KIRTON | McCONKIE

H1 2026: The Critical Window for AI Regulatory Compliance

Peter Shiozawa




KIRTON | McCONKIE

AGENDA

I. The AI Regulatory Landscape

- AI Experimentation → AI Accountability
- The EU AI Act
- US Developments
- Global Trends

II. Highest ROI Implementations to comply with EU AI Act

- What "High Risk" Means in Practice
- Where Companies are Most Exposed
- The Moving Goalposts of the EU AI Act
- Operational Playbook

KIRTON | McCONKIE

Section I: The AI Regulatory Landscape

The Game is Changing with AI

- The early years of large language models and diffusion models (2022-2024) were characterized by high excitement and rapid innovation
  - Look no further than "Will Smith Eating Spaghetti"
- The recent Grok uproar is emblematic of the dour public attitude that has emerged around AI
- Most voters (57%) believe AI's risks outweigh its benefits
- Regulations started passing in 2024
- Just in 2026 there have been 1,500+ AI laws proposed

The Game is Changing with AI

The EU AI Act: the first comprehensive AI regulatory regime (1/4)

- **What is it?**
  - The first comprehensive AI law (risk-based framework)
  - Applies beyond the EU (extraterritorial reach)
- **How does it impact you?**
  - Covers companies placing AI into the EU market or **affecting** EU users (extraterritorial reach)
  - Obligations attach to use cases, not just developers
- **What does it regulate?**
  - Prohibited AI (e.g., social scoring)
  - High-risk systems (HR, credit, healthcare, etc.)
  - General-purpose AI (GPAI) obligations
- **What's next?**
  - Phased enforcement already underway
  - Key obligations hitting in 2026–2027

If your company uses AI in decisions affecting people, the EU AI Act likely applies

The EU AI Act: the first comprehensive AI regulatory regime (2/4)

- **Why should you care?**
  - Significant financial penalties: up to **€35M or 7% of global annual turnover** (whichever is higher) for prohibited practices
  - Up to **€15M or 3% of global annual turnover** (whichever is higher) for high-risk practices or transparency failures
- **Regulators decide compliance**
  - National supervisory authorities in each EU member state
  - Coordinated through the **European AI Board**
- **Enforcement can be triggered externally**
  - Complaints from individuals
  - Competitor challenges
  - Regulatory investigations

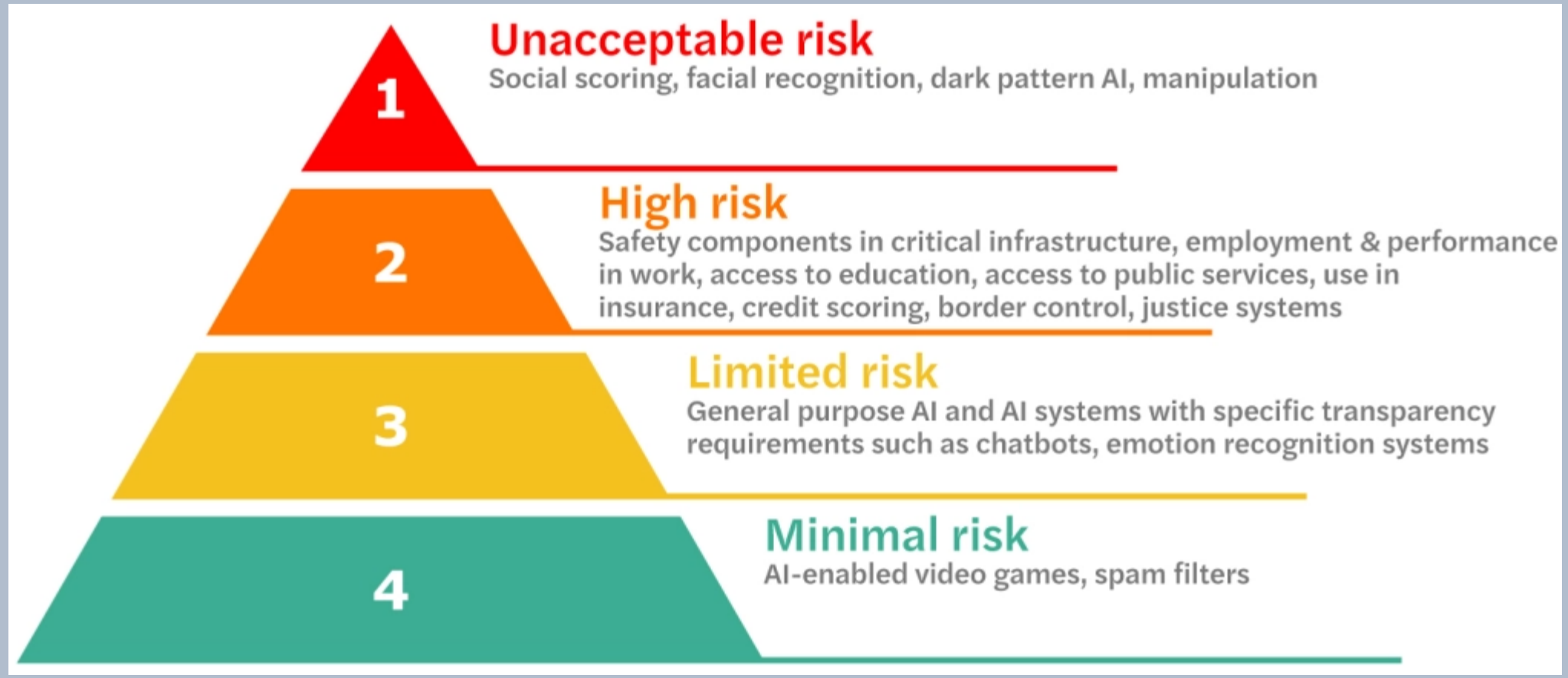
If your company uses AI in decisions affecting people, the EU AI Act likely applies

The EU AI Act: the first comprehensive AI regulatory regime (3/4)

- **How the EU AI Act affects your business**
  - HR and employment decisions
    - Hiring, screening, performance evaluation, terminations
  - Customer-facing decisions
    - Credit, pricing, eligibility, personalization
  - Internal enterprise tools
    - Productivity AI, copilots, knowledge systems (often overlooked but still in scope)
  - Third-party AI vendors
    - You may still be the "deployer" under the Act
  - Marketing & AI claims
    - Representations about AI capabilities

This is not about whether you build the AI—it's about whether you use it

The EU AI Act: the first comprehensive AI regulatory regime (4/4)

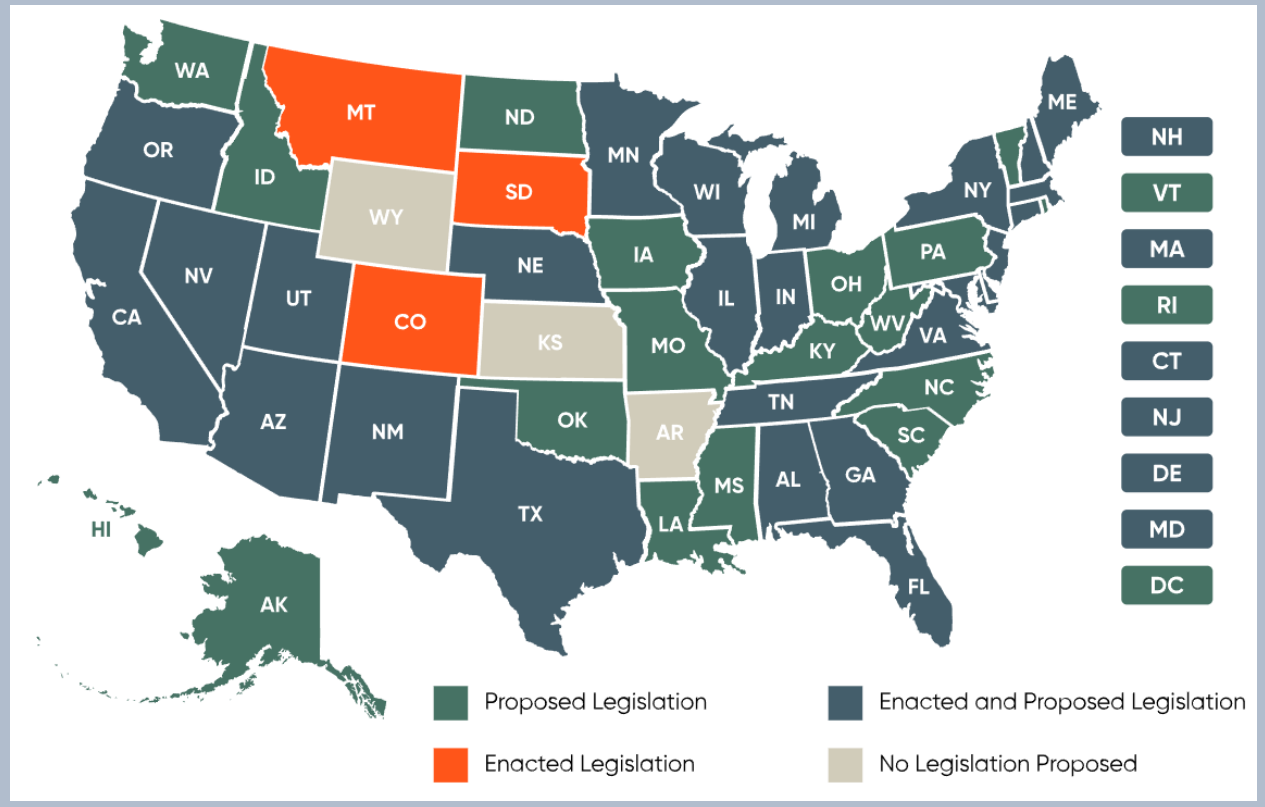


The EU AI Act introduces a risk-based framework with different obligations and penalties indexed to the risk category and the organization's role (e.g. "provider" vs. "deployer")

US AI Regulatory Developments

- Like privacy, no federal AI law exists (yet)
- Patchwork of state laws has cropped up in its stead
  - California, Colorado, and Utah are the leaders in this space, but more are popping up all the time
  - Colorado AI Act (2024)
  - California (CPRA, ADMT regulations)
  - Utah (professional licensure, deepfakes)
- Regulators are already active:
  - FTC, CFPB, EEOC, State AGs

If your use of AI affects people, regulators are paying attention



Colorado AI Act

- **Applies to "high-risk" AI systems**
  - Systems that make or substantially influence decisions about individuals (e.g., employment, credit, housing, insurance)
- **Creates a "duty of care"**
  - Companies must take reasonable steps to prevent algorithmic discrimination
- **Applies to deployers—not just developers**
  - If you *use* the system, you have obligations
- **Requires governance + documentation**
  - Risk management policies
  - Impact/risk assessments
  - Ongoing monitoring
- **Transparency obligations**
  - Disclosures to consumers in certain use cases

Global AI Regulatory Trends

- **Risk-based frameworks are becoming standard**
  - Focus on **high-impact use cases**, not all AI
- **Regulation targets use—not just development**
  - "Deployers" (companies using AI) are in scope globally
- **Accountability is shifting to documentation**
  - "Show your work" → risk assessments, testing, monitoring
- **Bias and fairness are central concerns**
  - Discrimination risk is a primary enforcement driver
- **Transparency expectations are rising**
  - Disclosures to users and regulators
- **Enforcement is becoming real**
  - Fines, audits, and investigations—not just guidance

"As goes Europe, so goes the world." Complying with EU AI Act positions you for most global requirements

KIRTON | McCONKIE

Section II: The Highest ROI Implementations to Comply with the EU AI Act

What "high risk" means in practice

- The enforcement of most AI laws hinges on this definition
- EU AI Act includes the following in its definition of "high risk AI systems"
  - Biometrics (e.g., facial recognition)
  - Critical infrastructure (energy, transport, utilities)
  - Education and training
  - Employment and HR decisions
  - Access to essential services (e.g., credit scoring)
  - Law enforcement
  - Migration, asylum, border control
  - Justice and democratic processes

Many everyday AI tools can qualify as "high risk" AI systems!

What you actually have to do for high-risk AI systems (operational burden)

- Risk assessments before deployment
- Documented use + intended purpose
- Human oversight requirements
- Ongoing monitoring & incident reporting
- Data governance expectations

More like product compliance than IT policy

The hidden trap: vendor-supplied AI

- Using a vendor ≠ outsourcing liability
- You may still be the “deployer”
- Key gaps:
  - No visibility into model behavior
  - Weak contractual protections
  - No audit rights

If your vendor breaks the law, you’re still exposed

Enforcement date for high-risk AI

- Originally slated for August 2, 2026

- Amendments being advanced by EU lawmakers may delay this to December 2027 ***at the latest***

- The enforcement date depends on the resources that the EU is preparing, including standards and codes of practice
    - European Commission may choose to enforce high-risk rules as soon as the resources are ready
    - No indication of when they will be ready

Far from being a relief, this delay <u>increases uncertainty</u> and makes planning ahead more difficult

Risk Classification and Compliance

- All AI use cases should be reviewed to ascertain any potential obligations under AI laws
  - Identify the AI system and its inputs and outputs
  - Assess impact on individuals
    - Does it affect employment, access to credit, housing, healthcare, legal or financial outcomes, education, or use biometric data?
  - Determine level of influence
    - Automated decision, decision support, or low impact?
  - Map to risk tier
    - EU AI Act high-risk categories vs. “limited risk” (transparency obligations) vs. “minimal risk”
  - Apply controls accordingly
    - High risk: Full governance + documentation
    - Transparency obligations: user disclosure
    - Minimal risk: internal documentation

Risk Classification Hypothetical

- Your company uses a third-party AI tool to screen resumes
  - Which laws apply?
  - Is it a high-risk use?
  - What obligations apply?
  - Where does liability sit?

KIRTON | McCONKIE

Additional AI Governance Recommendations

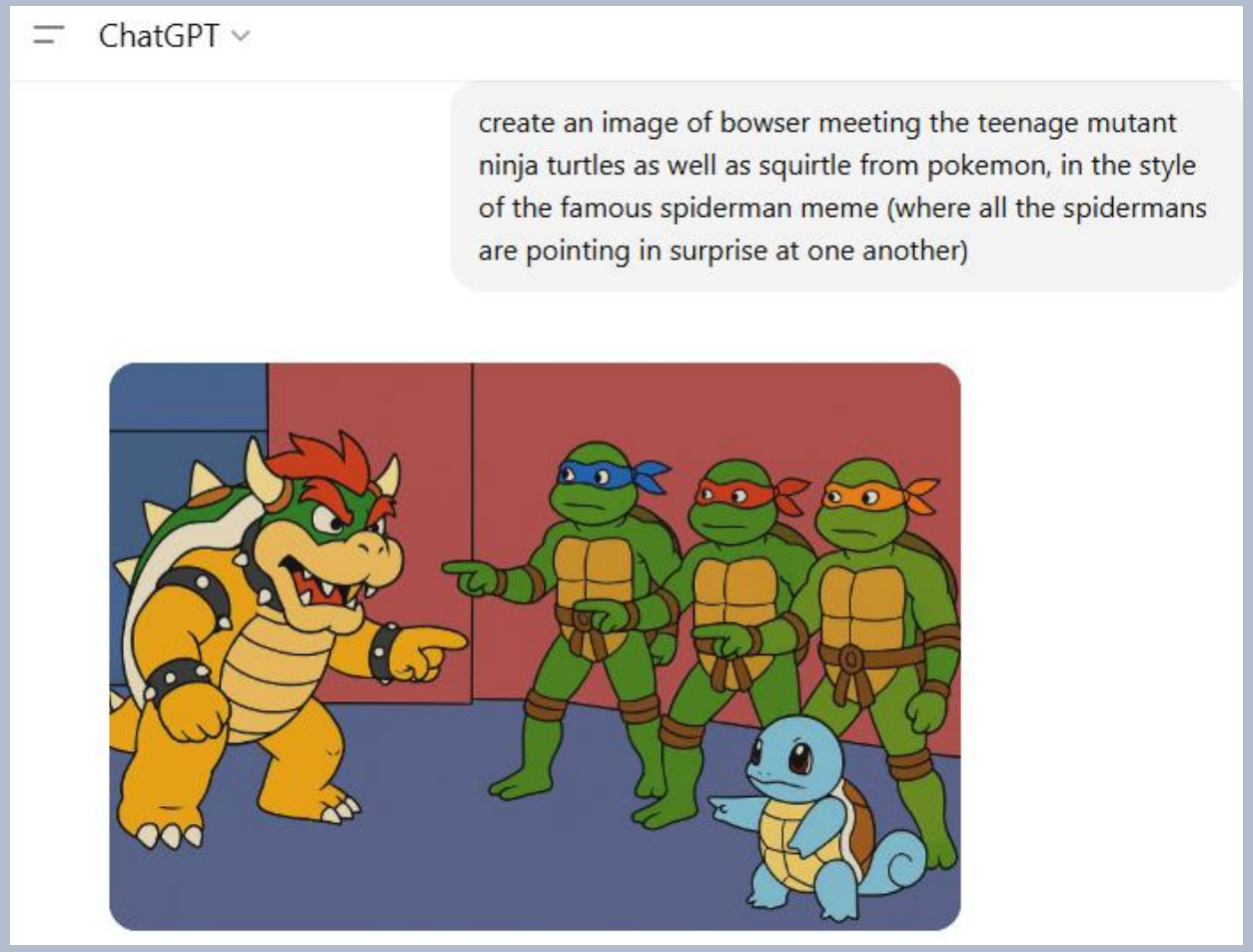
Intellectual property controls

- Some people will use your enterprise's AI chatbot as their free "enterprise-tier" ChatGPT instance

- …and when they use it to commit blatant IP infringement—which frontier models struggle to fully suppress—you are liable

- Training-data copyright infringement is old news. The much more frightening frontier is **derivative works**

Do your terms and conditions address these risks? Do your internal governance policies?



Contracting with AI vendors

- Indemnification (at least from third-party IP claims)

- Reps and warranties
  - Necessary rights to provide AI services
  - Does not infringe
  - Complies with relevant laws and regulations

- Model training and data retention

- Disclosure of subprocessors and flow-down terms
  - Objection right

- Assistance with compliance obligations including transparency

- Ownership of output

Internal controls—Shadow AI

- "Shadow AI" use should be a top concern for every organization
  - Over one-third (38%) of employees acknowledge sharing sensitive work information with AI tools without their employers' permission

- Frontier model providers like OpenAI, Google, and Anthropic are incentivized to collect and train models on user data

- Almost all free accounts and ***even many paid accounts*** allow for permanent model training

All use of AI should only be through enterprise accounts and <u>never</u> through personal accounts!

Internal controls—Agentic AI

- Agentic AI has expanded from well-defined in-app workflow automation apps to tools that essentially take over a user's computer or browser and act ***as that user***

- Agentic AI, like LLMs generally, is inherently unpredictable. By handing it the keys to the car, the risks scale dramatically

- Computer-use agentic tools, like OpenClaw personal AI assistants, should be closely controlled

Agentic AI tools need to be safely sandboxed so that they don't access off-limits data or tools

NEVER ENTER CONFIDENTIAL OR SENSITIVE DATA INTO A NON-ENTERPRISE AI TOOL

- Frontier AI developers are facing an acute scarcity of legal training data
- They are incentivized to train on your data
- The default setting for free and even many pro accounts allows model training
- It is unethical to enter confidential data into tools that train on data because it **irreversibly** enters that data into the model which may disclose the data to third parties *without your knowledge*

Q&A Session