2026 to 2 December 2026 for those providers that have placed their AI system on the market before 2 August 2026.

Deployer Obligations

Deepfakes

- Deployers of AI systems that generate content constituting a deepfake must disclose that the content has been artificially generated or manipulated.

Text on matters of public interest

- Deployers of AI systems that generate or manipulate text published for the purpose of informing the public on matters of public interest must disclose that the text has been artificially generated or manipulated. This disclosure requirement does not apply if the content has undergone human review or editorial control and a natural or legal person holds editorial responsibility for the content.

Emotion recognition or biometric categorisation systems

- Deployers of emotion recognition systems or a biometric categorisation systems must inform impacted individuals of the operation of the system, and must comply with the GDPR.

Transparency information must be provided to individuals in a clear manner when they first interact with the relevant AI system or are first exposed to the relevant content.

Transparency Obligations for High-Risk AI Systems

Providers of high-risk AI systems must comply with specific transparency requirements intended to ensure that deployers of high-risk AI systems can interpret the system's output and use it appropriately. These requirements mandate that high-risk AI systems be accompanied by concise, accurate, and comprehensive instructions that contain:

- the identity and contact details of the provider;
- the characteristics, capabilities, and performance limitations of the high-risk AI system (including intended purpose, accuracy, explainability, cybersecurity, and training data specifications);
- changes to the relevant high-risk AI system and its performance that have been pre-determined by the provider at the moment of the initial conformity assessment, if any;
- human oversight measures (see High-Risk AI Systems) including the technical measures put in place to facilitate the deployer's interpretation of the system outputs;
- the computational and hardware resources needed, the expected lifetime of the high-risk AI system, and any necessary maintenance and care measures; and
- if relevant, a description of the mechanisms that allow the deployer to collect, store, and interpret system logs.

Transparency

Transparency Obligations for Providers of GPAI Models

(see GPAI Models)

Providers of GPAI models are required to:

- Make publicly available a sufficiently detailed summary of the GPAI model's training data in the mandatory form provided by the AI Office.
- Make available to providers of downstream AI systems that integrate the GPAI model relevant and up-to-date information, including mandatory minimum information set out in the Act, to enable those providers to understand the capabilities and limitations of the GPAI model and comply with their obligations under the Act.
- Maintain technical documentation, including mandatory minimum information set out in the Act, to be made available to the AI Office and national authorities.

The transparency chapter of the GPAI Code of Practice (see GPAI Models) includes a model documentation form aligning with the above transparency requirements. In relation to the requirement to provide a public summary of the model's training data, the AI Office has published a mandatory template that all providers of GPAI models must complete in order to comply with this transparency requirement (see Guidance).

PRACTICAL STEPS

- Map AI systems and identify AI systems that could potentially be subject to specific transparency requirements under the Act (e.g., chatbots).
- Determine your organisation's role in relation to each AI system (e.g., provider, deployer, etc.) in the context of the wider AI value chain.
- Develop and document a compliance approach to meet the transparency requirements under the Act applicable to each relevant AI system, depending on your organisation's role. Compliance with relevant transparency requirements under the Act may require alignment with similar transparency obligations in other EU regulations, such as the GDPR.
- In relation to high-risk AI systems and GPAI models, integrate compliance with applicable transparency requirements into broader compliance approaches for such systems or models (see High-Risk AI Systems and GPAI Models).

Related Insights: EU AI Act: GPAI Model Obligations in Force and Final GPAI Code of Practice in Place

Supervision and Enforcement

KEY POINTS

CHAPTER VII, CHAPTER IX, CHAPTER XII

In force from:
2 August 2025, excluding enforcement and penalties against GPAI model providers, which apply from 2 August 2026

Applicable to:
Providers and deployers of AI systems; providers of GPAI models

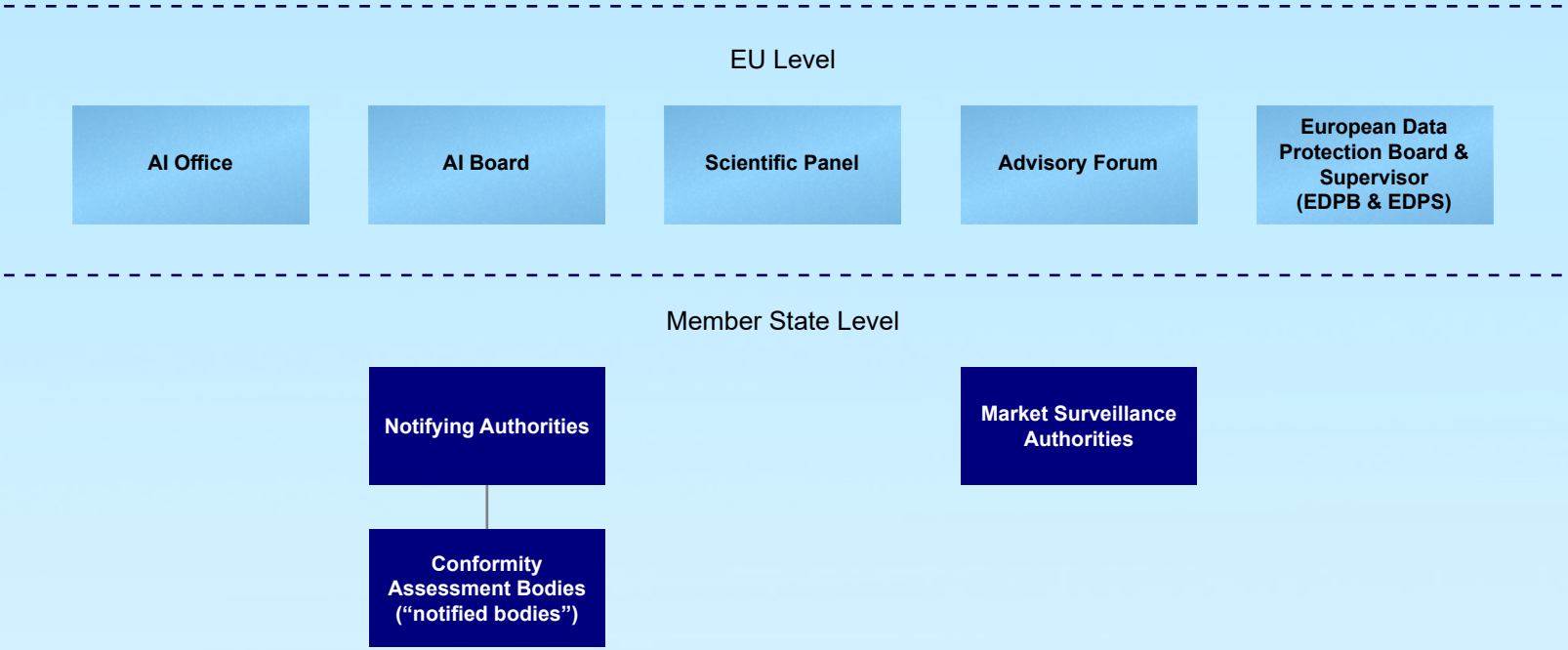
The Act is supervised and enforced by various bodies at both EU and Member State levels, including:

- The **AI Office** is a function within the European Commission with overall responsibility for the implementation of the Act, including delegated regulation and guidance. In addition, the AI Office is exclusively responsible for supervision and enforcement of the Act against providers of GPAI models and for classifying GPAI models with systemic risk (see GPAI Models).
- The **AI Board** is composed of one representative per Member State and tasked with advising, assisting, and coordinating between the Commission and the Member States to facilitate consistent and effective application of the Act. For example, by issuing recommendations and opinions and sharing technical expertise among Member States.
- The **Advisory Forum** provides technical expertise to the AI Board and the AI Office. It includes a mix of stakeholders including industry, startups, small- and medium-sized enterprises, civil society, and academia.
- The **Scientific Panel** consists of AI experts selected by the Commission who are impartial and independent from the AI industry and AI system providers. The Panel advises and supports the AI Office, for example by identifying possible systemic risks and advising on the classification of AI models.
- The **European Data Protection Supervisor (EDPS)** is the competent authority for the supervision of EU institutions, bodies, offices, and agencies to the extent they fall within the scope of the Act (see AI Act Scope).

Supervision and Enforcement

- **National authorities**, including **market surveillance authorities** (**MSAs**) and **notifying authorities,** are responsible for enforcing requirements related to prohibited AI practices, high-risk AI systems, transparency, and all other aspects of the Act except GPAI requirements (which are exclusively enforced by the AI Office in the European Commission). MSAs are empowered to investigate potential violations of the Act, including requesting information and evaluating AI systems. Member States were required to appoint at least one market surveillance authority by 2 August 2025. Member States were also required to appoint at least one notifying authority by this date, responsible for designating national **conformity assessment bodies** (**notified bodies**) to conduct the conformity assessments required for certain high-risk AI systems.

Authorities under the AI Act



Supervision and Enforcement

Penalties

Penalties under the Act include non-monetary penalties (such as warnings or compliance orders) and significant fines.

Penalties Imposed by National Authorities Against AI System Providers and Deployers

Member States are responsible for establishing national penalty frameworks under the Act for enforcement by national MSAs and notifying authorities, which must be effective, proportionate, and dissuasive within the parameters set out in the Act:

- Fine range:
  - Prohibited AI practices (see Prohibited AI Practices): The higher of €35 million or 7% of total worldwide annual turnover
  - Cooperation obligations (for example, providing incorrect, incomplete, or misleading information to an MSA): The higher of €7.5 million or 1% of total worldwide annual turnover
  - High-risk AI system, transparency, and other obligations (excluding GPAI requirements): The higher of €15 million or 3% of total worldwide annual turnover
- Criteria for determining fines: The Act sets out non-exhaustive list of criteria that MSAs must consider when deciding on the imposition and amount of a fine.

Penalties Imposed by the AI Office Against GPAI providers

The AI Office may impose fines on providers of GPAI models for violations of the GPAI model-specific requirements, and other applicable obligations (such as the appointment of an EU representative), under the Act (see GPAI Models). Fines can amount to the higher of €15 million or 3% of total worldwide annual turnover. The AI Office may also require GPAI providers to permit access to GPAI models and to take corrective measures or restrict or withdraw the model from the market. Penalties for GPAI model providers apply from 2 August 2026.

Fines Under the Act and the GDPR

AI systems frequently interact with personal data regulated by the GDPR (for example, as part of training data sets, inputs, and outputs). AI system providers and deployers may therefore be exposed to fines and other penalties from both Act supervisory authorities and GDPR supervisory authorities (though the principle against double jeopardy, confirmed in the Act, would prevent authorities from applying penalties under multiple regulations for the same violation or action).

Supervision and Enforcement

Civil Liability Risks

In parallel to the penalties regime under the Act, civil liability frameworks apply to various aspects of the development and deployment of AI systems, including:

- **AI Act:** Whilst the Act does not explicitly provide for a private or civil right of action, impacted parties are able to invoke the Act directly in EU national courts as a basis for a damages claim.
- **Revised Product Liability Directive:** AI systems and AI components fall within the expanded scope of the revised Product Liability Directive's strict liability regime for defective products; an AI system may be considered defective if it fails to meet the Act's relevant safety standards (see High-Risk AI Systems).
- **GDPR:** AI systems that interact with personal data regulated by the GDPR may be subject to civil damages claims under the GDPR for violations of the GDPR.
- **Representative Actions Directive:** The Act and the GDPR are included in the list of legislative instruments actionable under the Representative Actions Directive, and may therefore serve as a basis for collective damages actions.

PRACTICAL STEPS

- Maintain and document AI compliance approaches and governance, aligned with any broader data and innovation governance, to establish a robust, comprehensive, and consistent compliance position.
- Regularly review and refresh compliance and governance records, including risk assessments, risk categorisations under the Act, transparency, technical documentation, internal policies, etc.
- Conduct regular and comprehensive AI, data, and technology audits and testing.

Related Insights: New EU Product Liability Directive Comes Into Force

Contacts

Sophie Goossens
London / Paris
sophie.goossens@lw.com
+44.20.7710.3080

Jean-Luc Juhan
Paris
jean-luc.juhan@lw.com
+33.1.4062.2000

Susan Kempe-Müller
Frankfurt
susan.kempe-mueller@lw.com
+49.69.6062.6580

Alfonso Lamadrid
Brussels
alfonso.lamadrid@lw.com
+32.2.788.6310

Tim Wybitul
Frankfurt / Brussels
tim.wybitul@lw.com
+49.69.6062.6560

Calum Docherty
London
calum.docherty@lw.com
+44.20.7710.1079

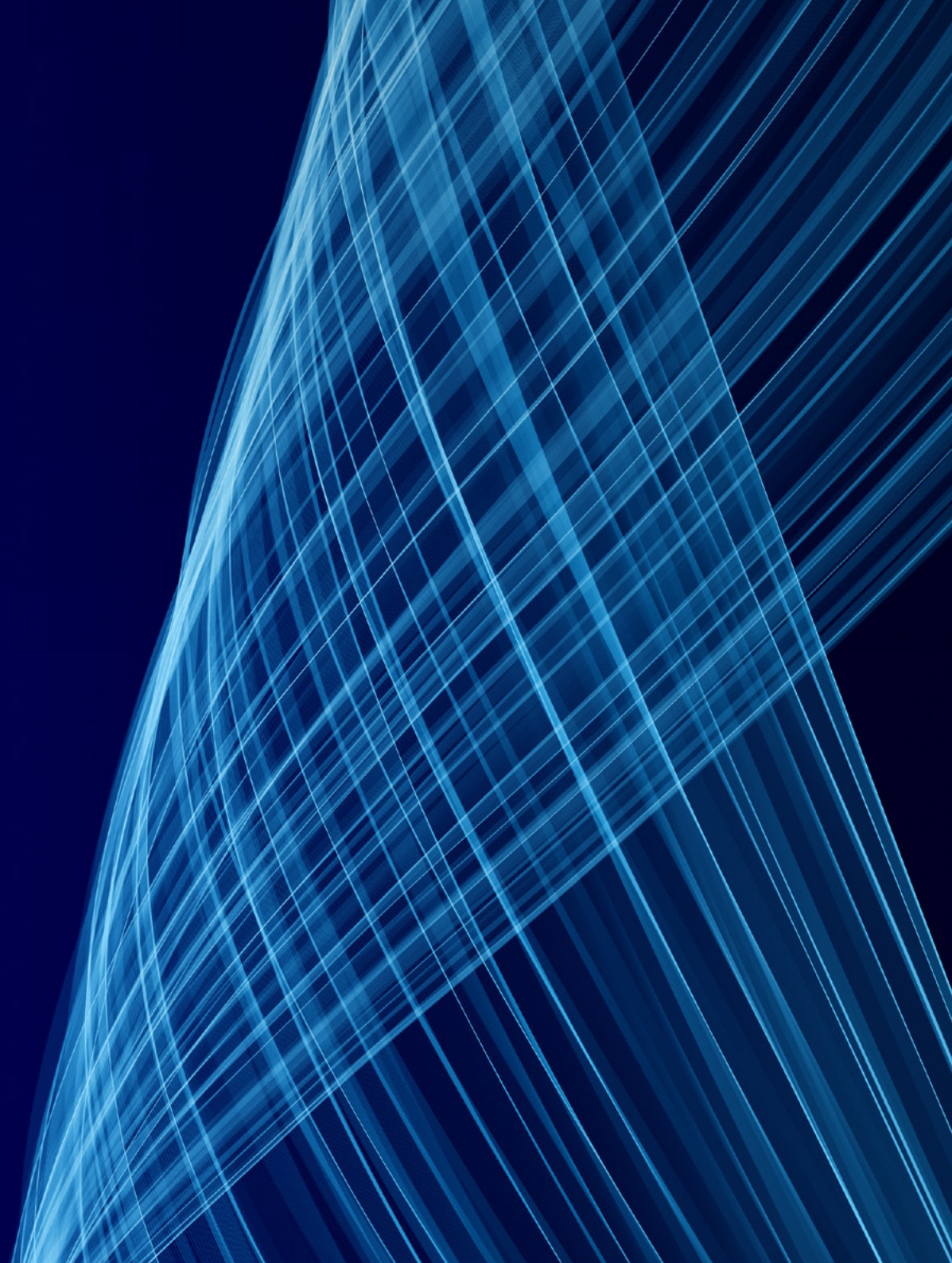
James Lloyd
London
james.lloyd@lw.com
+44.20.7866.2668

Fiona M. Maclean
London
fiona.maclean@lw.com
+44.20.7710.1822

Michael H. Rubin
San Francisco
michael.rubin@lw.com
+1.415.395.8154

LathamTECH

LATHAM&WATKINS



Latham & Watkins operates worldwide as a limited liability partnership organized under the laws of the State of Delaware (USA) with affiliated limited liability partnerships conducting the practice in France, Hong Kong, Italy, Singapore, and the United Kingdom and as an affiliated partnership conducting the practice in Japan. Latham & Watkins operates in Israel through a limited liability company, in South Korea as a Foreign Legal Consultant Office, and in Saudi Arabia through a limited liability company. © Copyright 2026 Latham & Watkins. All Rights Reserved.