Getting Your Contracts Ready for AI Laws

ANA BRUDER & ARSEN KOURINIAN

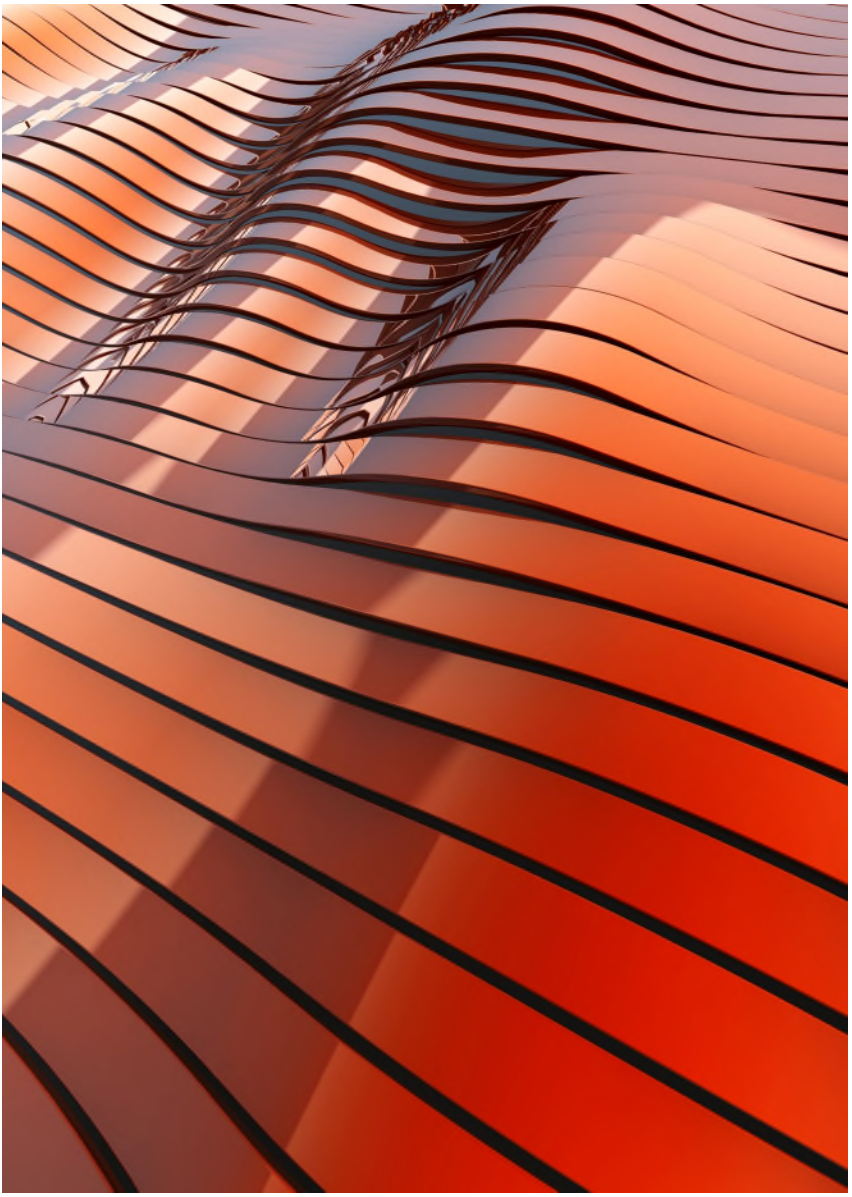
AGENDA

1. Background
2. Evolution of AI laws and changing terms of AI contracts
3. What contract terms may we see based on the AI laws?


BACKGROUND

SECURING AI

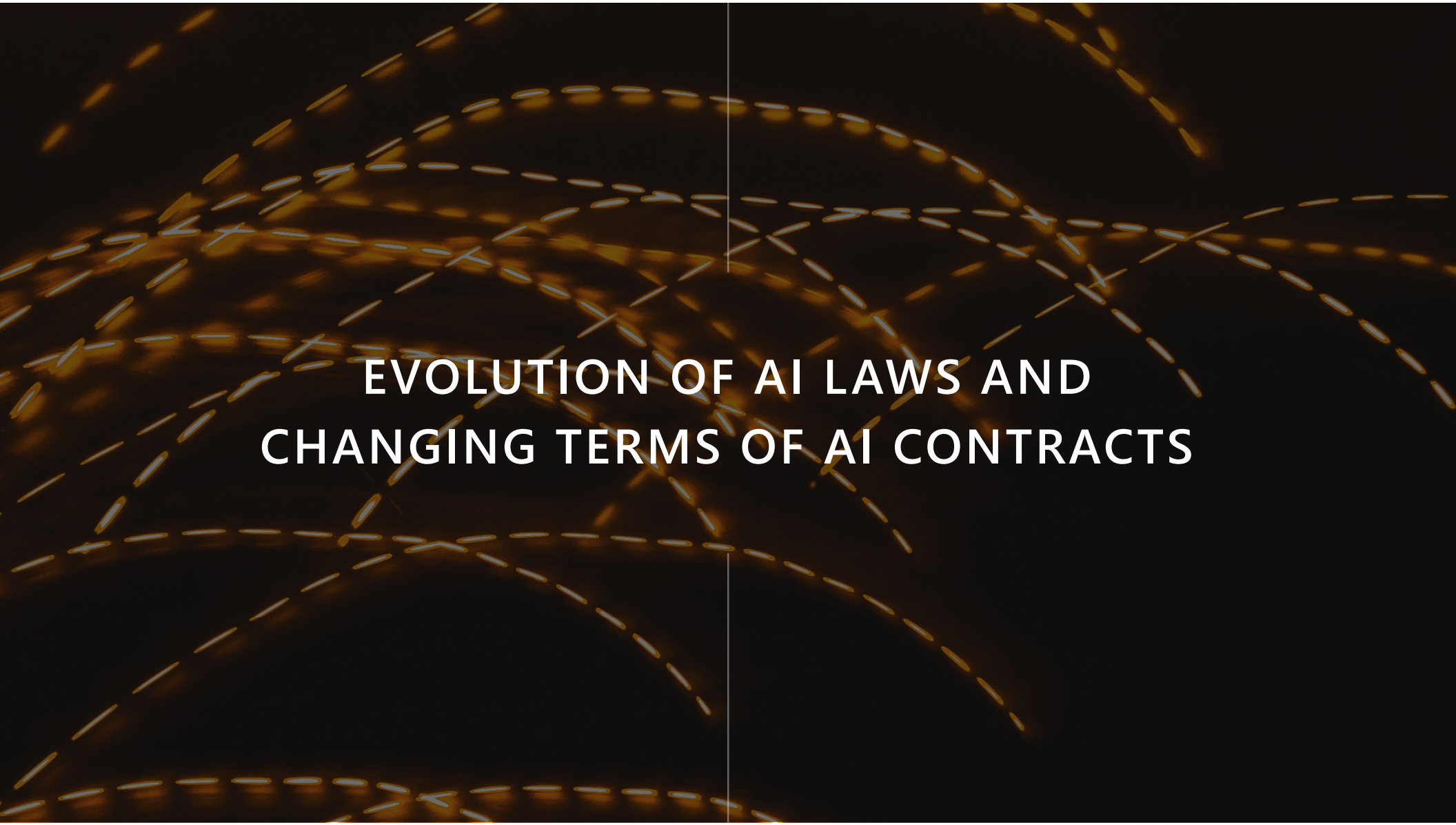
- Increasing leverage of AI in daily operation of companies;
- Ready-made AI systems can be licensed from external providers for functions such as recruitment or document analysis; and
- In-house development is possible, either with independent training of the model or by incorporating foundation models such as GPT.

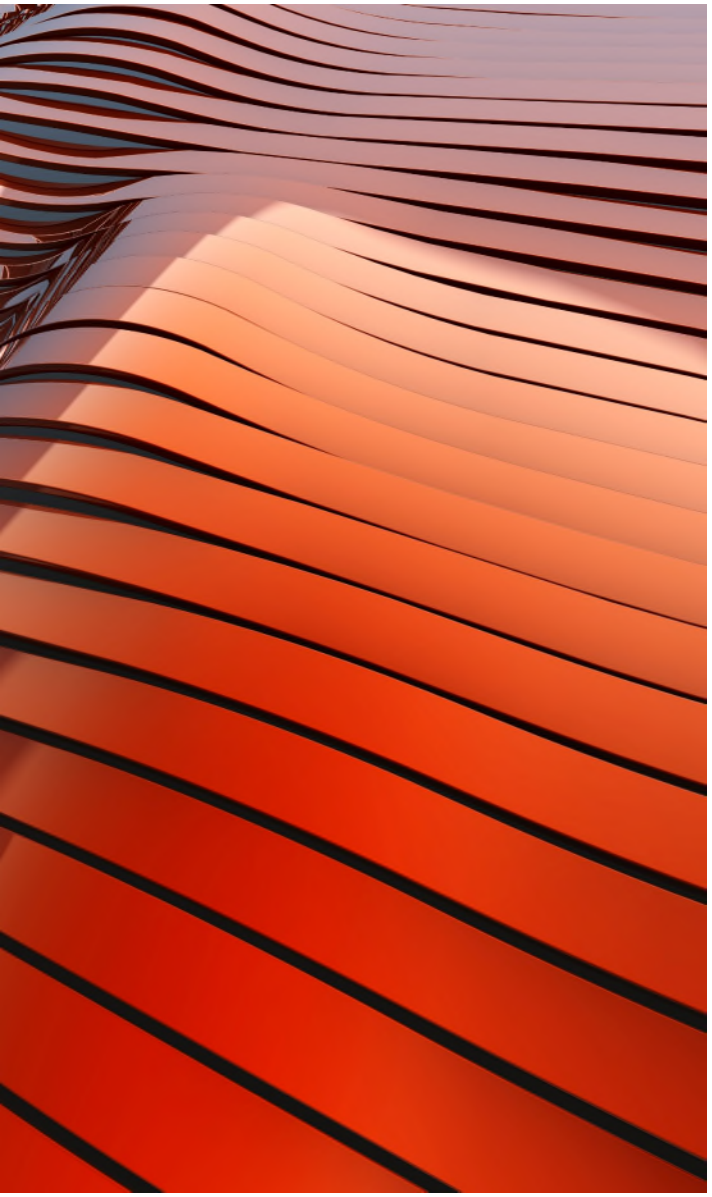


CONTRACTING REQUIREMENTS

- No mandatory provisions imposed on AI contracts – contrast with privacy laws (Article 28 of GDPR; or Section 7051 of CCPA Regulations);
- Minimum expected – mutual representation on compliance with AI laws; and
- Likely to be negotiated – indemnities and exclusions of liability.

  – Note: AI contracts may intersect with other legal areas: personal data protection, use of data, intellectual property.


EVOLUTION OF AI LAWS AND
CHANGING TERMS OF AI CONTRACTS

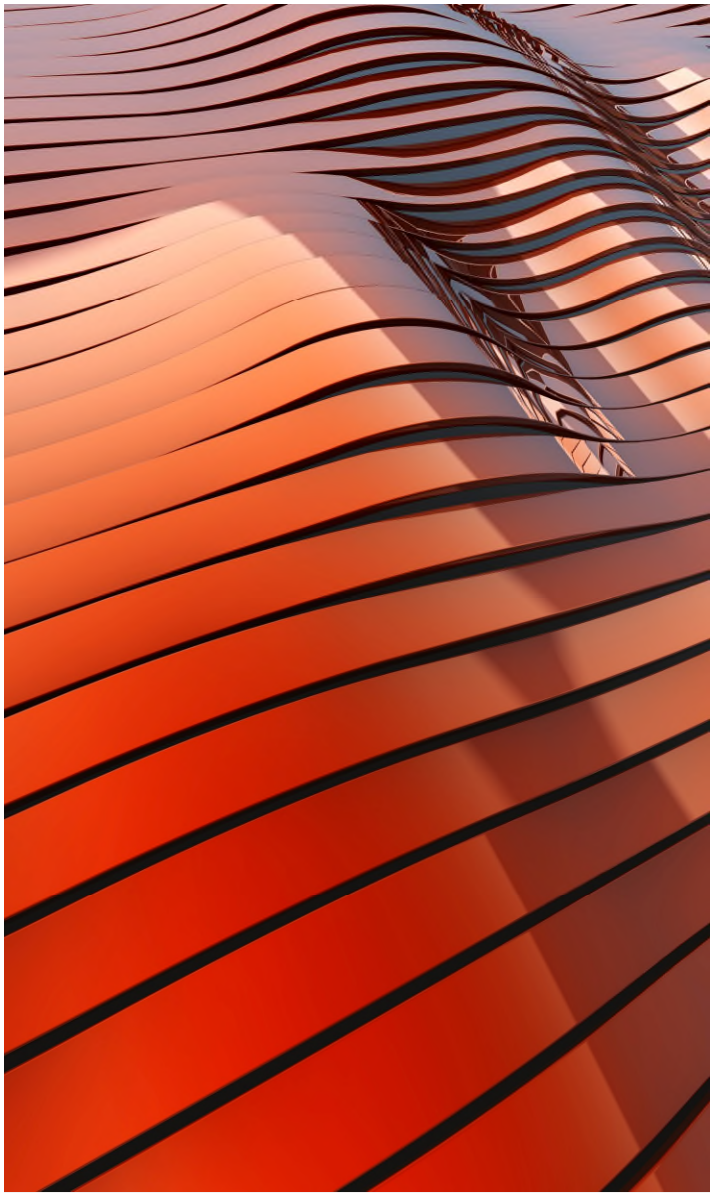


EU AI ACT

- Extraterritorial scope:
  - Applies to public and private bodies;
  - Applies when AI is placed on market or put into service in the EU; or
  - Where the output of the AI system is used in the EU.
- Tiered approach to regulation:
  - Certain use cases are prohibited;
  - Others, classed as “high-risk”, are subject to obligations; and
  - Fewer requirements imposed on limited-risk systems.
- Role of organization is important:
  - Different obligations apply to providers (developers) and deployers (users) of AI; and
  - Duties are also imposed on importers and distributors of AI systems.

COLORADO AI ACT

- Scope:
  - Applies to organizations doing business in Colorado.
- Similar tiered approach:
  - Distinguishes between high-risks and other “low-risk” systems.
- Position of organization still relevant:
  - The Act distinguishes between developers of AI and deployers (users).



PROHIBITED PRACTICES

EU AI Act

Range of AI use cases are banned: manipulative or deceptive systems; social scoring; crime-prediction; untargeted scraping of facial images; and certain applications of biometrics and emotion recognition.

Colorado AI Act

No strictly banned practices; but parties are obliged to avoid "algorithmic discrimination": systems which lead to unlawful discrimination based on specified characteristics.

PENALTIES

EU AI Act

Breaches of the prohibition attract the highest fines up to **EUR 35 million** or **7%** of the undertaking's worldwide turnover.

Colorado AI Act

No tiered penalties; instead, each violation can be treated as a deceptive trade practice – attracting a fine of up to **USD 20,000** per transaction or customer (increased to **USD 50,000** if the customer is over the age of 60).

HIGH-RISK AI SYSTEMS

EU AI Act

The following constitute high-risk uses of AI under the Act:

- As a safety component of certain regulated products, or where the system is itself a regulated product;
- In biometrics;
- As a safety component of critical infrastructure;
- In education and employment;
- To determine access to essential services;
- For law enforcement, migration, or asylum purposes; and
- In administration of justice.

Colorado AI Act

A system which makes (or substantially contributes to) a decision with legal or otherwise significant effects on an individual is deemed a high-risk system.

Specifically refers to areas of:

- Education and employment;
- Healthcare;
- Financial services, including insurance;
- Essential government services;
- Housing; and
- Legal services.

TIMELINES

EU AI Act

- 1 August 2024 – entry into force (but obligations do not apply);
- 2 February 2025 – provisions on prohibited use cases start to apply;
- 2 August 2025 – GPAI rules start to apply;
- 2 August 2026 – high-risk provisions start to apply to systems based on their use case (**Note**: obligations on product manufacturers apply from 2 August 2027).

Colorado AI Act

- 17 May 2024 – signed into law;
- 1 February 2026 – obligations start to apply;
- Colorado Attorney General may release additional regulations;
- Law may be amended, and effective date can be changed.

INFLUENCE OF AI LEGISLATION ON CONTRACTS

No prescribed language

Neither of the statutes imposes mandatory AI terms. However, parties may insist on mapping the legal obligations to terms of the contract.

Some parties may be content with simple general compliance representations; others may include a list of all AI-related compliance issues.

Market's response

Whether parties will actually negotiate remains to be seen. Big AI companies insist on contracting on their standard terms and conditions.

Major AI players are yet to respond to the two pieces of legislation. Given the enforcement timelines, change could be seen within one or two years.


WHAT CONTRACT TERMS MAY WE SEE
BASED ON THE AI LAWS?

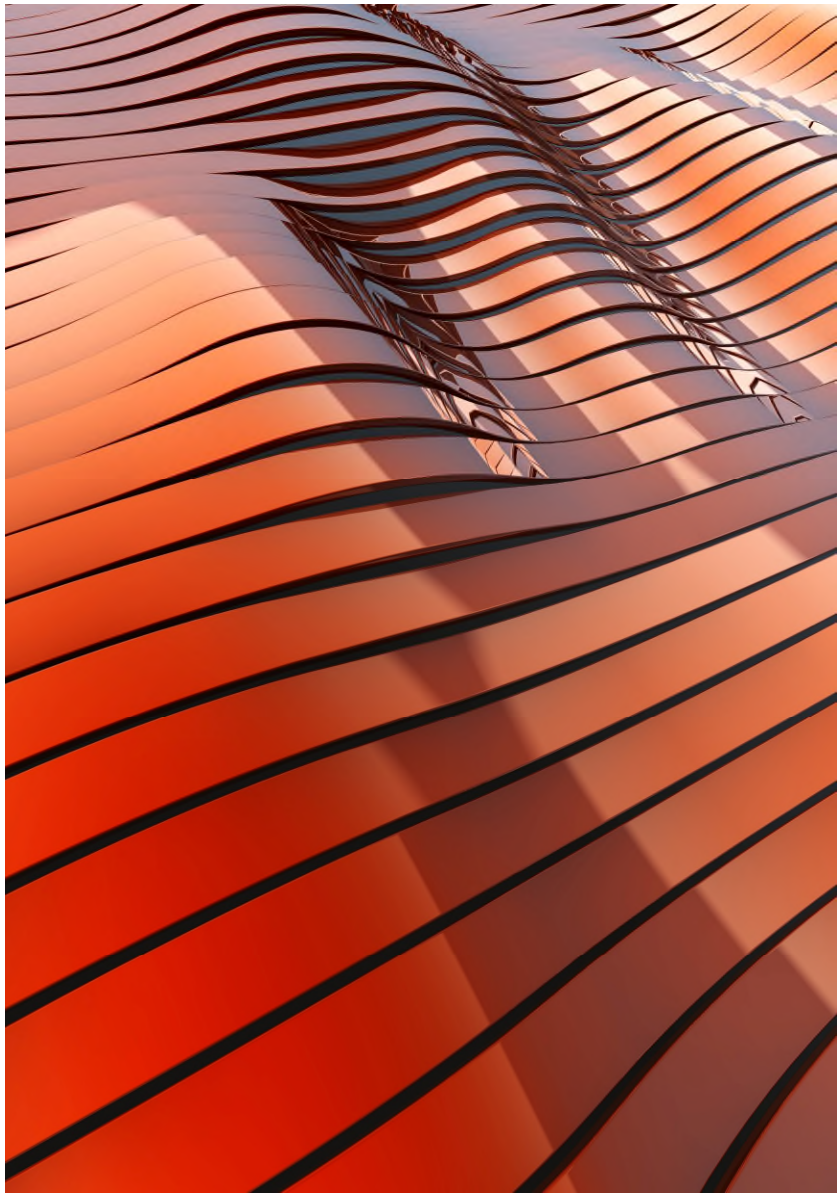
MAKING CHANGES TO THE SYSTEM

Changing the AI system can expose both parties to additional obligations:

- Original deployer – obligations placed on providers apply to the changed system with the deployer presumed to be a provider for that change; and
- Original provider – now obliged to assist and cooperate with the deployer.

The original provider may also suffer reputational risk due to the system being changed.

Contracts will likely specify whether deployers are entitled to make any changes to the AI system.



MUTUAL CLAUSES

Cooperation

The governance provisions may prescribe close cooperation between the parties in the case of:

- A serious incident occurring because of AI use;
- Either party undertaking an impact assessment;
- An individual exercising their rights;
- An investigation; and
- Participation in post-market monitoring.

Risk Management System (RMS)

The EU AI Act requires providers (developers) to implement a risk management system. The Colorado Act places this obligation expressly on deployers, but implicitly required for developers.

Risk management may become a mutual obligation of the parties; alternatively, diligence of the same will become an important precondition for the procurement.

PARTY-SPECIFIC CLAUSES

Providers (developers) will seek to:

- Ensure that the deployer fulfils their transparency obligations to its customers;
- Oblige the deployer to follow the instructions for use;
- Receive a warranty that the deployer has the right to use the input data and that it is appropriate; and
- Place an obligation on the deployer to honor AI-related rights of individuals (regarding decision-making).

Deployers (users) will seek to:

- Ensure the system satisfies technical requirements under the law;
- Include a representation that the system was developed with appropriate data governance techniques;
- Ensure that the provider had the right to use the training data;
- Receive certainty as to accuracy of the instructions they receive;
- Receive warranties as to the accuracy, robustness, and security of the system; and
- Require that interactive systems are transparent to users.


QUESTIONS?