ROPES & GRAY

The EU AI Act and Proposed Regulatory Frameworks in the UK and US:

The Road to Compliance

Topics

EU Artificial Intelligence Act 2024 (“EU AI Act”)

- Overview of EU AI Act
- Classification of Risk under EU AI Act
- Enforcement
- Timeline

What is the UK approach to AI regulation?

EU AI Act – Roadmap to Compliance

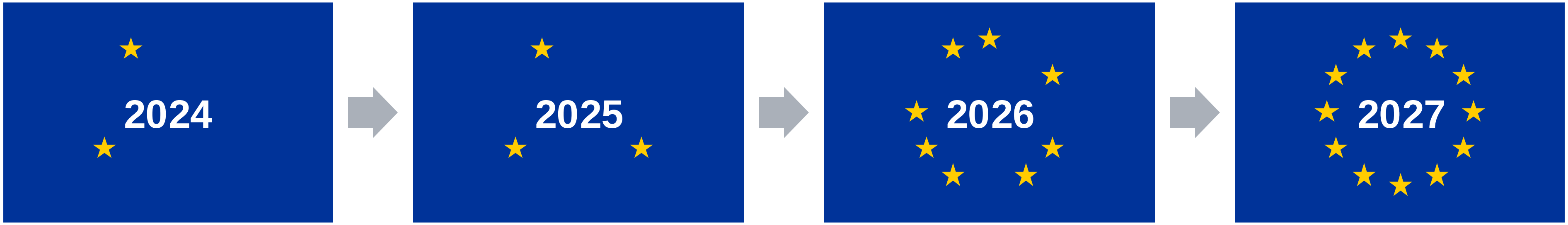
- Step 1: Create an AI Governance Committee
- Step 2: Define Involvement with AI Systems and Models
- Step 3: Assess Risk and Mitigation
- Step 4: Update Policies and Procedures
- Step 5: Implement AI Training
- Step 6: Monitor Legislative Developments

Key takeaways

Questions?

Overview of the EU AI Act

- Represents the first attempt to establish a legislative framework for AI.
- Classifies AI according to risk, with outright bans for AI presenting the highest risk and the degree of regulation corresponding with the risk presented by a particular AI system.
- Imposes significant obligations on a range of parties involved with high-risk AI systems.
- Broad territorial scope with an extraterritorial effect, covering providers and users of AI systems both within and outside of the EU.
- Enforcement options include fines of up to EUR 35 million or 7% of global revenue, as well as requests for information and powers to compel corrective measures or to recall the AI system from the market.
- Published in the Official Journal of the EU on 12 July 2024 and took effect on 1 August 2024.
- Staggered application of provisions between now and August 2027.


2024

Published

2025

Certain provisions take effect

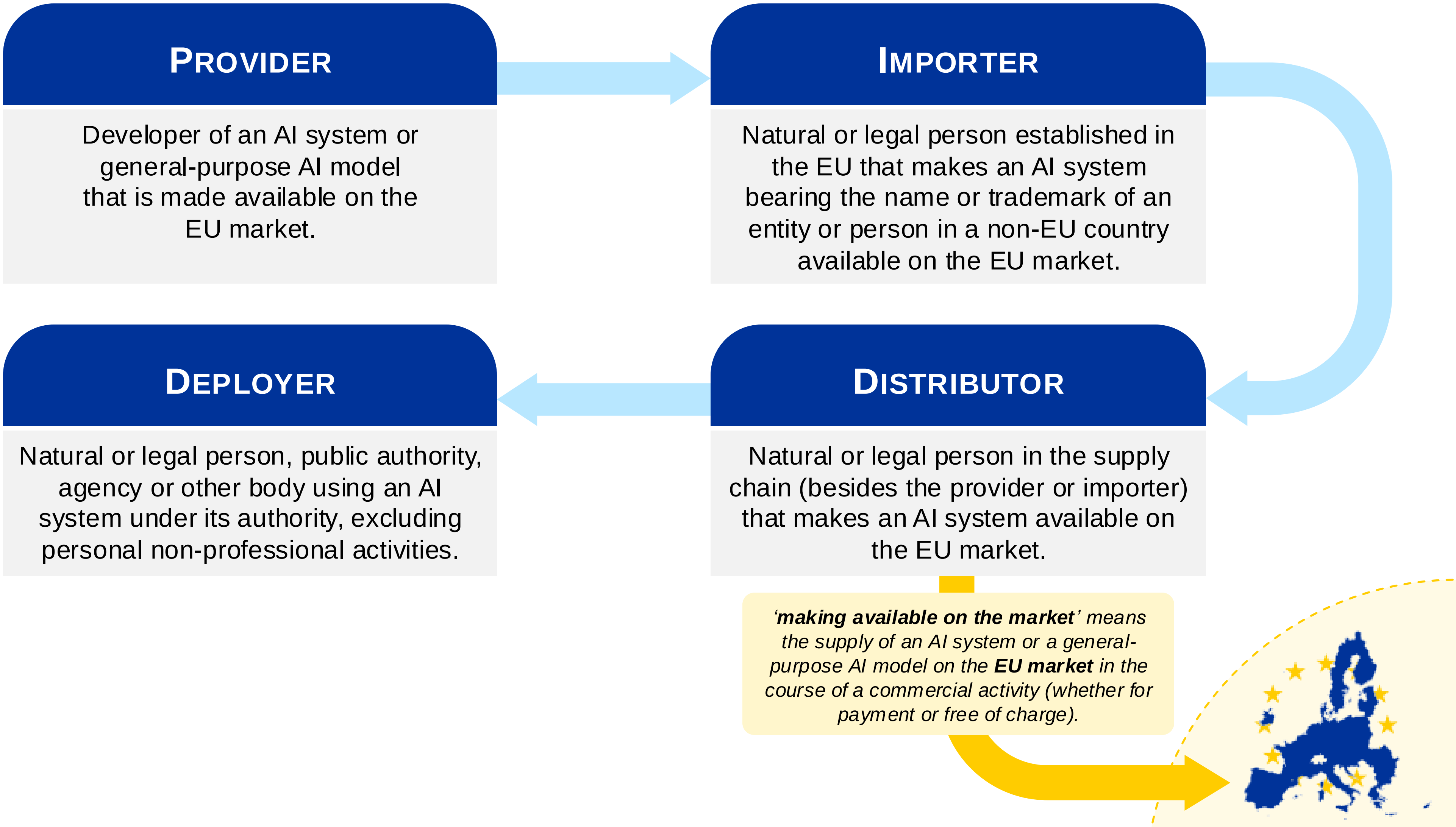
2026

Most provisions take effect

2027

Fully operational

Overview of the EU AI Act: Who falls within the scope?



PROVIDER

Developer of an AI system or general-purpose AI model that is made available on the EU market.

IMPORTER

Natural or legal person established in the EU that makes an AI system bearing the name or trademark of an entity or person in a non-EU country available on the EU market.

DISTRIBUTOR

Natural or legal person in the supply chain (besides the provider or importer) that makes an AI system available on the EU market.

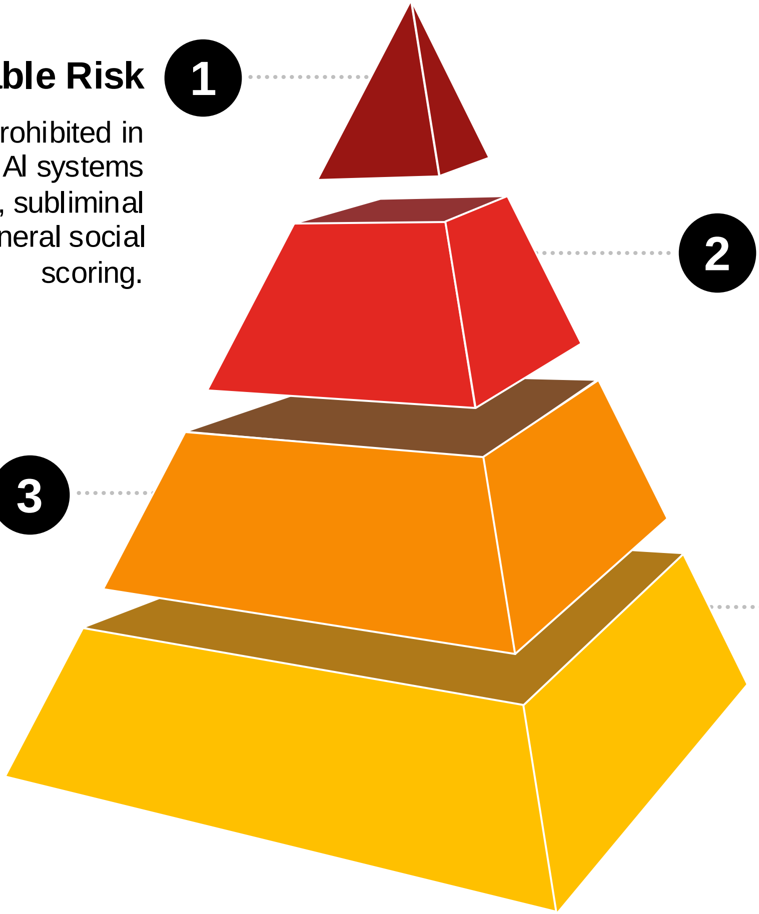
DEPLOYER

Natural or legal person, public authority, agency or other body using an AI system under its authority, excluding personal non-professional activities.

*‘**making available on the market**’ means the supply of an AI system or a general-purpose AI model on the **EU market** in the course of a commercial activity (whether for payment or free of charge).*

ROPES & GRAY

Classification of AI Risk under the EU AI Act



1 **Unacceptable Risk**

Highest level or risk prohibited in the EU. Includes AI systems using e.g., subliminal manipulation or general social scoring.

2 **High Risk**

Most regulated AI systems, as these have the potential to cause significant harm if they fail or are misused, e.g., if used in law enforcement or recruiting.

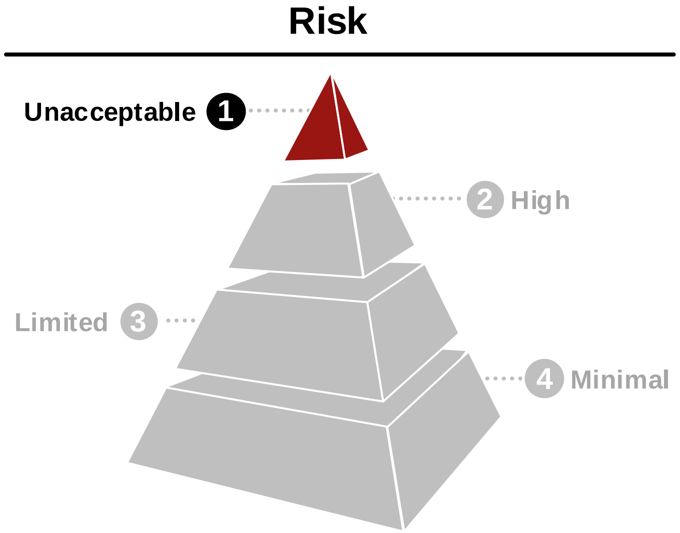
3 **Limited Risk**

Includes AI systems with a risk or manipulation or deceit, e.g., chatbots or emotion recognition systems. Humans must be informed about their interaction with the AI.

4 **Minimal Risk**

All other AI systems, e.g., a spam filter, which can be deployed without additional restrictions.

Classification of AI – Unacceptable Risk



**Limited exemptions, typically biometrics and in the context of law enforcement, medical, or safety sectors.*

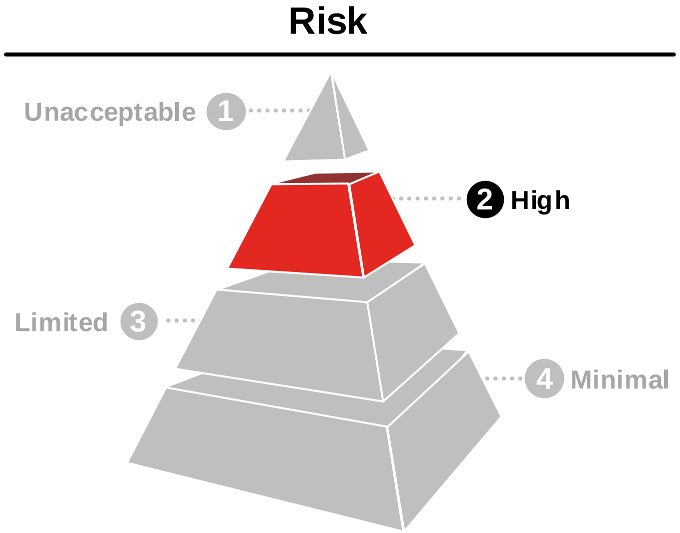
Unacceptable Risk – AI systems deemed to present an 'unacceptable risk' will be banned*, including those that:

- seek to materially distort the behaviour of a person or a group of persons;
- exploit vulnerabilities in a person or group of persons (e.g., age or disability);

  Example: Using techniques designed to manipulate children.
- use biometric categorisation to infer sensitive characteristics (e.g., political beliefs);
- engage in untargeted data scraping;

  Example: Scraping facial images from the internet or CCTV footage to create facial recognition databases.
- are used to infer emotions in the workplace and educational institutions; and/or
- conduct social scoring based on behaviour or personal characteristics.

Classification of AI – High-risk AI



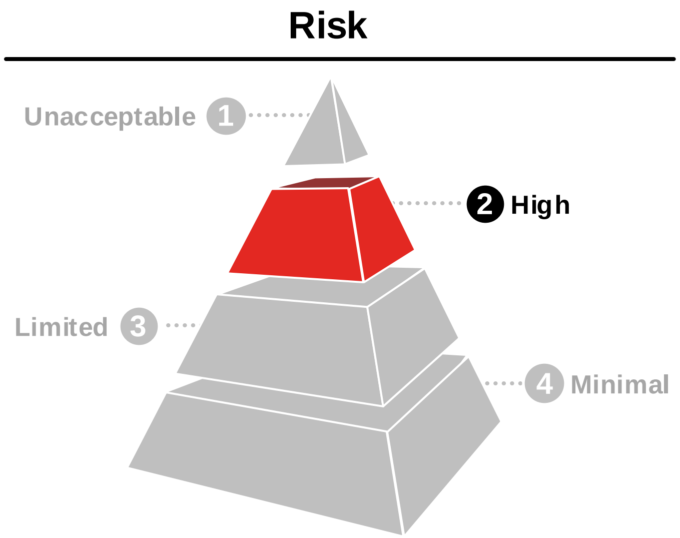
- **High Risk** – AI systems deemed to be high risk will be subject to the greatest number of obligations, including those used:
- as a safety component or safety product;

  Example: Deployment of AI in medical devices.
- for biometric or emotional identification;
- in educational and vocational training;
- in employment and management of workers;

  Example: Analysing and evaluating job applications and candidates.
- for essential public and private systems and services; and/or

  Example: Evaluating eligibility for access to credit or insurance.
- in the context of law enforcement, border control management and administration of justice processes.

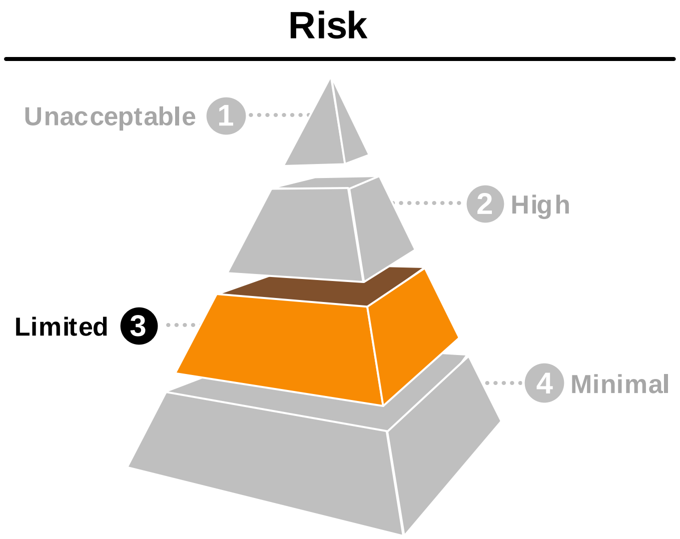
Classification of AI – High-risk AI



High Risk – The most onerous obligations fall on providers (developers) of AI systems, who must, amongst other things:

- implement a risk management system;
- conduct data set training, validation and testing requirements;
- maintain technical documentation;
- ensure accurate record-keeping;
- meet transparency requirements to aid users;
- ensure their systems are capable of being effectively overseen by humans; and
- meeting accuracy, robustness and cybersecurity requirements.

Classification of AI – Limited Risk AI



Limited Risk – AI systems that (otherwise present minimal risk but) are:

- intended to interact directly with humans;

  Example: Chatbot assistants on websites.

- capable of manipulating content; and
- capable of generating synthetic content.

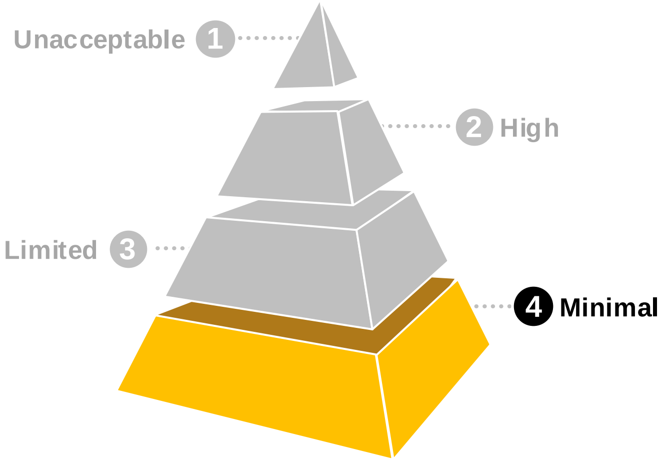
  Example: Generative AI systems (e.g., ChatGPT).

Obligations imposed on limited-risk AI systems include:

- Ensuring AI-generated content is detectable as having been artificially generated or manipulated; and
- Notifying users that they are engaging with an AI system rather than a human.

Classification of AI – Minimal Risk AI

Risk



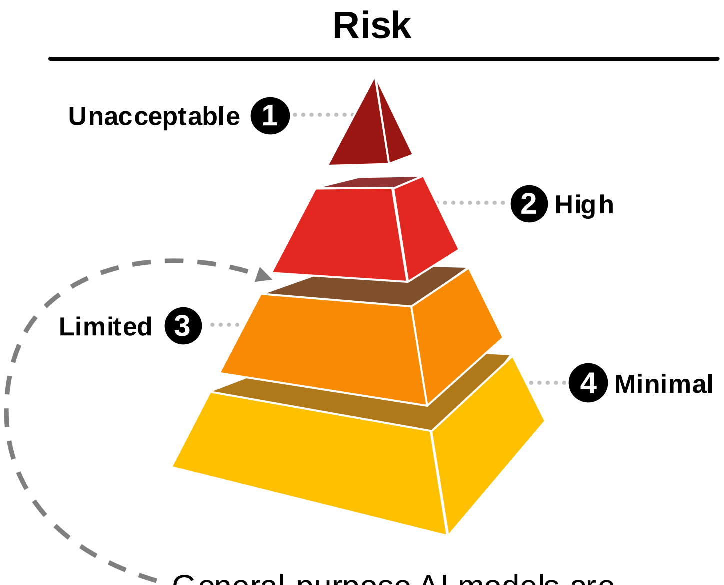
Minimal Risk – Minimal-risk AI systems include many existing technologies that pose little or no harm to the rights and safety of the user.

Example: AI-enabled video games

Example: Spam filters

Minimal-risk AI systems are subject to **no obligations** under the EU AI Act.

Classification of AI – General-Purpose AI Models



General-purpose AI models are deemed to present a level of risk between high and limited.

General-purpose AI models are regulated separately under EU AI Act, which uses a two-tier system to impose the following obligations:

- Tier 1 – **All general-purpose models**:
  - Maintain technical documentation;
  - Transparency obligations to users and downstream providers (including publishing information on the training data set); and
  - Maintain a copyright policy.
- Tier 2 – **General-purpose models posing 'systemic risk'** (trained with large amounts of data and complex capabilities).
  - Evaluation and testing requirements;
  - Cybersecurity obligations; and
  - Monitoring and reporting obligations.

Enforcement

New Regulators:

- EU member states will each designate a notifying authority and a market surveillance authority;
- **AI Office** (within the European Commission) will enforce the EU AI Act across the EU; and
- **AI Board**, comprising representatives of the member states, will advise and assist the European Commission and member states on application of the EU AI Act.

Market surveillance authorities have the authority to:

- Evaluate AI systems;
- Compel corrective action; and
- Prevent an AI system from being put into service or made available on a national market.

European Commission powers of enforcement in relation to generative AI:

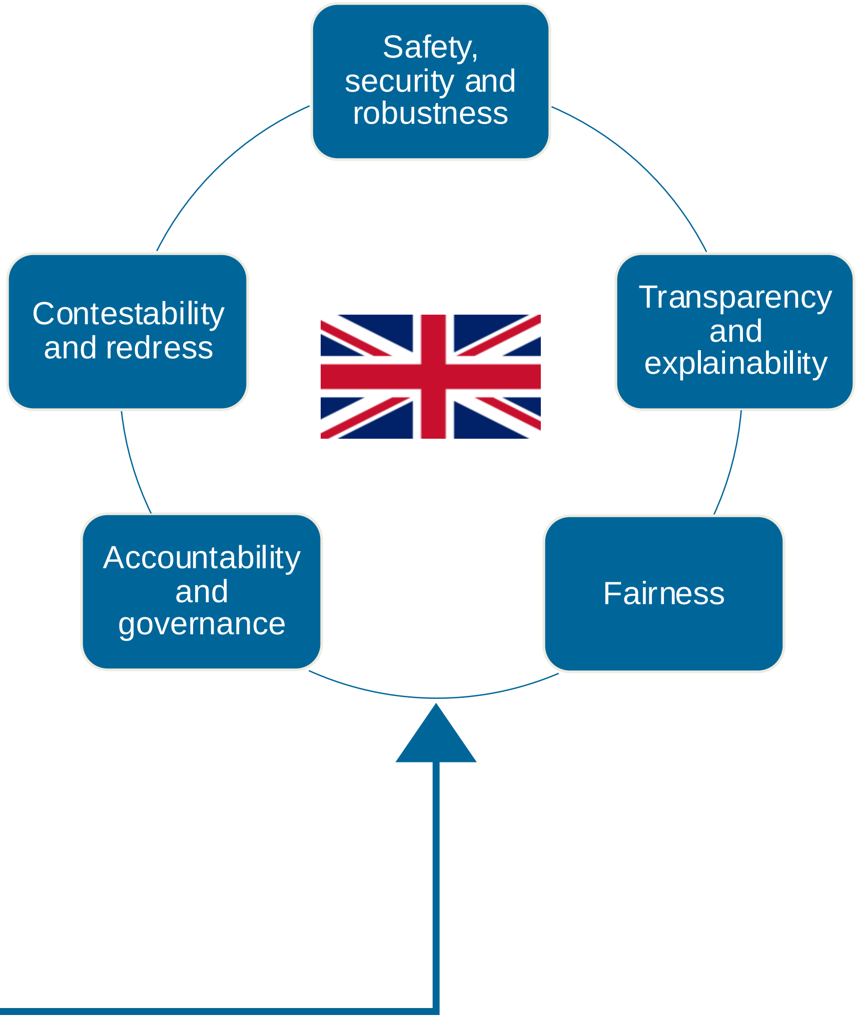
- Request documentation;
- Conduct evaluations;
- Implement measures; and
- Restrict, withdraw or recall AI models.

Fines

- Natural persons: a fine of up to EUR 35 million; and
- Undertakings: a fine of up to the higher of EUR 35 million or 7% of total worldwide turnover for the previous financial year.

What is the UK approach to AI regulation?

- UK proposals for regulating AI do not target specific technologies.
- The focus is on context to avoid stifling innovation or placing an undue burden on businesses.
- No new laws or sanctions have been proposed.
- Sector-specific guidance for organisations has been published by regulators including:
  - Competition and Markets Authority;
  - Bank of England; and
  - Information Commissioner's Office.
- New Government: The Labour Party's 2024 General Election manifesto pledged to introduce "binding regulation" on the handful of companies developing the most powerful AI models, in a way that "supports the development of the AI sector".
- Likely to take the form of a **principles-based regime**.



Safety, security and robustness

Transparency and explainability

Fairness

Accountability and governance

Contestability and redress

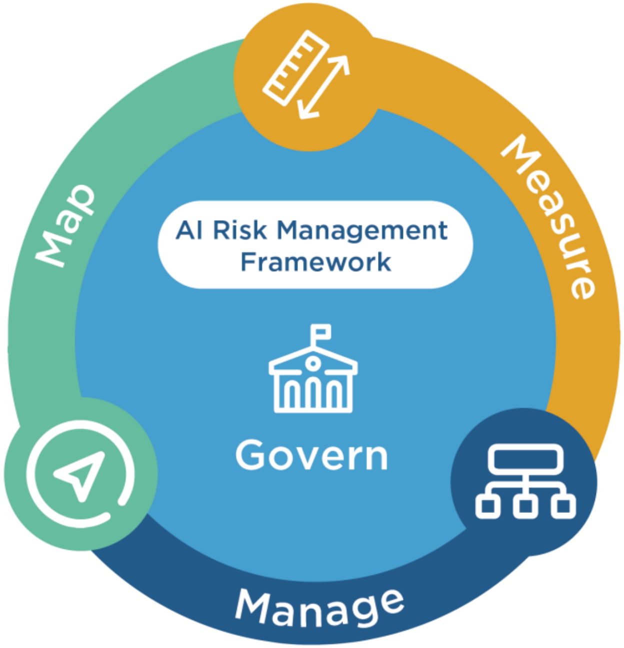
What is the US approach to AI regulation?

- **Executive Order No. 14110, "Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence"**
  - Issued by President Biden on Oct. 30, 2023
  - Does not directly regulate private industry, but notes AI's potential impact to national security
  - Requires agency guidelines that are likely to have significant impact through their incorporation into federal contracts as well as through voluntary adoption

- **Congress's Proposed AI Regulatory Frameworks**
  - Several proposed frameworks, including the SAFE Innovation Framework announced by Sen. Majority Leader Schumer in June 2023 and the Bipartisan Framework introduced by Senators Blumenthal and Hawley in September 2023
  - Congress has introduced targeted legislation to address the following issues: "(1) promoting AI [Research & Development] leadership; (2) protecting national security; (3) disclosure; (4) protecting election integrity; (5) workforce training; and (6) coordinating and facilitating federal agency AI use"

What is the US approach to AI regulation?

- NIST Guidance – Artificial Intelligence Risk Management Framework (January 2023)
  - Adopted broad non-binding guidance for the use of AI. Provides helpful insight into how the US government will generally think about the use of AI.



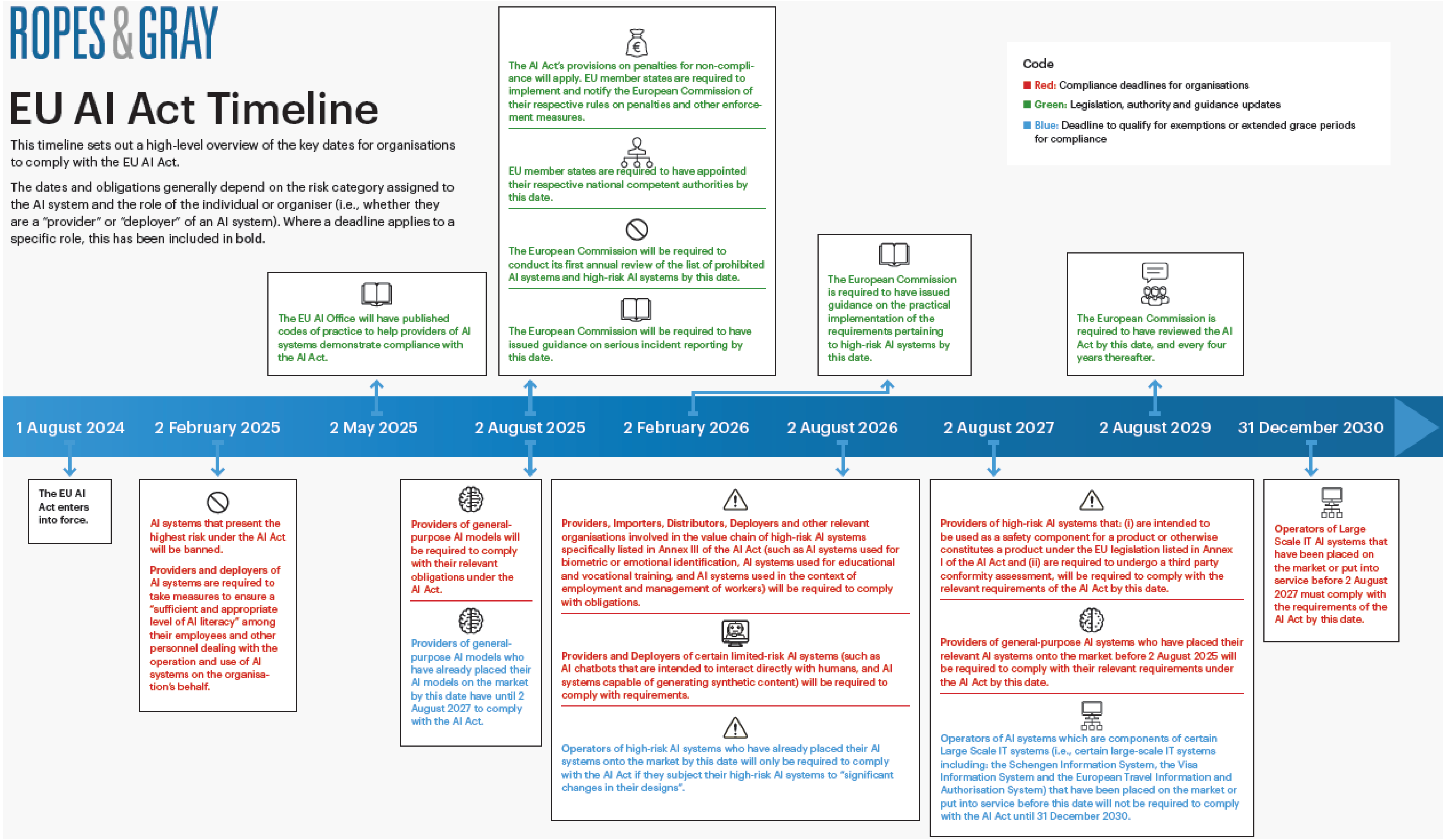
- Validation and reliability: demonstrating through ongoing testing or monitoring to confirm AI systems perform as intended
- Safety: providing real-time monitoring, backstops, or other intervention
- Secure and resilient: employing protocols to avoid, protect against, or respond to attacks against the AI system, and withstanding adverse events
- Accountability and transparency: making information available about the AI system to individuals interacting with it at various stages of the AI life cycle and maintaining organizational practices and governance to reduce potential harms
- Explainable and interpretable: understanding and properly contextualizing the mechanisms of an AI system as well as its output
- Fair, with harmful bias managed: promoting equity and equality and managing systemic, computational and statistical, and human-cognitive biases

What is the US approach to AI regulation?

- The National Conference of State Legislature reported that, as of June 3, 2024, at least 40 states have introduced AI bills, with many establishing task forces to study AI
  - Thirteen states have now enacted comprehensive privacy laws, many of which include requirements around “automated decisionmaking” or “profiling” technologies.
  - Antibias Laws – many states introduced or enacted legislation that prevents AI from making sensitive decisions to prevent bias

- Colorado passed the first comprehensive AI legislation in the US; goes into effect February 2026
  - Regulates High Risk AI systems that make a consequential decisions related to sensitive areas such as employment or insurance
  - Prohibits algorithmic discrimination / disparate treatment by AI
  - Requires disclosures and consumer transparency measures, including a statement from companies using High Risk AI

EU AI Act Timeline



ROPES & GRAY

EU AI Act Timeline

This timeline sets out a high-level overview of the key dates for organisations to comply with the EU AI Act.

The dates and obligations generally depend on the risk category assigned to the AI system and the role of the individual or organiser (i.e., whether they are a "provider" or "deployer" of an AI system). Where a deadline applies to a specific role, this has been included in bold.

Code

🟥 Red: Compliance deadlines for organisations

🟩 Green: Legislation, authority and guidance updates

🟦 Blue: Deadline to qualify for exemptions or extended grace periods for compliance

1 August 2024

The EU AI Act enters into force.

2 February 2025

AI systems that present the highest risk under the AI Act will be banned.

Providers and deployers of AI systems are required to take measures to ensure a "sufficient and appropriate level of AI literacy" among their employees and other personnel dealing with the operation and use of AI systems on the organisation's behalf.

2 May 2025

The EU AI Office will have published codes of practice to help providers of AI systems demonstrate compliance with the AI Act.

2 August 2025

The AI Act's provisions on penalties for non-compliance will apply. EU member states are required to implement and notify the European Commission of their respective rules on penalties and other enforcement measures.

EU member states are required to have appointed their respective national competent authorities by this date.

The European Commission will be required to conduct its first annual review of the list of prohibited AI systems and high-risk AI systems by this date.

The European Commission will be required to have issued guidance on serious incident reporting by this date.

Providers of general-purpose AI models will be required to comply with their relevant obligations under the AI Act.

Providers of general-purpose AI models who have already placed their AI models on the market by this date have until 2 August 2027 to comply with the AI Act.

2 February 2026

The European Commission is required to have issued guidance on the practical implementation of the requirements pertaining to high-risk AI systems by this date.

2 August 2026

Providers, Importers, Distributors, Deployers and other relevant organisations involved in the value chain of high-risk AI systems specifically listed in Annex III of the AI Act (such as AI systems used for biometric or emotional identification, AI systems used for educational and vocational training, and AI systems used in the context of employment and management of workers) will be required to comply with obligations.

Providers and Deployers of certain limited-risk AI systems (such as AI chatbots that are intended to interact directly with humans, and AI systems capable of generating synthetic content) will be required to comply with requirements.

Operators of high-risk AI systems who have already placed their AI systems onto the market by this date will only be required to comply with the AI Act if they subject their high-risk AI systems to "significant changes in their designs".

2 August 2027

Providers of high-risk AI systems that: (i) are intended to be used as a safety component for a product or otherwise constitutes a product under the EU legislation listed in Annex I of the AI Act and (ii) are required to undergo a third party conformity assessment, will be required to comply with the relevant requirements of the AI Act by this date.

Providers of general-purpose AI systems who have placed their relevant AI systems onto the market before 2 August 2025 will be required to comply with their relevant requirements under the AI Act by this date.

Operators of AI systems which are components of certain Large Scale IT systems (i.e., certain large-scale IT systems including: the Schengen Information System, the Visa Information System and the European Travel Information and Authorisation System) that have been placed on the market or put into service before this date will not be required to comply with the AI Act until 31 December 2030.

2 August 2029

The European Commission is required to have reviewed the AI Act by this date, and every four years thereafter.

31 December 2030

Operators of Large Scale IT AI systems that have been placed on the market or put into service before 2 August 2027 must comply with the requirements of the AI Act by this date.

EU AI Act – Roadmap to Compliance

1 Form Governance Committee

2 Clarify your company’s role in relation to AI systems

3 Assess risk and mitigation strategies

4 Update or draft policies and procedures

5 Implement AI training

6 Maintain programme and monitor for developments

Create an AI Governance Committee

STEP 1

STEP 2

STEP 3

STEP 4

STEP 5

STEP 6

Establish an AI Governance Committee

- Establish a dedicated AI Governance Committee with direct responsibility for ensuring adherence to the EU AI Act.
- Appoint members with appropriate expertise across all relevant fields, including AI, IT, the law, compliance, risk management and data governance and experience in their respective fields.
- Purpose of an AI Governance Committee:
  - Undertake independent audits of AI systems;
  - Set risk standards that must be adhered to; and
  - Advise development teams on compliance with regulatory and organisational standards.

Create an AI Governance Committee

STEP 1
STEP 2
STEP 3
STEP 4
STEP 5
STEP 6

AI Governance Committee – Key Functions

- Implement a long-term plan to ensure the necessary **frameworks, systems and documentation** are in place as each provision of the EU AI Act comes into force over the next three years.
- Begin collating information on **ethics, bias monitoring and data risks** immediately.
- Establish **internal standards and expectations** for the business using published guidance from bodies such as the International Organisation for Standardisation (ISO).
- If your client is a government body or public company, they may require guarantees that an AI system does not present bias and ethics concerns before agreeing to use it.

Define Involvement with AI Systems and Models

STEP 1 STEP 2 STEP 3 STEP 4 STEP 5 STEP 6

Clarify involvement of the business with AI systems and General-Purpose AI Models

- Determine whether your business is a **provider** (developer), **importer**, **distributor** or **deployer** (user) of AI systems, for the purpose of the EU AI Act.
- Identify practical considerations for the business that stem from the **extraterritorial scope** of the EU AI Act, such as:
  - Which third-party countries are relevant?
  - What is the nature of their relationship with the EU (e.g., Norway is not a member state but is in the Schengen area)?

Define Involvement with AI Systems and Models

STEP 1

STEP 2

STEP 3

STEP 4

STEP 5

STEP 6

Conduct a preventive AI inventory

- **Create an inventory** of all AI systems developed or used by the business.
- Categorise your inventory by reference to **purpose**, **functionality and data processed**, using your existing record of processing activities mechanisms and procedures.
- Identify those systems within the **scope of the EU AI** Act and classify them according to **risk**, using the risk classifications set out in the EU AI Act and the risk matrix below.
- Identify AI systems and models within the scope of the EU AI Act with which the business intends to **engage in the future**.

Risk Matrix				
Risk rating	Unacceptable	High	Moderate	Low
Role	Developer	Importer	Distributor	Deployer
Jurisdiction	European Union	Non-European Union		

Assess Risk and Mitigation

STEP 1

STEP 2

STEP 3

STEP 4

STEP 5

STEP 6

Apply risk ratings under EU AI Act and identify relevant obligations

- Using the risk classification framework set out in the EU AI Act, allocate a level of risk to each of the AI systems and models in which the business is involved.
  - Guidance from the new EU-wide regulators and regulators across the EU member states may be forthcoming, but do not wait for guidance before taking action.
- Identify, consider and prepare to fulfil the obligations imposed upon providers (developers), importers, distributors and deployers (users) of AI systems.
- Undertake risk analysis of dataset biases and data governance plans to ensure training of AI systems is done in accordance with an AI Ethics policy.
- If your business is buying into AI, consider whether guarantees as to the safety and quality of the system have been provided.

Assess Risk and Mitigation

STEP 1 STEP 2 **STEP 3** STEP 4 STEP 5 STEP 6

Develop compliance plans and mitigation strategies

- Design AI systems with built-in human oversight mechanisms so that humans always have the capacity to intervene in and override an AI system when necessary.
- Develop and implement a response plan for potential incidents, particularly in relation to high-risk AI systems.
- Undertake risk analysis of dataset biases and data governance plans to ensure training of AI systems is done in accordance with an AI Ethics policy.
- Agreements should ensure all parties are clear about their roles in the AI supply chain and that they are able to comply with their obligations.

Update Policies and Procedures

STEP 1

STEP 2

STEP 3

STEP 4

STEP 5

STEP 6

Update or draft AI policies and procedures

- As in the case of the GDPR, compliance is dynamic, not static.
- Ensure AI systems meet requirements of transparency, accuracy and accountability under the EU AI Act by updating data practice procedures and improving existing documentation around use of such systems.
- Deployers (users) of AI systems face obligations to take positive steps around data protection, such as:
    - Adhering to instructions of use and handling personal and sensitive data accordingly;
    - Monitoring operations of the AI system(s) and ensuring data processing activities comply with privacy laws and risks to data subjects are identified and addressed; and
    - Inform the provider and relevant authorities if an AI system is non-conforming.

Update Policies and Procedures

Update or draft AI policies and procedures

- Update existing policies and procedures to reflect requirements of the EU AI Act, particularly those relating to obligations under the GDPR.
- Update existing agreements with customers and clients to reflect requirements and obligations under the EU AI Act.
- Ensure policies reflect EU AI principles of **respect for human autonomy**, **prevention of harm**, **fairness** and **transparency**.
    - This could be published either as a standalone policy or as part of a broader Code of Ethics outlining the development and deployment of AI systems and reflecting obligations under EU AI Act.

Implement AI Training

STEP 1 STEP 2 STEP 3 STEP 4 **STEP 5** STEP 6

Roll out employee training and embed AI awareness in the business

- Develop and roll out a training programme that focuses specifically on the provisions of the EU AI Act, ensuring employees are aware of its implications and the risks of non-compliance.
- Provide levels of training appropriate for employees of varying seniority and experience and be prepared to make changes and updates based on feedback and results.
- Incorporate specific training on AI Ethics into existing training programmes to improve understanding and awareness of both the value of and risks presented by AI systems.
- Work with your AI Governance Committee to maintain training sessions and materials and ensure employees at all levels can identify and mitigate against the latest risks associated with AI systems.
- Take positive steps to foster a culture that promotes the safe, transparent, fair and ethical use of AI systems and encourages the use of AI systems within the framework of approved policies and procedures.

Monitor Legislative Developments

STEP 1

STEP 2

STEP 3

STEP 4

STEP 5

STEP 6

Monitor updates to and interpretations of the EU AI Act and potential UK AI legislation

- Using the EU AI Act timeline of events, ensure you know when its provisions come into operation.
- Review European Court of Justice judgments when cases on the EU AI Act come before it.
- Ensure you are aware of any shift in AI regulation in the UK – the newly elected UK government has suggested legislation will be tabled during this parliament.
- Evaluate and respond to developments in the business over time, including:
  - Geography of operations;
  - Involvement in new AI systems and general-purpose models; and
  - Changes to role in relation to AI systems under EU AI Act (e.g., from importer to distributor).
- Consider whether relevant exceptions to the provisions of the EU AI Act apply to the business as a result of changes to its activities.

Takeaways and Final Considerations

- Dedicated AI Governance Committee
- Inventory of AI systems and models
- Risk classification and mitigation strategies
- Ensure it is possible to fulfil all obligations

Context is Key

- Draft and update policies, procedures and agreements
- AI Literacy: Employee training programmes
- Monitoring changes to legislation and the regulatory landscape
- Reflect on changes to your business and its products

ROPES & GRAY

Boston
Chicago
Dublin
Hong Kong
London
Los Angeles
New York
San Francisco
Seoul
Shanghai
Silicon Valley
Singapore
Tokyo
Washington, D.C.

ropesgray.com