MAYER | BROWN

ARTIFICIAL INTELLIGENCE PROVISIONS IN TECHNOLOGY CONTRACTING:

KEEPING UP WITH THE EVOLVING REGULATORY LANDSCAPE

SPEAKERS

ANA
BRUDER

FRANKFURT

ARSEN
KOURINIAN

LOS ANGELES

OLIVER
YAROS

LONDON

AGENDA

1. Overview of major AI regulations
2. Converting the AI regulations to contract terms

01

OVERVIEW OF AI REGULATIONS

DOMESTIC AND GLOBAL AI LAWS

Comprehensive AI Laws

- EU AI Act
- Colorado's Concerning Consumer Protections in Interactions with AI ("Colorado AI Law")
- South Korea's Artificial Intelligence Development and Establishment of a Foundation for Trustworthiness

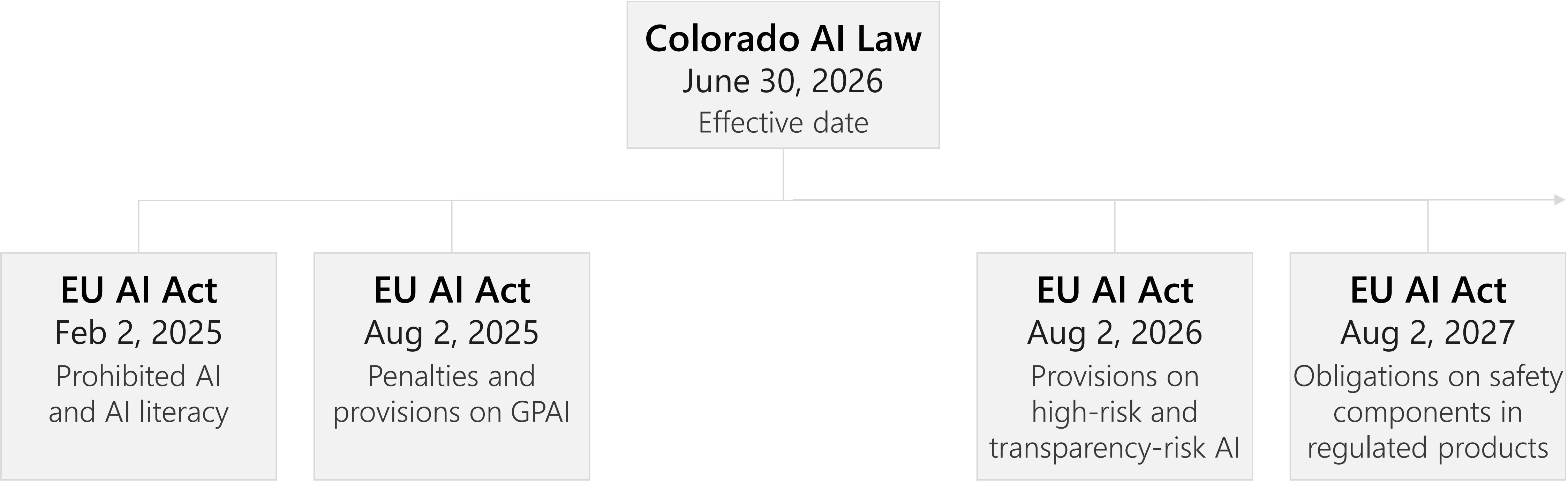
Narrower AI Laws in the US

- Texas Responsible AI Governance Act (prohibited practices)
- Utah Artificial Intelligence Policy Act (transparency)
- Illinois AI law amending Human Rights Act (transparency and avoiding discrimination)
- Illinois AI Video Interview Act (transparency and consent)
- New York City Local Law 144 (transparency and bias audit)
- California Generative AI: Training Data Transparency (AB2013) (transparency regarding training data)
- California AI Transparency Act (SB942) (AI detection tool and manifest and latent disclosures on AI-generated content)
- California AI in Healthcare Services (AB3030) (transparency regarding communication generated by AI)
- Chatbot Laws (transparency)

Interaction with Existing Laws

- Data privacy law considerations (state Attorneys' General and California Privacy Protection Agency)
- Employment laws (Equal Employment Opportunity Commission)
- Unfair and deceptive practices (Federal Trade Commission)
- Explaining credit decisions following adverse action (Consumer Financial Protection Bureau)

TIMELINE FOR EU AI ACT AND COLORADO AI LAW



Colorado AI Law
June 30, 2026
Effective date

EU AI Act
Feb 2, 2025
Prohibited AI and AI literacy

EU AI Act
Aug 2, 2025
Penalties and provisions on GPAI

EU AI Act
Aug 2, 2026
Provisions on high-risk and transparency-risk AI

EU AI Act
Aug 2, 2027
Obligations on safety components in regulated products

PLAYERS IN THE ECOSYSTEM AND JURISDICTION

EU AI ACT

Role	Provider	Deployer	Product Manufacturer	Importer	Distributor
Definition	Develops an AI system or GPAI model and places it on or puts into service in the EU under its own name or trademark	Uses an AI system (excluding personal non-professional use)	Manufactures a product under its own name or trademark that incorporates an AI system into product design	First makes a non-EU company's AI system available in the EU	Makes an AI system available in the EU (not otherwise a provider or importer)
Jurisdiction	Placing on the market or putting into service in the EU *or* Output of an AI system used in the EU	Established or located in the EU *or* Output of an AI system used in the EU	Placing on the market or putting into service an AI system together with their product	Initially putting a provider's AI system into service in the EU	Making provider's AI system available in the EU

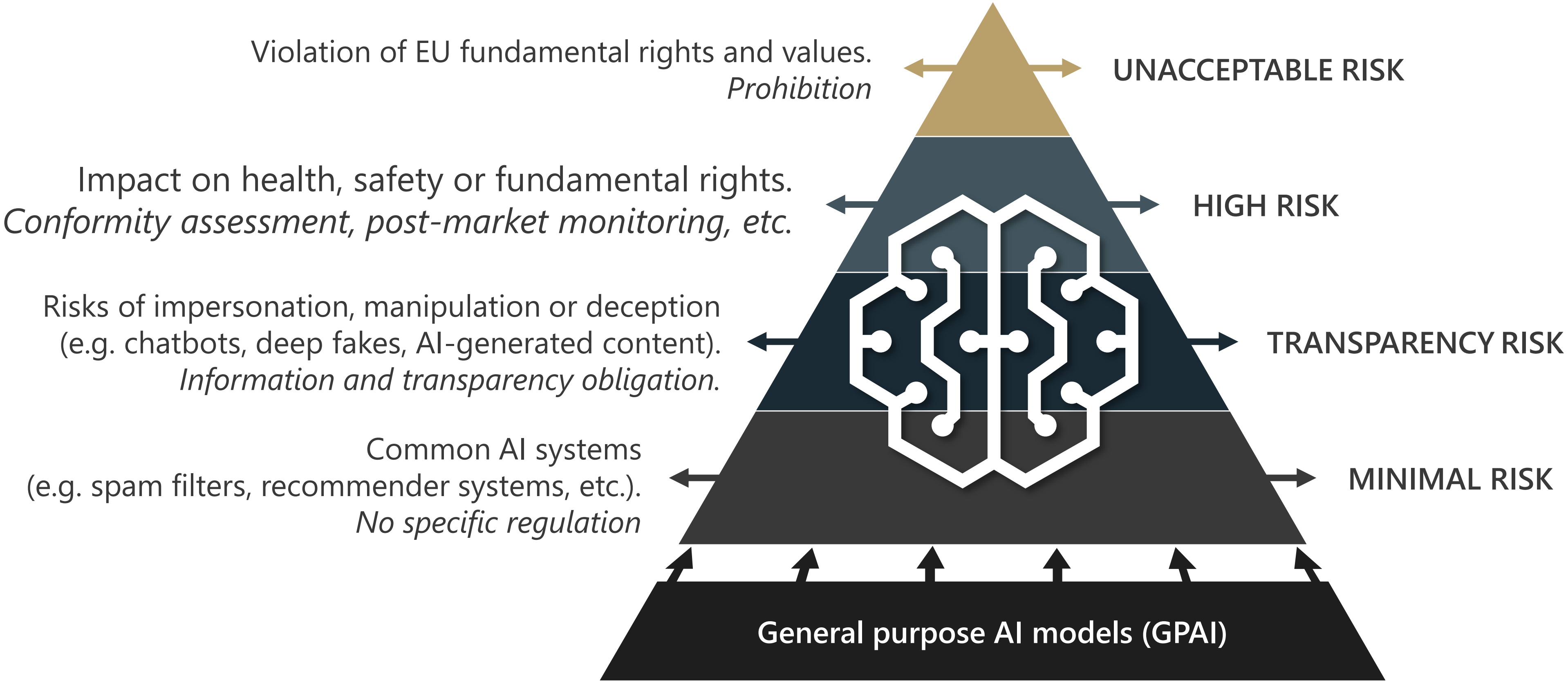
Consider Article 25

Transforming into a provider if you: (1) put your name or trademark on high-risk AI system; (2) make substantial modifications (change not foreseen or planned in conformity assessment); or (3) modify the intended purpose of AI system such that it becomes a high-risk AI system.

COLORADO AI LAW

Deployer	Developer
Uses an AI system	Develops or intentionally and substantially modifies an AI system
Conducting business in Colorado	Conducting business in Colorado

EU AI ACT: TIERED APPROACH



UNACCEPTABLE RISK

Violation of EU fundamental rights and values.
Prohibition

HIGH RISK

Impact on health, safety or fundamental rights.
Conformity assessment, post-market monitoring, etc.

TRANSPARENCY RISK

Risks of impersonation, manipulation or deception
(e.g. chatbots, deep fakes, AI-generated content).
Information and transparency obligation.

MINIMAL RISK

Common AI systems
(e.g. spam filters, recommender systems, etc.).
No specific regulation

General purpose AI models (GPAI)

GPAI models – *Transparency requirements*
GPAI with systemic risks – *Transparency requirements, risk assessment and mitigation*

Data source: https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf

UNACCEPTABLE RISK / PROHIBITED AI SYSTEMS

EU AI ACT	COLORADO AI LAW
Use **subliminal, manipulative or deceptive techniques** to distort a behavior/decision	Reasonable care to avoid **algorithmic discrimination**
Exploit vulnerabilities like age, disability, social or economic situation to distort behavior	
Classify individuals based on social behavior or personal characteristics (**social scoring**) leading to detrimental or unfavorable treatment that is out of context or disproportionate	
Make risk assessments of individuals to assess or predict the risk of them committing a crime (**predictive policing**)	
Untargeted scraping of the internet or CCTV for **facial images** to build or expand facial recognition databases	
Inferring emotions in the workplace and educational institutions, unless for medical or safety reasons	
Biometric categorization systems based on biometric data (like facial images or fingerprints) to deduce or infer individuals’ race, political opinions, trade union membership, religious or philosophical beliefs, or sexual orientation	
Real-time biometric identification system in publicly accessible spaces **by law enforcement**, subject to narrow exceptions	

HIGH-RISK AI SYSTEMS

EU AI ACT	COLORADO AI LAW
Education and vocational training	Education enrollment or an education opportunity
Employment, worker’s management and recruitment	Employment or employment opportunity
Essential public and private goods, services, and benefits • Evaluate the creditworthiness of natural persons or establish their credit score; • Life and health insurance	A financial or lending service, insurance, health-care service, essential government service
Law enforcement, administration of justice and democratic processes	Legal services
Immigration and border control	Housing
Biometrics	
Safety component in regulated products	
Safety components in critical infrastructure (e.g., digital infrastructure, road traffic, or in the supply of water, gas, heating or electricity	

ROLE-SPECIFIC OBLIGATIONS: EU AI ACT (1) – HIGH RISK

PROVIDER	DEPLOYER
Risk management system	Follow instructions of use
Data governance	Human oversight
Maintain technical documentation and logs	Relevant and representative input data
Transparency and instructions of use to deployer	Monitoring and notice of serious incidents
Ensure accuracy, robustness, cybersecurity, and accessibility	Maintain autogenerated logs
Quality management system and declaration of conformity	Impact assessments
Human oversight	Transparency
Name, trademark, CE marking, and registration	Honor data subject rights, including automated decisions

ROLE-SPECIFIC OBLIGATIONS: EU AI ACT (2) – HIGH RISK

IMPORTER	DISTRIBUTOR
Verification of conformity assessment, technical documentation, CE marking and appointment of provider's authorized representative	Verification of CE marking and compliance with provider's / importer's obligations
Flagging non-conformity	Flagging non-conformity and withdraw, recall, or provider / importer takes corrective actions
Not jeopardize compliance with high-risk requirements while under their responsibility, storage or transport	Not jeopardize compliance with high-risk requirements while under their responsibility, storage or transport
Provision of information and cooperation with authorities	Provision of information and cooperation with authorities
Contact details	
Record keeping	

ROLE-SPECIFIC OBLIGATIONS: EU AI ACT (3) – TRANSPARENCY RISK

PROVIDER	DEPLOYER
Transparency about user interaction with an AI system	Transparency about using emotion recognition or biometric categorization systems
Marking synthetic audio, image, video or text as such	Transparency about deep fake image, audio or video content
	Transparency about artificially generated or manipulated text published with the purpose of informing the public on matters of public interest

ROLE-SPECIFIC OBLIGATIONS: EU AI ACT (4) – GPAI

ALL GPAI PROVIDERS	PROVIDERS OF GPAI WITH SYSTEMIC RISK
Technical documentation	Model evaluation, including adversarial testing
Information and documentation for downstream providers	Assessment and mitigation of systemic risks
Policy for compliance with EU copyright law	Documentation and reporting of serious incidents
Public summary of the content used for training	Adequate level of cybersecurity
Cooperation with authorities	
Appointment of authorized representative if established outside the EU	

ROLE-SPECIFIC OBLIGATIONS: COLORADO AI LAW

DEVELOPER	DEPLOYER
Information to deployer regarding uses, benefits, harms, limitations, summary of training data, risk of discrimination, evaluation steps taken, mitigation, intended output, and how the AI system will be monitored	AI impact assessment
Statement on website about the types of AI systems available and how risks are managed	Risk management policy (e.g., NIST AI RMF & ISO/IEC 42001)
Reporting within 90 days to CO AG and deployer if discovers AI system caused or reasonably likely to cause algorithmic discrimination or receives credible report from deployer that algorithmic discrimination caused	Annual review of AI system to ensure no algorithmic discrimination
	Notice to Colorado residents regarding deployment, including that a high-risk AI system deployed for consequential decision, purpose and nature of decision and description of AI, instructions on how to access website statement, right to opt out and contact
	Challenge adverse decisions
	Website statement about the type of AI systems deployed, how risks are managed, and nature, source and extent of information collected and used
	Disclose to CO AG within 90 days if AI system caused algorithmic discrimination

TEXAS RESPONSIBLE AI GOVERNANCE ACT (TEXAS AI ACT)

- **Who does it apply to?**
  - The Texas AI Act applies to any person who: (1) promotes, advertises, or conducts business in Texas; (2) produces a product or service used by Texas residents; or (3) develops or deploys an AI system in Texas. The law also contains provisions that apply to Texas government agencies.
- **Prohibited practices (private entities)**

  1. <u>Manipulation of human behavior</u>: It is prohibited to develop or deploy an AI system with the intent to incite or encourage a person to: (a) commit physical self-harm, including suicide; (b) harm another person; or (c) engage in criminal activity.
  2. <u>Constitutional protection</u>: It is prohibited to develop or deploy an AI system with the sole intent for the AI system to infringe, restrict, or otherwise impair an individual's rights guaranteed under the United States Constitution.
  3. <u>Unlawful discrimination</u>: It is prohibited to develop or deploy an AI system with the intent to unlawfully discriminate against a protected class in violation of state or federal law. The law notes, however, that a disparate impact is not sufficient by itself to demonstrate an intent to discriminate. Insurance entities and federally insured financial institutions are exempt from this prohibition.
  4. <u>Certain sexually explicit content and child pornography</u>: It is prohibited to develop or distribute an AI system with the sole intent of producing, assisting or aiding in producing, or distributing unlawful visual material or deep fake videos or images. It is also prohibited to develop or distribute an AI system that engages in text-based conversations that simulate or describe sexual conduct, while impersonating or imitating a child under 18.

CALIFORNIA GENERATIVE AI: TRAINING DATA TRANSPARENCY

- Effective January 1, 2026
- Developers of AI systems (or those that substantially modify it, e.g., finetuning or retraining) must provide a high-level summary on their website about the training data used to train the generative AI system.
- This law emphasizes the importance of maintaining a data provenance record.

CALIFORNIA GENERATIVE AI: TRAINING DATA TRANSPARENCY

- Effective January 1, 2026
- Developers of generative AI systems that are made publicly accessible and have over 1 million monthly visitors and users need to:
  - (1) make available an AI detection tool at no cost to the user;
  - (2) offer the user the option to include a manifest disclosure in image, video, or audio content clearly identifying the content as AI-generated; and
  - (3) include a latent disclosure in AI-generated image, video, or audio content.

02

CONVERTING THE AI REGULATIONS TO CONTRACT TERMS

CONTRACTUAL ISSUES TO CONSIDER

- **What are my AI use cases?**
  - High-risk AI use cases should incorporate more robust contract terms that address party-role obligations in a commercially reasonable way in the contract.
  - The parties should consider a contractual provision stating that neither party will engage in prohibited practices.
- **Level of granularity**
  - Consider taking a balanced approach with the contract terms that are mapping to AI regulatory requirements.
  - Neither party will be able to address word-to-word each AI regulatory provisions/subparts in a contract.
  - The issues can be addressed with a provision requiring the parties to comply with AI regulations, but also expressly addressing important topics, such as risk management, human oversight, continuous monitoring, transparency, instructions of use, data issues, safety and security, etc.
- **Only requiring compliance with AI rep is not enough**
  - If the AI system is deployed or developed for use cases that do not trigger major AI laws, you will have no contractual protections.
  - There still remains the concern about use of data to train AI models, which should be covered in the contract even without a legal requirement.
  - Even low-risk use cases (e.g., chatbots) can have practical high-risk impact (e.g., chatbot tarnishing company brand, mistreating customers, etc.)
- **Future proofing and being geographically agnostic**
  - Avoid contract terms drafted to just address one law.
  - Naming specific laws may limit the scope of the terms and include detailed provisions that don’t apply in every scenario.
  - AI laws are also rapidly developing, which is why definitions and concepts should be broadly addressed as commercial terms, instead of legal compliance obligations.
  - However, if both parties are aligned on applicability of major AI laws, there might be flexibility in including specific references.

CONTRACTUAL ISSUES TO CONSIDER

- **Party Leverage**
  - Major LLM providers have their own online terms and unlikely to accept adhoc terms. However, discuss with them whether they have template provisions for particular use cases.
- **Market reaction**
  - AI terms are no longer a foreign concept to companies.
  - Small-to-mid-size companies use AI terms when outsourcing, and parties appear to understand the need for these terms.
  - Common terms we have seen have evolved since 2022 when companies were initially focused on use of data concerns but now understand that risk mitigation measures are also necessary in contracts.
  - Start off broad but scale back depending on your AI use case during negotiations.
- **Incorporation by reference**
  - Consider drafting an AI policy that applies to suppliers and incorporating by reference into the agreement.
  - Another approach is to have a template AI addendum with your preferred terms based on party-role (situations where you are a developer v. deployer).
- **Downstream LLMs**
  - Some AI system providers are not training an AI model. Instead, they are incorporating a major LLM.
  - Consider conducting diligence on the underlying LLMs that they use based on available online terms.

EU AI ACT TERMS

- **Article 25(2) of the EU AI Act**
  - *"Where the circumstances referred to in paragraph 1 occur* [**white-labelling, substantial modification or change of purpose**]*, the **provider** that initially placed the AI system on the market or put it into service shall no longer be considered to be a provider of that specific AI system for the purposes of this Regulation. That **initial provider shall closely cooperate with new providers** and shall **make available the necessary information** and **provide** the reasonably expected **technical access** and other **assistance** that are required for the fulfilment of the obligations set out in this Regulation, in particular regarding the compliance with the conformity assessment of high-risk AI systems. This paragraph shall not apply in cases where the initial provider has clearly specified that its AI system is not to be changed into a high-risk AI system and therefore does not fall under the obligation to hand over the documentation."*

- **Template contractual term (Company is the new provider)**
  - *4.2.2 To the extent that Supplier's AI Solutions constitute an AI system and Company is considered the provider of a high-risk AI system under Article 25(1) of the EU AI Act, Supplier shall closely cooperate with Company and shall, without undue delay and at Supplier's expense, make available the necessary information and provide the reasonably expected technical access and other assistance that are required for the fulfilment of the obligations set out in the EU AI Act, in particular, without limitation, regarding compliance with the conformity assessment of high-risk AI systems*

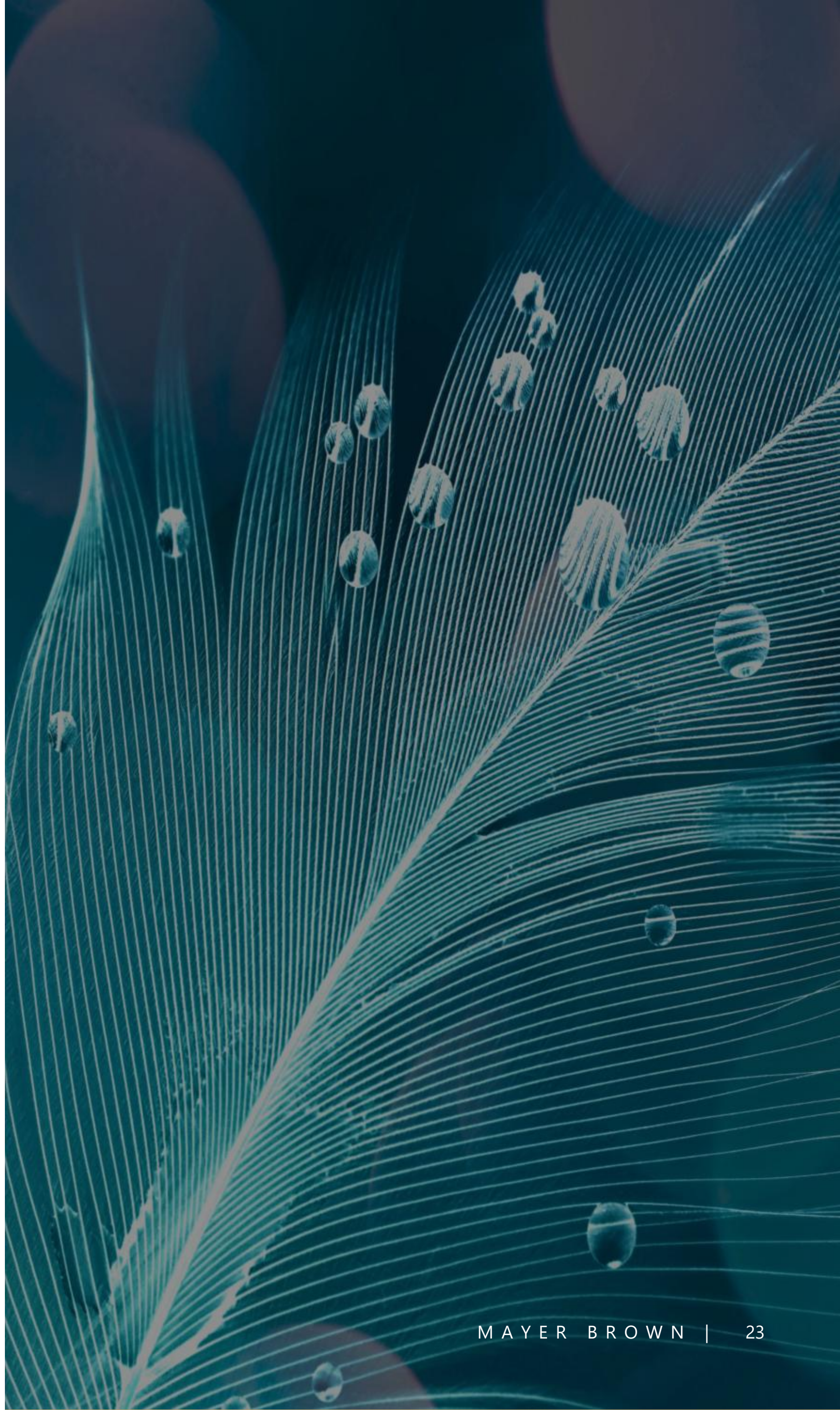
EU AI ACT TERMS (CONTINUED)

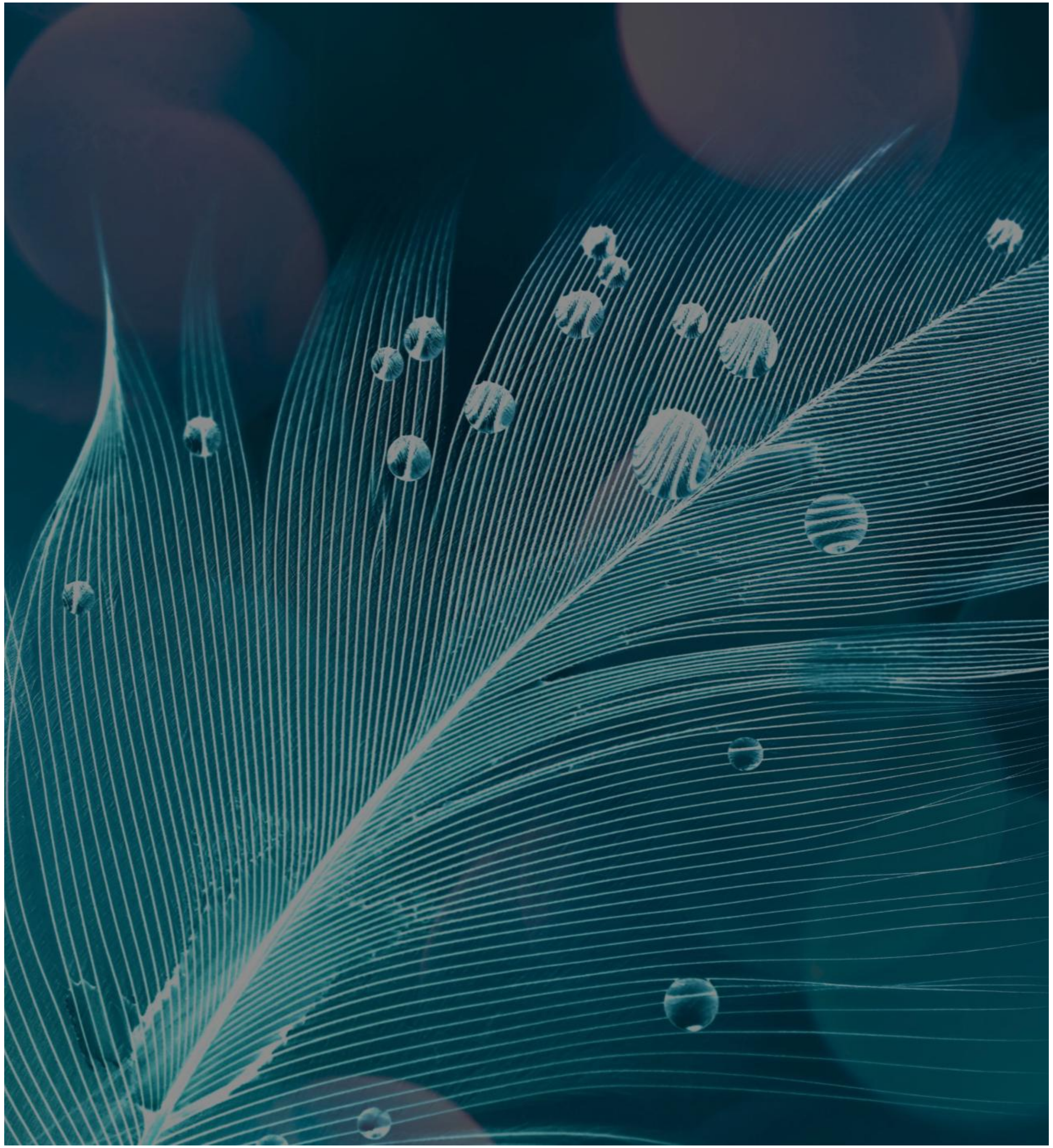
- **Article 25(4) of the EU AI Act**
  - *"The **provider of a high-risk AI system** and the **third party** that **supplies an AI system, tools, services, components, or processes** that are used or integrated in a high-risk AI system **shall, by written agreement**, specify the **necessary information, capabilities, technical access** and **other assistance** based on the generally acknowledged state of the art, in order to enable the provider of the high-risk AI system to fully comply with the obligations set out in this Regulation. This paragraph shall not apply to third parties making accessible to the public tools, services, processes, or components, other than general-purpose AI models, under a free and open-source license."*

- **Template contractual term (Company is a provider of a high-risk AI system integrating a component from Supplier, e.g., an LLM model)**
  - *4.2.1 To the extent that Supplier's AI Solutions constitute an AI system, tool, service, component and/or process that is used or integrated into a high-risk AI system of which Company is the provider under the EU AI Act, Supplier agrees to provide the following information and documentation to Company at Supplier's expense:*
- *(…)*
  - Advisable to reflect in the contract the specific information and documentation needed for the Company as high-risk AI system provider to comply with its EU AI Act obligations (e.g., technical documentation reflecting Annexes of the EU AI Act).

MANDATORY TERMS - CALIFORNIA

- **California AI Transparency Act**
  - Removal of latent disclosures prohibited
    - *"(c) (1) If a covered provider licenses its GenAI system to a third party, the covered provider **shall require by contract** that the licensee maintain the system's capability to include a disclosure required by subdivision (b) in content the system creates or alters.*
    - *(2) If a covered provider knows that a third-party licensee modified a licensed GenAI system such that it is no longer capable of including a disclosure required by subdivision (b) in content the system creates or alters, the covered provider shall revoke the license within 96 hours of discovering the licensee's action.*
    - *(3) A third-party licensee shall cease using a licensed GenAI system after the license for the system has been revoked by the covered provider pursuant to paragraph (2)."*





QUESTIONS?

CONFIDENTIAL