The Changing AI Regulatory Scene: Generative AI and Agentic AI

Key Considerations for CFTC Registrants

Reminders

- The webinar will be recorded and posted to the FIA website within 24 hours of the live webinar.
- Please use the "question" function on your webinar control panel to ask a question to the moderator or speakers.
- *Disclaimer: This webinar is intended for informational purposes only and is not intended to provide investment, tax, business, legal or professional advice. Neither FIA nor its members endorse, approve, recommend, or certify any information, opinion, product, or service referenced in this webinar. FIA makes no representations, warranties, or guarantees as to the webinar's content*.

MoFo Presenters

Stephanie Sharron

Partner, *Technology Transactions*

Palo Alto

SSharron@mofo.com

Marijn Storm

Partner, *Privacy + Data Security*

Amsterdam

MStorm@mofo.com

Rhys Bortignon

Partner, *Derivatives, Commodities + Structured Products*

New York

RBortignon@mofo.com

Agenda

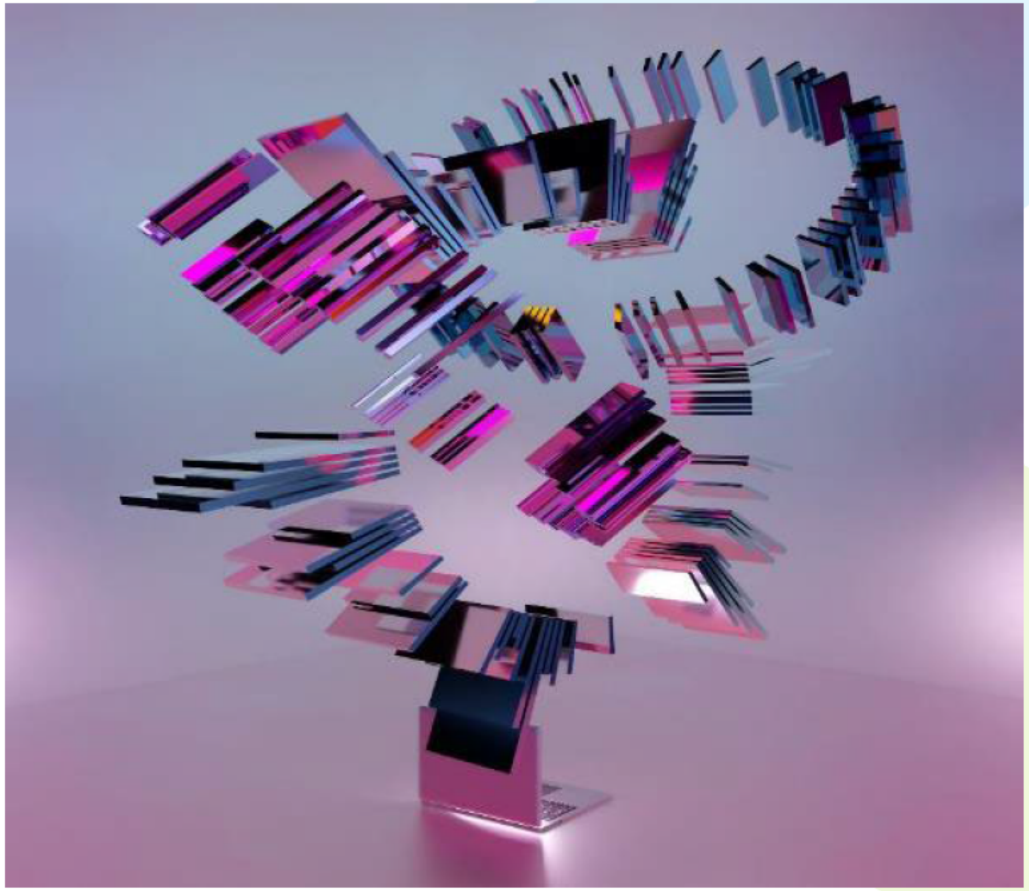
I. Regulatory Background
   1. CFTC Pronouncements
   2. State Legislation Update

II. AI Trends and Risks in Financial Service
   1. Gen AI and Agentic AI Overview
   2. Risks and Mitigations

III. Cybersecurity (EU and US)

IV. Privacy (EU and US)

V. EU AI Act



I. Regulatory Background

CFTC

CFTC: Advisory on Artificial Intelligence

On December 5, 2024, the CFTC staff issued an advisory on the use of AI by various CFTC-regulated entities.

- The advisory sets forth a non-exhaustive list of AI use cases and corresponding existing obligations under the Commodity Exchange Act (CEA) and CFTC regulations that may be potentially implicated in the use of AI by CFTC-regulated entities.
- The staff identified various AI use cases, including:

- Settlement
- Risk Assessment and Risk Management
- Compliance and Recordkeeping
- Customer Protection

- Order Processing and Trade Matching
- Market Surveillance
- System Safeguards
- Member Assessment and Interaction

Best Practices

Partnership Between Legal, Compliance, Technology Services, and Risk Management

Explore AI Governance and Oversight Framework

Create AI Policies and Procedures, including:

- Policy Integration
- Model Risk Management
- Per-Deployment review and validation
- Documentation and Explainability
- Ongoing Monitoring and Performance Standards
- Incorporate AI-specific risk assessment
- Implement AI vendor management
- Executing vendor data protection terms that impose minimum cybersecurity controls and data use restrictions (e.g., for model training)
- Use Case Restrictions

Disclosure Standards and Considerations

Evaluation of and Strengthening Existing Cybersecurity Controls

Ensure Data Input and Confidentiality

Employee Training and Awareness

Monitoring and Supervisory Controls

Board Reporting Considerations

CFTC – Concerns About Fraudulent Use of Generative AI

On March 19, 2025, the CFTC Office of Customer Education and Outreach released a customer advisory, “Criminals Increasing Use of Generative AI to Commit Fraud”

- The Advisory warns that fraudsters use AI to create fake images, voices, videos, live-streaming video chats, social media profiles, and malicious websites designed to look like legitimate financial trading platforms
- The Advisory describes methods that consumers can use to protect themselves, which include:
  - Studying images and videos for imperfections
  - Tightening social media privacy settings to limit exposure to unknown third parties
  - The Advisory also mentions the Federal Bureau of Investigation’s December 3, 2024 public service announcement as an additional resource for consumers to learn more about protecting themselves from AI-related fraud

State Legislation Update

State AI Legislative Developments with Potential Impact on Financial Services

State lawmakers have been increasingly concerned about the potential misuse or unintended consequences of AI

In the last year, for example, states have taken steps in three main areas:

Transparency.

- Utah's Artificial Intelligence Policy Act, S.B. 149, enacted in March 2024, requires a person who provides services in an occupation regulated by the state Department of Commerce to prominently disclose when a person is interacting with generative AI in the provision of regulated services
  - The law became effective on May 1, 2024
- Colorado S.B. 24-205, enacted in May 2024, regulates the use of high-risk AI systems, including those used in financial services
  - The law requires organizations to exercise reasonable care to prevent algorithmic discrimination
  - It mandates transparency when AI-driven tools are used in financial decision-making
  - The law will become effective on February 1, 2026

State AI Legislative Developments with Potential Impact on Financial Services

Transparency.

- Connecticut S.B. 2, introduced on January 8, 2025, aims to ensure fairness, accountability, and transparency in AI applications by emphasizing human oversight in AI-driven decisions and requiring organizations to inform individuals regarding use of AI, particularly in sectors like credit and lending
- Hawaii S.B. 640, introduced on January 17, 2025, would require organizations to clearly and conspicuously inform consumers when they are interacting with AI-powered chatbots, rather than humans, in an effort to prevent deceptive practices
  - If passed, this may require financial institutions employing advanced, agentic AI or chatbot technologies to provide clear notice when consumers are interacting with a non-human conversational interface, especially in the context of dispute resolution or other transactional services
  - Financial institutions using automated dialogue systems for inquiries, dispute resolutions, or negotiations would be required to explicitly disclose that a chatbot is facilitating the interaction, rather than a live representative

State AI Legislative Developments with Potential Impact on Financial Services

Employment.

- The Illinois Limit Predictive Analytics Use Act, Public Act 103-0804, enacted on August 9, 2024, prohibits AI-driven employment decisions that result in discrimination based on protected classes
    - The law will become effective on January 1, 2026
- Published in April 2023, regulations implementing New York City Local Law 144 prohibit employers from using an automated employment decision tool unless the tool undergoes a bias audit within one year of use
    - The regulations became effective in July of 2023

State AI Legislative Developments with Potential Impact on Financial Services

Risk assessment.

- Colorado's law on Consumer Protections in Interactions with Artificial Intelligence Systems, S.B. 24-205, enacted in May 2024, requires developers and deployers of high-risk AI systems to use "reasonable care" to prevent algorithmic discrimination
  - The law will become effective on February 1, 2026
- The California AI Transparency Act, S.B. 942, enacted on September 19, 2024, requires developers of generative AI systems with over one million monthly visitors or users that are publicly accessible in California to provide a free AI detection tool, ensuring that AI-generated content is identifiable while protecting personal provenance data
  - The law will become effective on January 1, 2026
- California A.B. 2013, enacted on September 28, 2024, requires, on or before January 1, 2026, and before each time thereafter, that a developer of generative AI systems post documentation on its website regarding the data used to train the system, when the system is made available for use in California

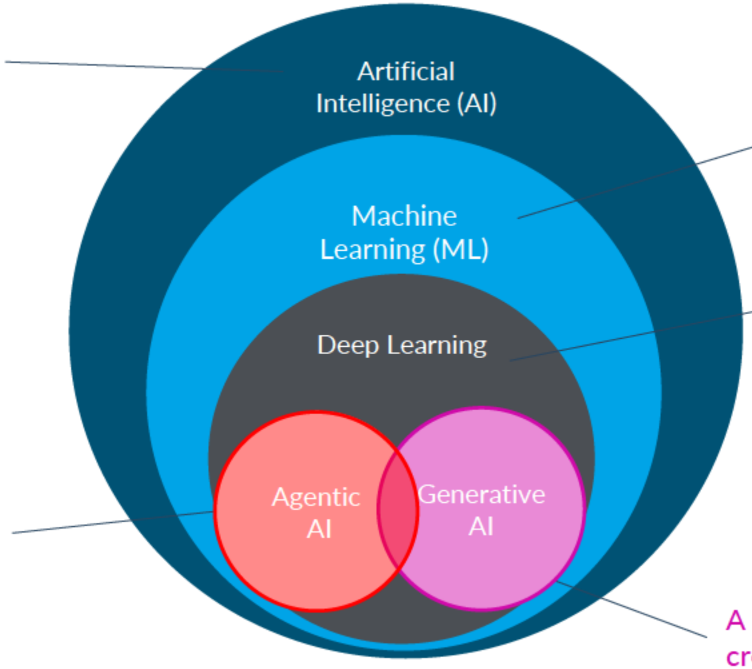
II. AI Trends and Risks in Financial Services

Generative AI and Agentic AI Overview

What is AI?

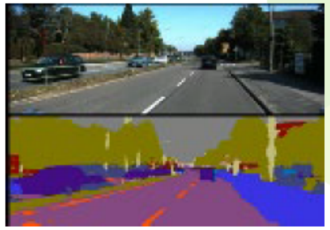
“The ability of machines to imitate intelligent human behavior.”

Software and machines that are capable of tasks that normally require human intelligence



A type of AI that learns from data without explicit step programming

A type of ML that utilizes multi-layered neural networks



A type of AI capable of taking actions autonomously to achieve goals

A type of deep learning that creates new content

Use Cases

AI is being used in back, middle, and front offices to create increase efficiency, reduce cost, better tailor products and services, and to create edge.

Customer Facing

- Virtual assistants/chatbots
- Email inquiries
- Potential customer identification

Operational and Process Oriented

- Brokerage account management, including,
  - Holistic customer profile creation for targeted marketing campaigns
- Asset pricing and allocation
- Portfolio management
- Trade execution
  - Maximize speed and price, including for smart order routing, pricing discovery, best execution, and achieving ideal block trade allocation.
- Investment research/trend identification
- Liquidity/cash management
- Credit risk management

Compliance

- KYC / AML / CTF
- Risk management and regulatory compliance tasks like market surveillance, trade verification, regulatory reporting, capital and margin determinations, and risk assessments
- Monitoring and assessment of evolving compliance landscape
- Cybersecurity protocols

What is Agentic AI?

What makes an AI offering "agentic"?

- Broadly, the term "**agentic**" when applied to AI refers to a software program that **interfaces with other tools, systems, and networks**, and leverages an AI model (usually an LLM) to interpret, plan, and execute a defined set of tasks with **minimal or no human intervention.**
- Agentic AI is sometimes referred to as "**emergent**" because of the surprising activity that appears to infer deeper reasoning capabilities that these solutions sometimes produce, but whether that is in fact true remains hotly debated within the AI community.
- Note, though, that there is no universally agreed upon taxonomy or technical definition of agentic AI or AI agents.

Not all AI Agents are Agentic

- **A customer service chatbot** may seem intelligent (e.g., it gives advice, maybe even initiates a rebooking) but it's still reactive and relies on human oversight.
- **Agentic AI goes further:** "*You have my credit card. I want dark blue jeans. Get me a good deal."* Agentic AI selects, purchases, and ships with no further input.

Risks and Mitigations

Key Risks

Accuracy, Reliability, Validity

- Incorrect or incomplete outputs
- Results not consistent and reproducible
- Results not aligned with intended use case

Transparency and Explainability

- Lack of disclosure of training data sets used for AI
- Lack of ability to explain the basis for generation of the outputs of the AI solution

US Regulatory

- Executive Orders
- Product and industry specific regulatory guidance
- DOJ/EEOC (bias/anti-discrimination)
- State laws and medical boards

IP Infringement and other Violation of 3d Party Rights

- Infringement or violation of 3d party rights by inputs or outputs
- Lack of IP protection for outputs
- Lack of rights in output and usage data
- Confidentiality concerns (e.g., unintended disclosure in outputs)

Key Risks

Privacy

- Privacy violations resulting from use of personal data to train models without proper notice and when required, consent (federal and state regulatory enforcement (e.g., FTC 20-year consent decrees, algorithmic disgorgement))
- AI output biased or unfair, reflecting lack of representative training data
- Discrimination claims (federal and state agency enforcement)

Security

- "Poisoning" of data model by injection of "fake" training data
- Manipulation of output
- Unauthorized access to sensitive data and IP
- Fraud
- Unauthorized access to and exploitation of AI agents and the tools and resources on which they rely

Safety and Product Liability

- Threats to the physical or personal safety of individuals (e.g., patients), groups of individuals or the public
- Lack of human oversight of autonomous decision-making

Environmental and other Risks

- Cost of energy consumption
- Risk to sustainability and environment; ESG reporting
- Impact on labor and workforce
- Risks to human agency
- Risks of vendor use of AI
- Risks of third-party use of AI (independent of company AI adoption)
- Competition issues

Amplified Risks: What's Different About Agentic AI Solutions?

Accuracy, Reliability, and Alignment

- New and amplified risks with accuracy, reliability, and misalignment of results with user intentions.

Data Exposure

- Increased risk of expanded or unintended sharing of personal data, IP, and confidential information with third-party tools and resources.

Security Vulnerabilities

- New attack vectors on external resources on which agentic AI solutions rely, along with amplified risks of model poisoning and other GenAI vulnerabilities.

Harm at Scale

- Amplified risk of harm to individuals and enterprises resulting if the agentic AI's behavior is misaligned with user intention

Transparency

- "Black box" or transparency issues increase as interactions among agentic AI solutions become more complex.

Bias and Fairness

- Amplified risk of unfair or biased results due to scope, complexity, speed, and scale at which agentic AI solutions operate.

Regulatory Compliance

- New risks related to liability and risk allocation under laws not designed with agentic AI in mind.

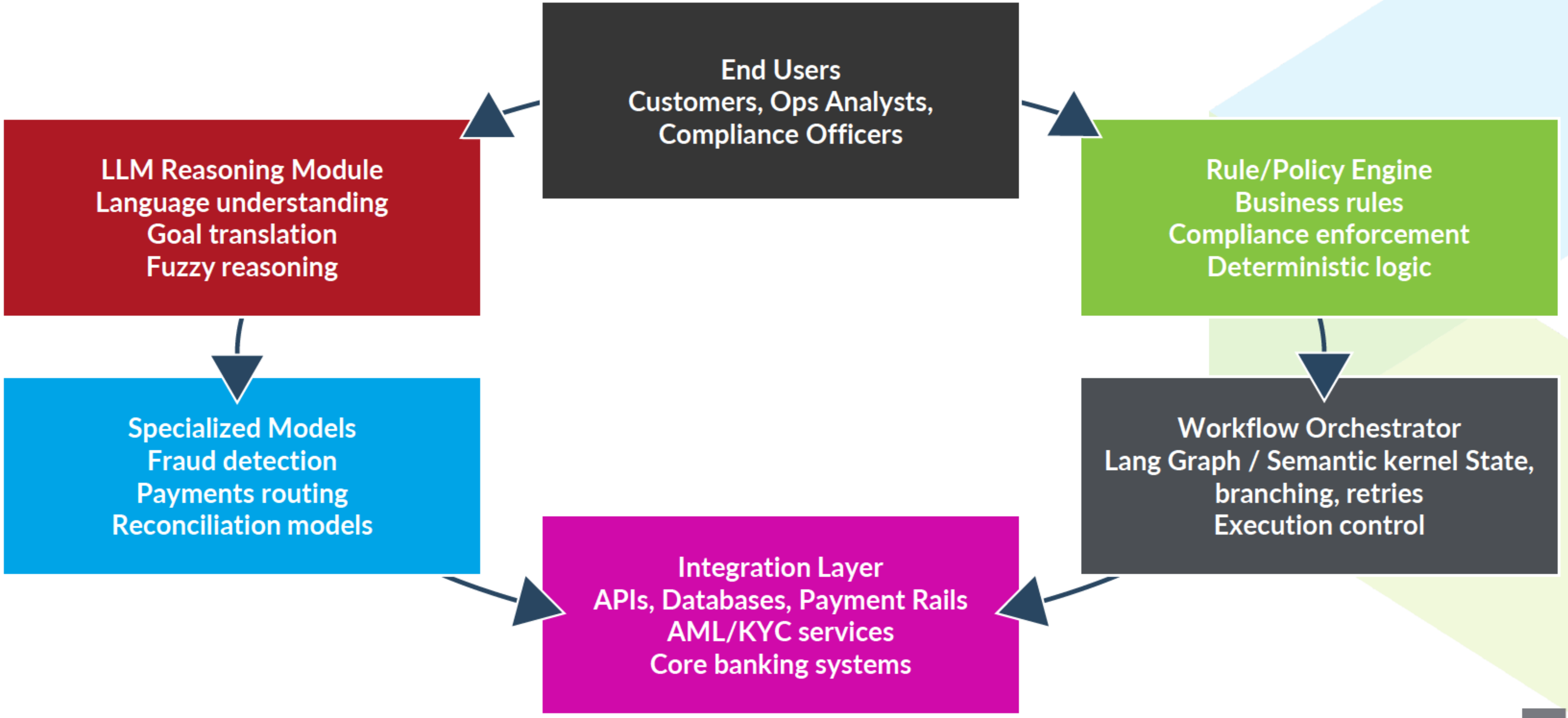
Social and Labor Impacts

- New and amplified labor-related and societal risks.

The Hidden Risk - What Pre-Assessments Miss

- **Self-Modification:** Agents adapt prompts, goals, or parameters after deployment.
- **Scaffolding Effects:** Layers of interconnected agents amplify or alter behavior dynamically.
- **Expanded Tool Access:** Real-time API or data access can introduce new, unvetted risk vectors.
- **User-Level Modifications:** End users can customize or fine-tune behavior beyond the original compliance review.
- **Real-World Scale:** Interactions at enterprise scale can create compound or emergent risks not visible in lab testing.

Hybrid Architecture: The Next Evolution



End Users
Customers, Ops Analysts,
Compliance Officers

LLM Reasoning Module
Language understanding
Goal translation
Fuzzy reasoning

Rule/Policy Engine
Business rules
Compliance enforcement
Deterministic logic

Specialized Models
Fraud detection
Payments routing
Reconciliation models

Workflow Orchestrator
Lang Graph / Semantic kernel State,
branching, retries
Execution control

Integration Layer
APIs, Databases, Payment Rails
AML/KYC services
Core banking systems

Agency Law, Contractual Terms, & Liability

Common Law of Agency and Agentic AI

- AI agents are not legal persons … at least not yet!
- Attribution through principals: Delegated authority defines agency
- Standards of care: Human reasonableness vs. emerging machine-specific standards
- Gaps in personhood and accountability: AI systems cannot themselves be sued
- UETA and UNCITRAL Model Law of Automated Contracting: Provides limited but relevant guidance

Contractual Terms

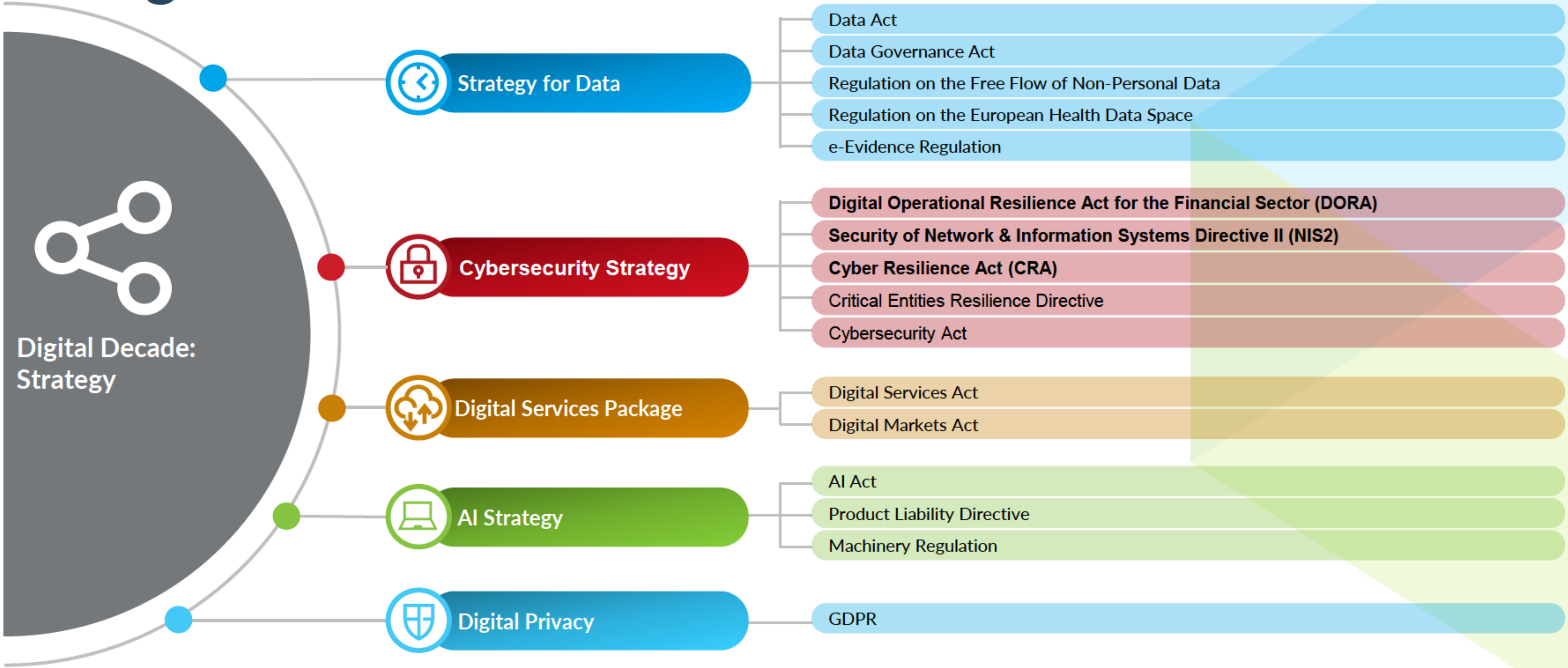
- Contractual provisions are critical for signaling the parties’ intent on allocation of risk and liability.
- Courts will rely on these terms to interpret conduct but contracts cannot insulate unlawful or tortious acts.
- Agreements should specify control, supervision, indemnities, and termination rights tied to agent behavior.

When Liability Should Arise

- Liability attaches where harms stem from foreseeable misuse, design failure, or inadequate oversight.
- The greater the autonomy delegated, the greater the duty to prevent or mitigate misuse.
- Courts will analogize to negligence, product liability, and respondeat-superior doctrines in assigning responsibility.

III. Cyber Security (EU and US)

Setting the scene: How does everything fit in the Digital Decade?



Digital Decade: Strategy

- Strategy for Data
  - Data Act
  - Data Governance Act
  - Regulation on the Free Flow of Non-Personal Data
  - Regulation on the European Health Data Space
  - e-Evidence Regulation
- Cybersecurity Strategy
  - **Digital Operational Resilience Act for the Financial Sector (DORA)**
  - **Security of Network & Information Systems Directive II (NIS2)**
  - **Cyber Resilience Act (CRA)**
  - Critical Entities Resilience Directive
  - Cybersecurity Act
- Digital Services Package
  - Digital Services Act
  - Digital Markets Act
- AI Strategy
  - AI Act
  - Product Liability Directive
  - Machinery Regulation
- Digital Privacy
  - GDPR

Setting the scene: The three cyber frameworks

CRA
Cyber Resilience Act

- Cyber security requirements for **products** with digital elements
- **Covered**: browsers, firewalls, password managers, routers, operating systems, smart meters

Regulation: applies from 11 December 2027

Notification duties: from 11 September 2026

NIS2
Network Information Security

- **Cyber** resilience
- **Covered**: essential + important entities

Directive: MS had to implement and apply from 18 October 2024

DORA
Digital Operational Resilience Act

- **Physical + cyber** resilience
- **Covered**: financial entities + ICT third party service providers
- **Lex specialis**:
  - for NIS2
  - for PSD2 as to notification

Regulation: in force since 17 January 2025

NIS2 - overview

NIS2 is a directive with minimum harmonization

Wider scope of application

- Energy, transport, banking, financial markets infrastructure, healthcare, drinking water, digital infrastructure (including cloud computing service providers), ICT services management (business-to-business), wastewater, public administration, space activities
- Digital providers (including certain online platforms), postal and courier services, waste management, manufacturing, production, and distribution of chemicals, production, processing, and distribution of food, research, manufacturing

Stricter governance requirements

More prescriptive incident reporting requirements

Extraterritorial scope

NIS2: Update on implementation / regulatory guidance

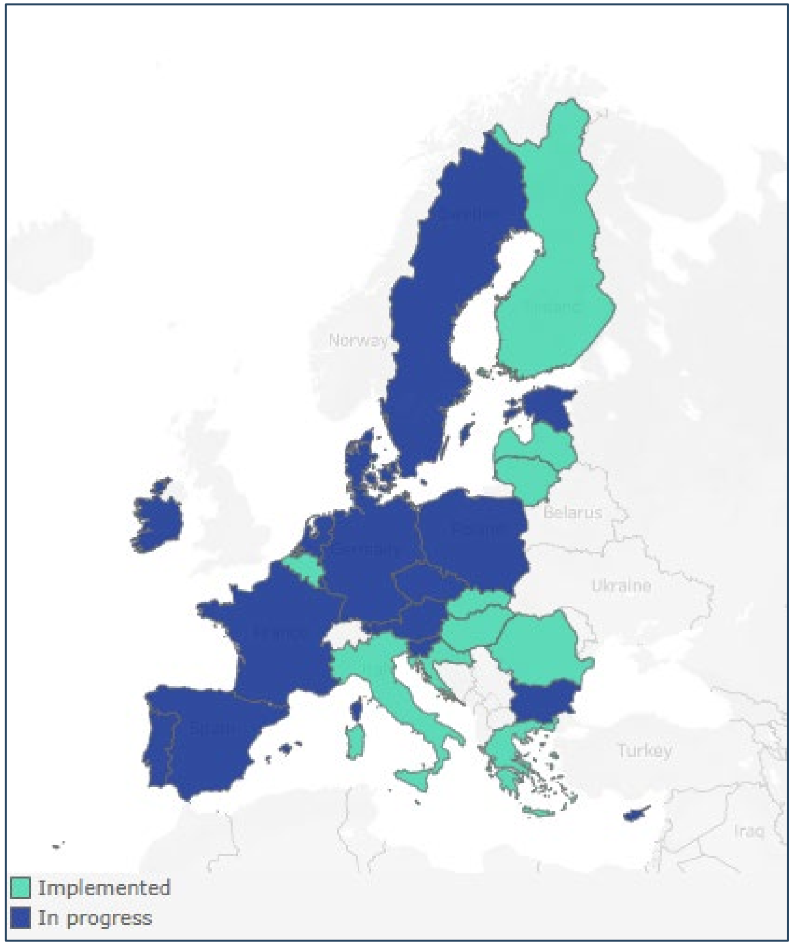
- Implementation inconsistent across Member States

  Implemented: 15

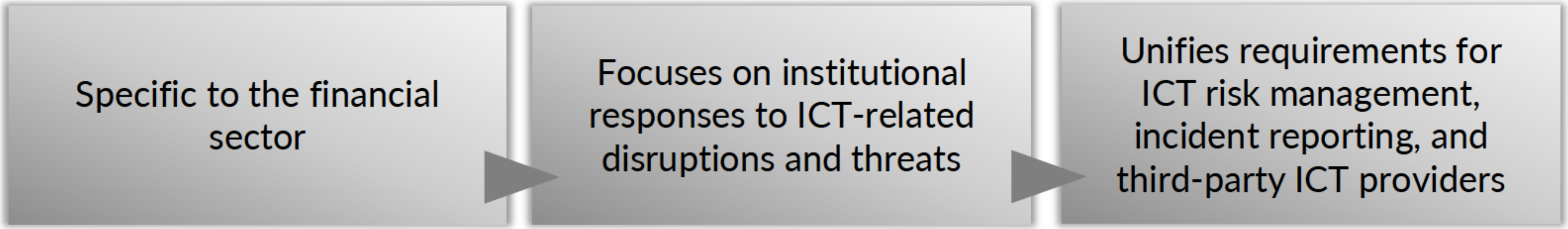
  - Most recently: Czechia, Hungary, Slovenia

  Still to come: 12

  - Expected Q3/4 2025: Portugal, Estonia, Sweden



DORA



Specific to the financial sector

Focuses on institutional responses to ICT-related disruptions and threats

Unifies requirements for ICT risk management, incident reporting, and third-party ICT providers

ICT risk management (*Chapter 2 DORA*)

ICT-related incidents (*Chapter 3 DORA*)

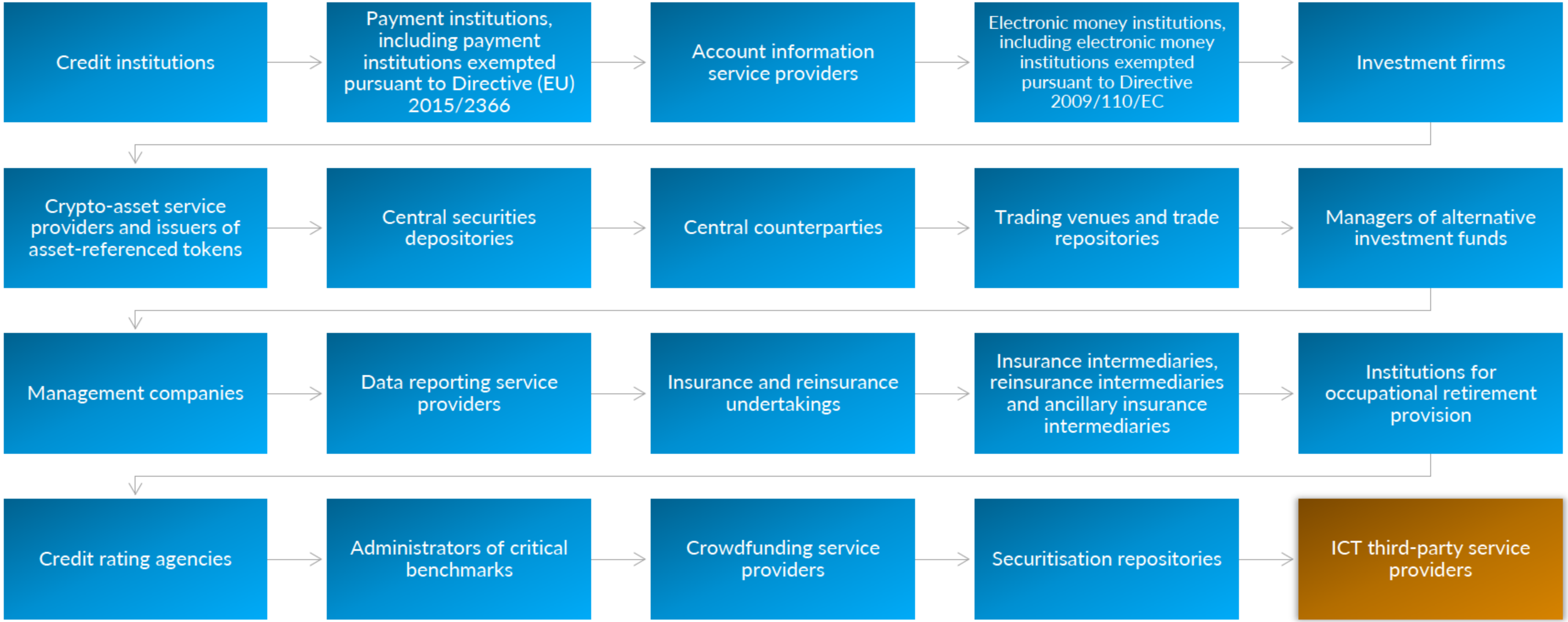
Digital operational resilience testing (*Chapter 4 DORA*)

Managing ICT third-party risk (*Chapter 5 DORA*)

Information sharing arrangements (*Chapter 6 DORA*)

DORA

In-scope entities (Article 2)



Credit institutions

Payment institutions, including payment institutions exempted pursuant to Directive (EU) 2015/2366

Account information service providers

Electronic money institutions, including electronic money institutions exempted pursuant to Directive 2009/110/EC

Investment firms

Crypto-asset service providers and issuers of asset-referenced tokens

Central securities depositories

Central counterparties

Trading venues and trade repositories

Managers of alternative investment funds

Management companies

Data reporting service providers

Insurance and reinsurance undertakings

Insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries

Institutions for occupational retirement provision

Credit rating agencies

Administrators of critical benchmarks

Crowdfunding service providers

Securitisation repositories

ICT third-party service providers

DORA: Distinguishing between a critical provider or a provider supporting critical or important functions

ICT providers

- Digital and data services provided through ICT systems to users on an **ongoing basis** (*Article 3(21)*)
  - E.g., providers of cloud computing services, software, data analytics services, and data centers

ICT providers supporting critical or important functions (CIFs)

- Certain ICT providers support functions that, if disrupted, would materially impair the financial performance, or the soundness or continuity of the financial entity's services, or the discontinued, defective or failed performance of that function would impair the continuing compliance of the financial entity (*Article 3(22)*)
  - These ICT providers are not "critical" providers
  - Determined by financial entities

Critical ICT providers

- Certain ICT providers designated as "critical" by the European Supervisory Authorities (*Article 3(23)*)

DORA

ICT Third-Party management

Financial entities are required to manage ICT third-party risk as part of their overall risk management:

- Explaining how ICT risk management framework supports business strategy and objectives
- Financial entities should have a policy which shall
  - **Require**: that *measures* and *key indicators* to measure third party performance are contractually agreed upon
  - **Specify**: *how the FE establishes* that third party ICT service provider meets its performance and quality standards
  - **Ensure**: that third party specialist ICT service provider provides *appropriate reports* including periodic reports, incident reports, service delivery reports, reports on ICT security and reports on business continuity measures and testing

    + That third party performance is assessed according to KPIs, KCIs, audits, self-certifications and independent review

- Contractual requirements under DORA itself:
  - Basic for ICT providers (Art. 30(1))
  - More expansive for ICT providers supporting CIFs (Art. 30 (2))

Understanding the CRA

Aim

Improving the security of digital products throughout the whole product life cycle and enhancing transparency

Scope

Products with digital elements made available on the EU market, with a data connection to a device or network (*Article 3(1)*)

Relevant Parties

Obligations imposed on hardware manufacturers, software developers, importers, and distributors

Cybersecurity

Critical Infrastructure and Ransomware Notice Obligations

CISA proposed rule

On April 4, 2024, CISA published its proposed rule to implement the CIRCIA requirements

The proposed rule appears to go far beyond the statute in defining the types of entities and incidents for which reporting obligations would apply

If a report is required, the proposed rule would apply to many financial institutions and impose detailed requirements for the information that must be shared with CISA at a level of granularity significantly beyond what any financial services regulator currently requires

With respect to financial services, an entity would be considered a covered entity as long as it falls within the financial services critical infrastructure sector, as defined by the CISA Financial Services Sector-Specific Plan, and is not a small business

Under the proposed rule, a covered entity would include any Financial Services Sector entity that is required to report cybersecurity incidents to its primary federal regulator

Cybersecurity

Critical Infrastructure and Ransomware Notice Obligations

Under the proposed rule, a covered entity would be required to submit a report to CISA within 72 hours after "reasonably believ[ing]" that a covered cyber incident has occurred

- CISA acknowledges that an entity may need to perform "preliminary analysis" before reaching a reasonable belief that a covered cyber incident has occurred
- But, the proposed rule indicates that the preliminary analysis "should be relatively short in duration"

The proposed rule would require the incident report to include:

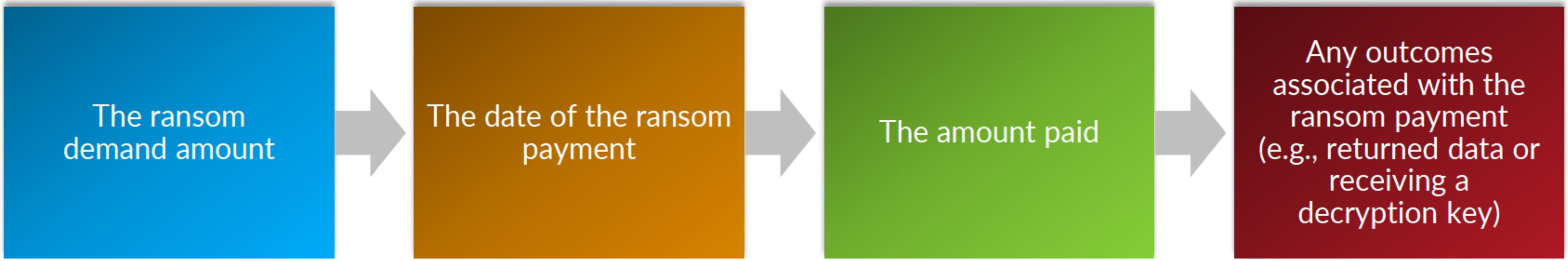
- A narrative description of the incident, including the impacted information systems, a timeline of the incident, and operational impact
- A description of any vulnerabilities, as well as the covered entity's security controls
- The tactics, techniques and procedures used by the perpetrator and any associated indicators of compromise
- Whether law enforcement was engaged and the identities of, and requested assistance from, any third parties

Cybersecurity

Critical Infrastructure and Ransomware Notice Obligations

Under the proposed rule, a covered entity also would be required to report to CISA any ransom payment within 24 hours of making the payment

- For these reports, the proposed rule would require that the information provided by a covered entity include:



The ransom demand amount

The date of the ransom payment

The amount paid

Any outcomes associated with the ransom payment (e.g., returned data or receiving a decryption key)

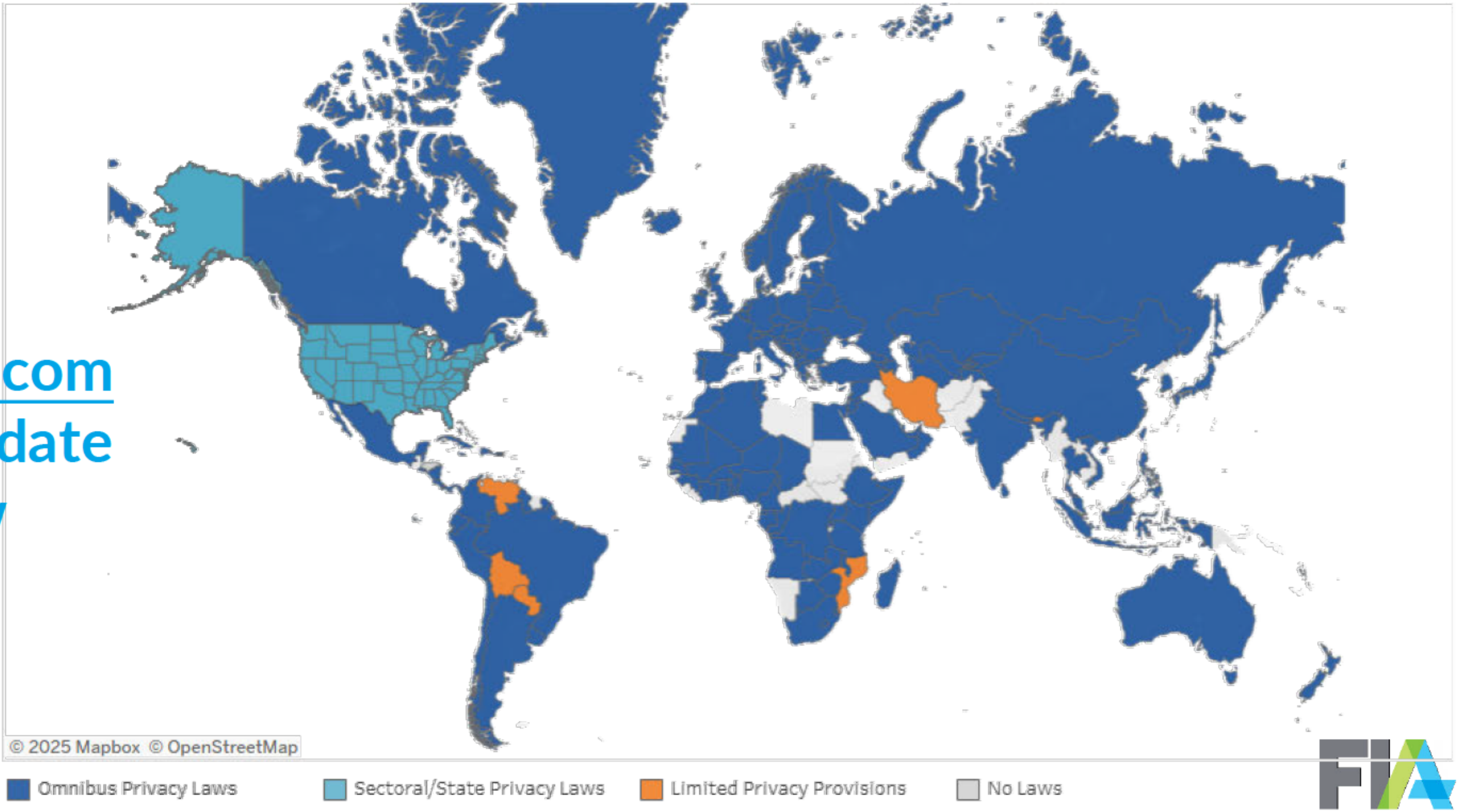
CISA was expected to issue a final rule by October 2025, but that has been delayed

- Rule would be effective in 2026

IV. Privacy (EU and US)

Privacy laws around the word continue to develop

Visit mofoprivacy.com for an up-to-date overview


© 2025 Mapbox © OpenStreetMap

California: CCPA Regulations

The Agency’s final regulations are detailed and prescriptive, and address:

Requirements for CCPA notices (e.g., notices at collection and privacy policies), including:

- Format
- Content
- Timing

Limitations on collection, use, retention and sharing of personal information relating to California residents

Business practices for handling the CCPA rights requests of California residents, including how a business must respond to requests and the timeline for such responses

Requirements for:

- Obtaining parental consent for the sale or sharing of personal information relating to California residents under the age of 13
- Obtaining opt-in consent of California residents between the ages of 13 and 16

Standards for contracts with service providers and contractors

GLBA = No CCPA

The CCPA, as amended by the CPRA, continues to include an exception for, and does not apply with respect to, information that is "subject to" the Gramm-Leach-Bliley Act

- Financial institutions almost uniformly rely on this exception and do not publicly extend the CCPA's privacy rights to data that is subject to the GLBA
- Nonetheless, financial institutions must identify the data that they handle that is not subject to the GLBA and implement controls designed to comply with the relevant obligations of the CCPA for that information
- This creates the challenge of complying with different privacy regimes for different data

The GLBA with respect to retail consumer financial data

The CCPA with respect to certain other data relating to California residents, such as personal information obtained in a commercial financial services context

Privacy laws in other states

Since California enacted the CCPA, 19 states have enacted similar, comprehensive privacy laws

GLBA exceptions are critical. Similar to the CCPA, each of these 19 state privacy laws creates a number of privacy rights for relevant state residents (and corresponding obligations for businesses), such as:

- Access
- Deletion
- Sale opt-out rights

Although the Oregon and Minnesota laws are more nuanced, these state privacy laws include exceptions for both financial institutions (and sometimes their affiliates) and data that is subject to the GLBA

- That is, these state privacy laws do not apply to financial institutions
- For example, the Virginia law does “not apply to” a “financial institution or data subject to Title V of the” GLBA

Executive Order and DOJ Rule on Cross-Border Data Access

In March 2024, former President Biden published Executive Order 14117 on Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern

The EO prohibits or restricts U.S. companies from knowingly providing Countries of Concern or Covered Persons with access to Covered Data

It likely will impact most entities operating in the U.S. that collect or transfer data within the Program's ambit—making routine business decisions and activities potentially unlawful

- **Countries of Concern:** China (including Hong Kong and Macau), Cuba, Iran, North Korea, Russia and Venezuela
- **Covered Person**: (i) non-U.S. person, resident of Country of Concern; or (ii) foreign entity, ≥50% owned by, organized under the laws of, or has principal place of business in Country of Concern
- **Covered Data:** six types of "bulk" sensitive personal data of U.S. residents + certain federal government-related data
  - **Bulk sensitive personal data** includes personal financial data (e.g., bank account information) or personal health information (e.g., physical and mental health condition) relating to at least 10,000 U.S. persons
  - **Government-related data** includes sensitive personal data that a party markets as linked or linkable to current or former employees or contractors of the federal government

Executive Order and DOJ Rule on Cross-Border Data Access

Prohibited transactions:

Selling, licensing, similar commercial transaction of Covered Data to a Covered Person, recipient did not collect the data directly from the individuals linked or linkable to the data

Restricted transactions:

Providing access to Covered Data to Covered Person, unless:

- Vendor agreements for goods or services
- Employment agreements
- Investment agreements in which a person obtains direct or indirect ownership of a U.S. legal entity or real estate in the U.S.

Financial services exceptions:

Limitations do not apply to transactions “to the extent that they are ordinarily incident to and part of the provision of financial services”

- DOJ FAQs: financial institutions are not categorically exempt
- Must evaluate each data transfer to determine whether it is “incident to and part of the provision of financial services”
- For example, a vendor agreement that provides a covered person with access to bulk U.S. sensitive personal data “is not ordinarily incident to and part of the provision of financial services for a financial institution’s wholly domestic operations”

What about the EU?

GDPR has been in effect for 7 years:

Hot enforcement topics: cross-border data transfers and data usage (including for other purposes than for which collected)

Specifically relevant for AI: opt-in or opt-out for AI training (xAI enforcement) and data transfers to non-EU AI tools (various DeepSeek enforcements)

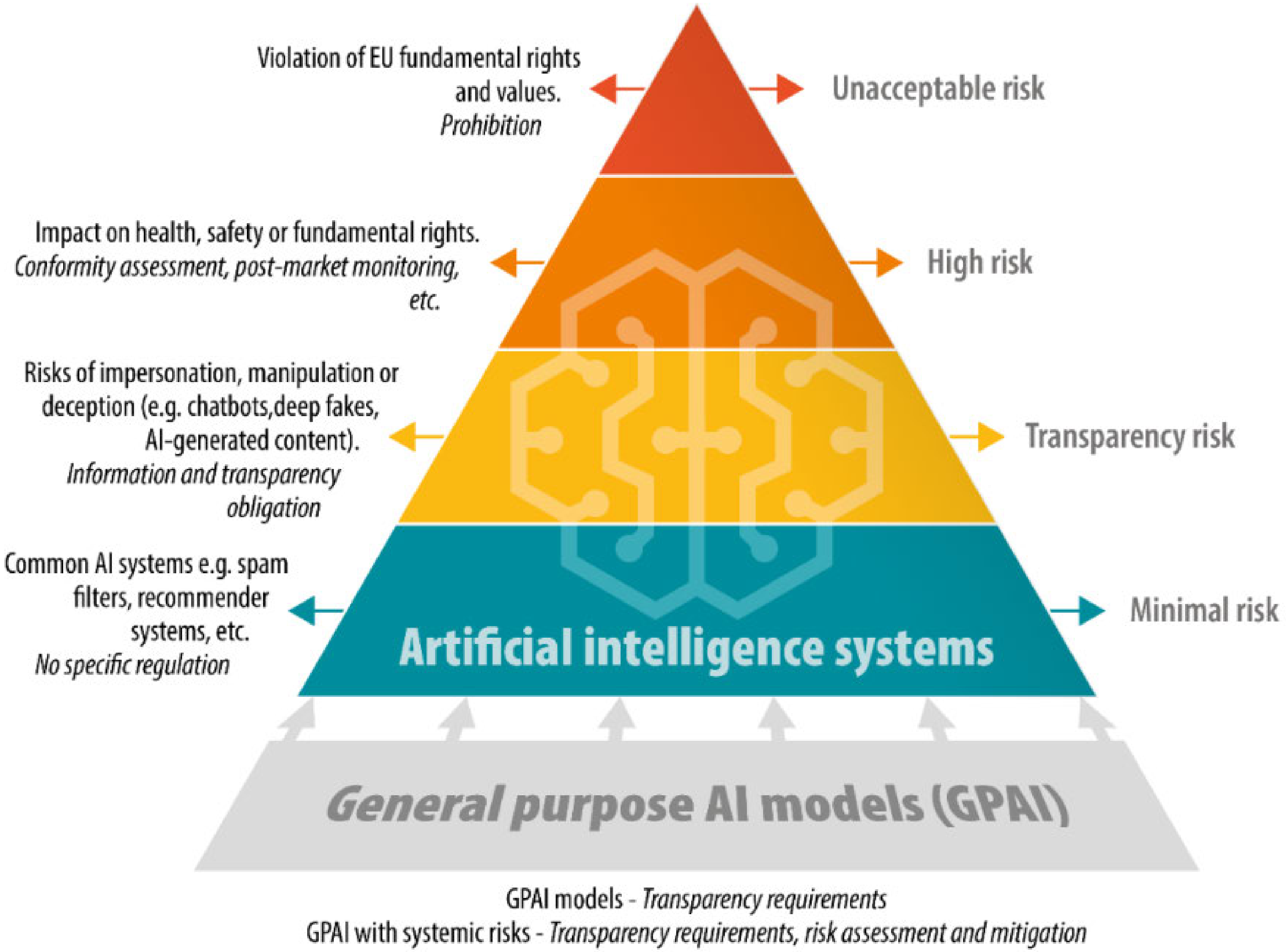
Relevance continues to increase: DPA appointed as supervisor for EU AI Act in majority of countries that have made an appointment, and DPAs were already enforcing under GDPR

V. EU AIA

Why an EU AI Act?

- Necessary for non-personal data
- Necessary for AI trained outside EU
- AI Act intended as a “top-on” of GDPR (**GDPR remains applicable**)
- Risk management obligations comparable to GDPR
  - Data governance requirements
- GDPR DPIA is basis for:
  - AI Conformity Assessment
  - AI Human Rights Impact Assessment

EU AI Act: Risk-Based Approach



Violation of EU fundamental rights and values.
Prohibition

Unacceptable risk

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

High risk

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

Transparency risk

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

Minimal risk

Artificial intelligence systems

General purpose AI models (GPAI)

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

Source: *European Commission*

High-Risk AI – AI Systems Intended to Be Used as/for…

- A regulated product or as a safety component of a regulated product
- Management and operation of critical infrastructures
- Education and vocational training
- **Employment, worker management, and access to self-employment**
- **Access to essential private services and public services**
- Law enforcement and predictive policing
- Biometric identification and categorization
- Migration, asylum, and border control management
- Assistance in legal interpretation and application of the law

High-Risk AI – AI Systems Intended to Be Used as/for...

- A regulated product or as a safety component of a regulated product
- Management and operation of critical infrastructures
- Education and vocational training
- **Employment, worker management, and access to self-employment**
- **Access to essential private services and public services**
- Law enforcement and predictive policing
- Biometric identification and categorization
- Migration, asylum, and border control management
- Assistance in legal interpretation and application of the law

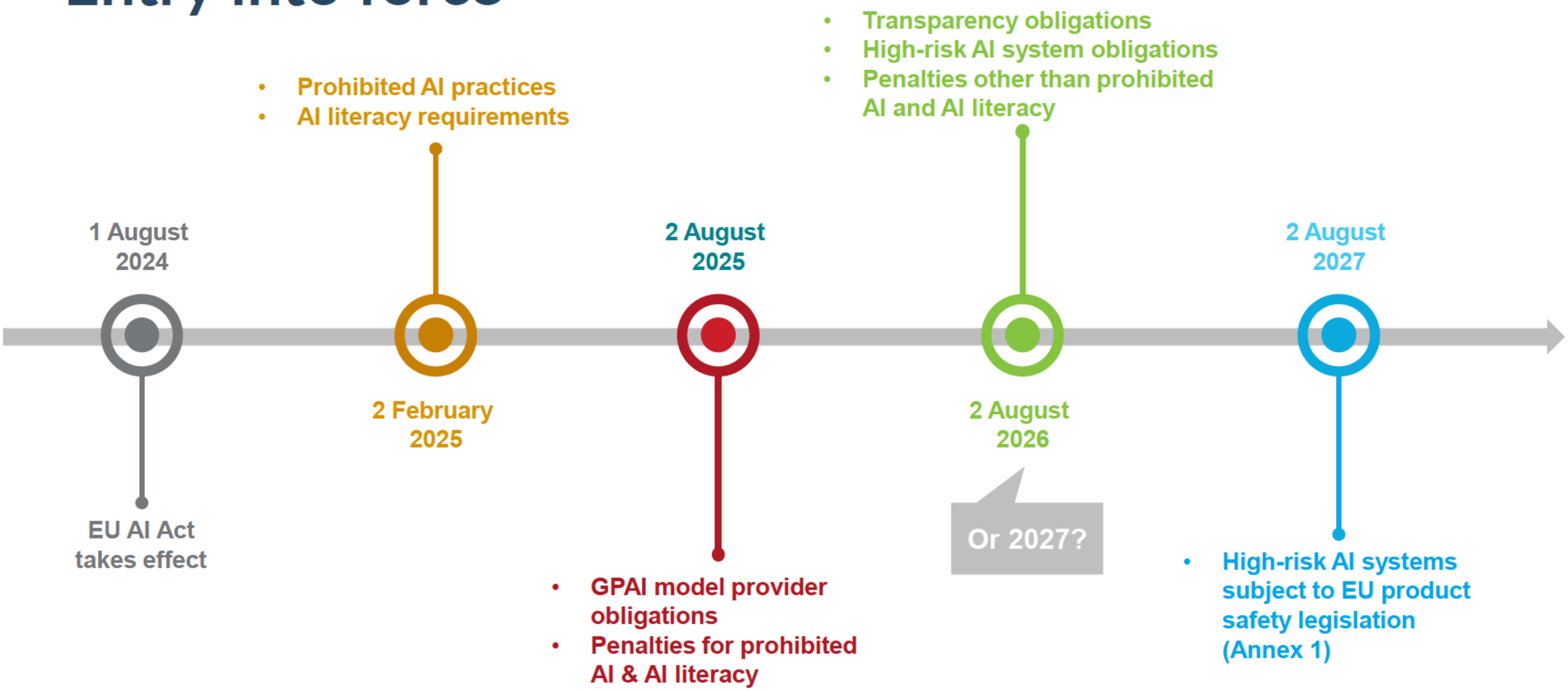
EU AI Act: Covered Entities

The EU AI Act applies to:

1. Providers of GPAI models
2. Providers of AI systems
3. Deployers of AI systems
4. Importers and distributors of AI systems
5. EU representatives of non-EU providers
6. Affected individuals (so they can use their rights)

An entity can have **several roles**, e.g., provider of a GPAI model and provider the AI system powered by the AI model; provider and deployer of an AI system.

Entry into force



1 August 2024

EU AI Act takes effect

2 February 2025

- Prohibited AI practices
- AI literacy requirements

2 August 2025

- GPAI model provider obligations
- Penalties for prohibited AI & AI literacy

2 August 2026

Or 2027?

- Transparency obligations
- High-risk AI system obligations
- Penalties other than prohibited AI and AI literacy

2 August 2027

- High-risk AI systems subject to EU product safety legislation (Annex 1)

Fines/Penalties

Non-compliance regarding prohibited AI systems:

- Administrative fines of up to **35 million EUR** or, if the offender is a company, up to **7% of its total worldwide annual turnover**, whichever is higher

Non-compliance with obligations for high-risk systems, GPAI models, or transparency obligations

- Administrative fines of up to **15 million EUR** or, if the offender is a company, up to **3% of its total worldwide annual turnover**, whichever is higher

Questions?

MoFo Presenters

Stephanie L. Sharron
Partner, Palo Alto
Technology Transactions
SSharron@mofo.com

Stephanie Sharron is a trusted advisor to companies with respect to technology, fintech, and life sciences transactions, related IP counseling, and responsible tech and AI governance practices.

Stephanie has over two decades of experience working with clients on the complex technology, intellectual property, and data rights issues across technology and business sectors, including, among others: artificial intelligence (including machine learning and other data analytics approaches), cloud services, life sciences and healthcare, the Internet of Things (IoT), fintech, digital transactions, autonomous systems, cybersecurity solutions, semiconductors, edtech and cleantech.

Additionally, Stephanie advises on the commercial technology and intellectual property aspects of mergers, acquisitions, asset spin-off transactions, and private equity investments. Stephanie is a member of the firm's global Sustainability + Corporate Responsibility and FinTech steering committees, where she helps to lead and collaborate with attorneys across multiple practices. Stephanie is also a sought-after speaker and thought leader on the issues at the intersection of technology and law, including regarding AI, Life Sciences and FinTech.

Marijn Storm
Partner, Brussels | Amsterdam
Privacy + Data Security
MStorm@mofo.com

Marijn Storm specializes on the intersection of law and technology, with a focus on cutting-edge technologies, such as (generative) artificial intelligence (AI) and large language models, ethical tech, and biometrics. Based in Morrison Foerster's Amsterdam office, he advises global companies and organizations on a wide range of their most complex and pressing privacy and data security challenges.

Marijn's deep experience in both law and technology enables him to navigate the rapidly evolving landscape of privacy, data security, and technological innovation. Bridging the gap between legal requirements and technological advancements, Marijn advises and educates in-house legal teams on how to effectively manage and oversee technical applications such as AI and, specifically, generative AI. In addition, Marijn trains technical teams on implementing technical solutions in a privacy-by-design fashion, enabling compliance with AI and data protection laws around the world.

MoFo Presenters

Rhys Bortignon
Partner, New York
Finance | Capital Markets
RBortignon@mofo.com

Rhys is a member of the firm's Derivatives, Commodities + Structured Products practice group and Co-Head of its Securities + Derivatives Regulatory Solutions team.

Rhys Bortignon's main area of practice involves derivatives and structured products. With a focus on practical and commercial solutions, Rhys provides counsel to a diverse range of U.S. and international clients, from both the buy-side and sell-side, including corporates, investment banks, commercial banks, private equity, funds, investment managers, and sovereigns. Rhys offers strategic guidance to his clients from both a transactional and a regulatory perspective, and navigates complex cross-border issues with proficiency, providing pragmatic advice to clients operating globally.

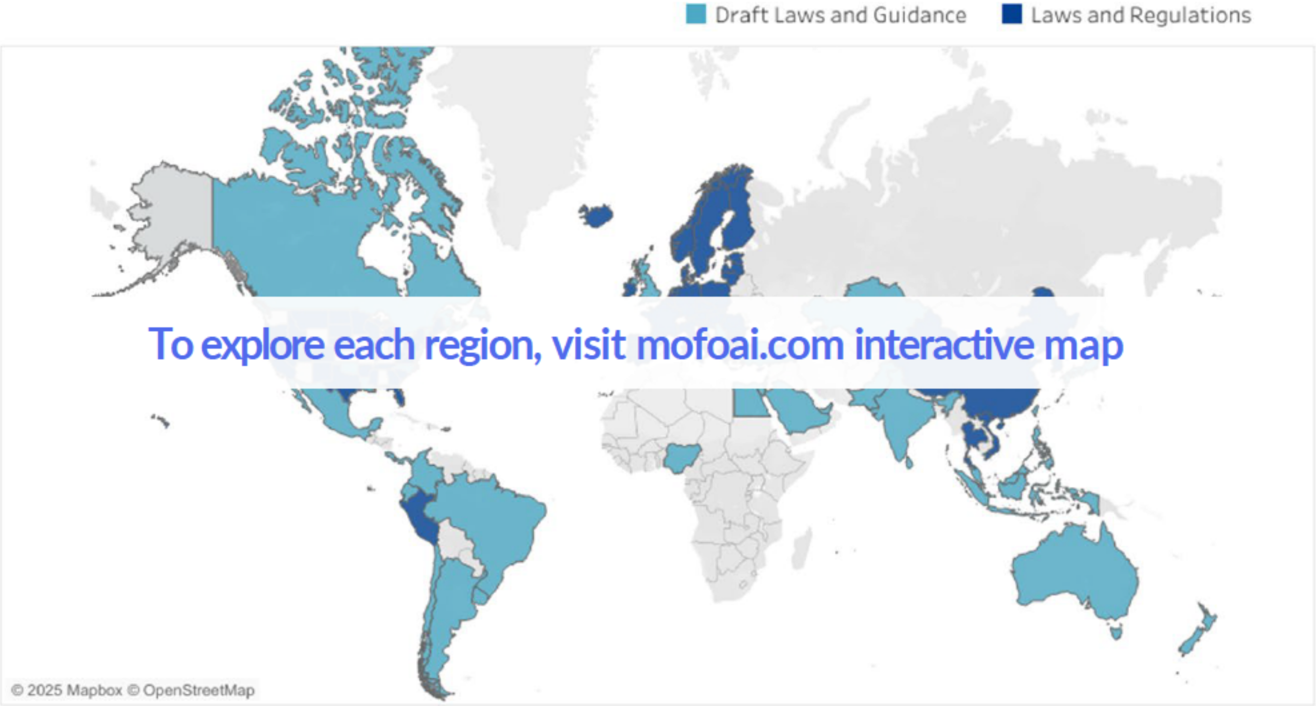
Rhys' experience spans the spectrum of derivative transactions across asset classes, including rates, foreign exchange, credit, equity, digital assets, and commodities. He also frequently advises on margin loans, repo and securities lending transactions, the hedging components of project and corporate financings, as well as various structured products.

AI Laws, Regulations, and Regulators

www.mofoai.com

Morrison Foerster is experienced and immersed in artificial intelligence (AI) technology, just like our clients.
Our cutting-edge AI lawyers track the latest and most significant developments in AI issued by government authorities. We successfully guide companies—across all industries—to comply with both new and existing regulatory regimes.

Our AI Legislative Map and Resource Center helps clients stay informed and navigate compliance effectively.


Draft Laws and Guidance
Laws and Regulations
To explore each region, visit mofoai.com interactive map
© 2025 Mapbox © OpenStreetMap

Scan the QR code to view this map:

FIA