



ALERT · AUGUST 5, 2025

# European Commission Issues Comprehensive Code of Practice for General-Purpose AI: A New Era of AI Governance

How to navigate the voluntary framework that seeks to reshape global AI development.

BY Kaitlin Betancourt Gretchen Scott Joseph Ndep

## Executive Summary

The European Commission published its final code of practice (the Code) for general-purpose artificial intelligence (GPAI) models on 10 July 2025, delivering on its promise to provide practical guidance for AI governance. This comprehensive framework represents the culmination of an extensive stakeholder process involving almost 1,000 participants and marks a pivotal moment in the evolution of AI regulation.

While technically voluntary, the Code offers something increasingly valuable in today's uncertain regulatory landscape: a clear pathway to demonstrate compliance with the EU AI Act's obligations for GPAI model providers. The Code takes effect on 2 August 2025, coinciding with key provisions of the AI Act itself, creating immediate practical implications for businesses across the AI value chain.

While the Code differs in many regards from the Trump administration's recently released AI Action Plan, namely the plan's focus on deregulation and competitive positioning, the Code and the plan both place a strong emphasis on comprehensive governance and risk management. For multinational businesses, this creates both opportunities and challenges in navigating an increasingly complex regulatory environment.

## Why This Matters Now

The AI industry has been watching European regulatory developments with a mixture of anticipation and apprehension. The Code represents the EU's attempt to translate broad regulatory principles into actionable guidance for businesses in the form of concrete steps, standardised forms, and specific timelines.

The European AI Office has indicated a grace period for good faith compliance efforts, reducing immediate enforcement risks for

signatories while providing a framework for demonstrating alignment with regulatory priorities in a rapidly evolving AI environment.

Responses from market participants have been mixed so far. While several major AI companies — including OpenAI, Anthropic and Mistral — have signaled their intention to sign the Code, others, most notably Meta, have explicitly declined, citing concerns over the direction of European AI policy. This divergence of opinion creates immediate competitive tension and regulatory uncertainty that will likely shape the market for years to come.

## Understanding Which Parties the Code Applies To

The Code primarily addresses providers of GPAI models — the companies behind the large language models, image generators, and multimodal systems that have captured public attention and regulatory focus in equal measure over the last few years. These providers include obvious industry players like OpenAI's GPT series and Google's Gemini as well as emerging competitors, but the technical thresholds mean the net is cast wider than many expect.

The framework applies to models that demonstrate “significant generality” and can perform diverse tasks across a range of downstream systems or applications. Models with at least one billion parameters typically meet this threshold, encompassing most commercially significant AI systems currently being developed or deployed.

A crucial distinction emerges for models posing “systemic risk” — typically those requiring  $10^{25}$  floating-point operations in training. These systems face additional safety and security requirements that go beyond basic documentation obligations. The threshold captures most frontier models currently in development, creating a two-tier compliance structure that recognises the heightened risks posed by the most powerful systems.

## Downstream Implications

The Code's influence extends well beyond companies providing their GPAI models directly. Businesses integrating GPAI models into their products and services also face indirect obligations through their supply chain relationships. The framework shapes what they can expect from providers, influences how parties enter into contracts, and creates new considerations around liability allocation and information sharing.

## The Transparency Code: Documentation as Governance

### The Documentation Framework

The core of the Code's transparency requirements is the comprehensive documentation and recordkeeping obligations for GPAI models, which cover the full life cycle from development to deployment. This not only includes basic information like model names and release dates but also detailed technical specifications, training methodologies, and energy consumption data. The framework recognises that transparency serves multiple audiences — including regulators, downstream providers, and the public — with various levels of access for different stakeholders.

Providers must keep documentation current throughout a model's life cycle and retain it for 10 years after a model's withdrawal from the market, creating significant data management obligations for in-scope companies. In essence, the Code's requirements go beyond simply creating documents; they're about building systems and processes that can support accurate, accessible information over extended periods.

### Proportionality and Flexibility

On a practical level, the Code recognises that one size doesn't fit all. Documentation requirements scale with provider size, representing an acknowledgment from the European Commission that startups and small and midsize enterprises can't be

expected to maintain the same comprehensive systems as major technology companies. This proportionate-first approach extends throughout the Code, creating simplified compliance pathways for companies with fewer resources while maintaining core safety and transparency standards in line with regulatory objectives.

The Code also allows flexibility for companies to make strategic disclosure decisions. While comprehensive information must be available to regulatory authorities upon request, public disclosure remains largely voluntary, enabling companies to balance transparency goals with competitive considerations and intellectual property (IP) protection.

## The Copyright Code: Navigating Rights and Innovation

The Code's copyright chapter addresses one of the most contentious issues in AI development: the relationship between training data acquisition and IP rights. Rather than prescribing specific technical solutions, the framework establishes principles-based obligations that companies must implement according to their specific circumstances.

## Policy Development and Implementation

Signatories must establish comprehensive copyright policies addressing EU copyright law compliance throughout the life cycle of an AI model. The key point here is that this obligation requires more than a simple box-checking exercise by in-scope companies. Instead, compliance will require active policy development, regular updates, and practical implementation across all aspects of model development and deployment. Companies are encouraged to publish policy summaries, promoting transparency while protecting sensitive operational details.

## Data Acquisition Standards

The Code also establishes clear boundaries around data acquisition practices. For example, web crawling must respect technological measures, including paywalls and subscription models, designed to restrict access to copyrighted works, and companies must exclude websites that are recognised by EU authorities as persistent copyright infringers from their web crawling activities. The AI Office will maintain dynamic lists of problematic sites to reduce compliance uncertainty while protecting rightsholders.

Perhaps most significantly, the Code requires compliance with machine-readable opt-outs, primarily through the robots.txt protocol. This creates immediate operational obligations for companies using web crawling for training data acquisition, requiring technical systems that can identify and respect rights reservations.

## Output Protection and Stakeholder Engagement

The Code additionally requires technical safeguards against copyright infringement in model outputs, though it stops short of prescribing specific technologies. This reflects the EU's recognition that technical solutions are evolving alongside AI capabilities, while maintaining the European Commission's core IP protection objectives.

Companies must also establish processes for engagement with rightsholders, including providing designated contact points and complaint mechanisms.

## The Safety and Security Code: Managing Systemic Risks

The safety and security chapter represents what may be considered among the most ambitious components of the Code, establishing a comprehensive framework for identifying, assessing, and mitigating systemic risks posed by the most powerful AI systems.

## Risk Management Frameworks

Companies developing models with systemic risk must establish a safety and security framework — a risk management protocol that documents how they will approach and mitigate potential harms throughout a model's life cycle. This framework must define trigger points for additional evaluations, establish risk acceptance criteria, and clearly assign responsibilities across organisational levels.

This framework-based approach recognises that effective risk management requires systematic processes rather than ad hoc responses. Companies must build capabilities for ongoing risk assessment, including both lighter-touch evaluations during development and comprehensive assessments before market placement.

## Assessment and Monitoring Requirements

The Code requires companies to systematically identify potential systemic risks through structured analysis of risk sources against model characteristics. This includes consideration of capabilities that could enable chemical or biological weapons development, loss of control scenarios, and cyber offence capabilities.

Post-market monitoring is also an essential consideration, requiring companies to gather information about real-world model performance through user feedback, incident reports, and usage pattern analysis.

## External Evaluation

Perhaps most significantly, the Code generally requires independent external evaluation of systemic risk models. Companies must provide evaluators with adequate access to model capabilities and reasoning processes while maintaining appropriate security protections. This creates new relationships and obligations that extend beyond traditional corporate and commercial norms.

## Incident Reporting and Transparency

The Code establishes strict incident reporting timelines ranging from two days for critical infrastructure disruption to 15 days for serious health, rights, or environmental harm. Reports must include root cause analysis and recommended responses, creating significant operational obligations for incident detection, analysis, and communication.

## Implementation Realities: Building Compliance Capabilities

### Resource Requirements and Organisational Change

Implementing the Code requires significant resource allocation across multiple dimensions. Companies need technical expertise for risk assessment and monitoring, legal capabilities for copyright compliance, and operational systems for documentation and reporting. However, successful implementation also requires a broader organisational culture change, particularly around risk management and transparency. The Code emphasises healthy risk culture development, requiring leadership commitment, clear communication channels, and appropriate incentives for staff to raise safety concerns.

## Transatlantic Policy Distinctions: Navigating Global Approaches

The European Commission published the Code at an interesting time for global AI policy given the release of the Trump administration's AI Action Plan. While the US approach seeks to prioritise innovation, speed, and global competitiveness through deregulation and competitive positioning, parallels can be drawn in that both Europe and the US focus on governance and comprehensive risk management, albeit the Code takes a more prescriptive approach. Read our alert on the AI Action Plan's explicit and inherent support for governance and risk management.

The extraterritorial reach of the European approach means that even companies primarily focused on other markets may need

to consider Code compliance if they have a European market presence. While the US emphasis on reducing regulatory burden may create competitive advantages for companies that can avoid European-style requirements, a common baseline across both approaches is found in governance and risk management. For global businesses, this requires sophisticated strategies that can navigate different frameworks while maintaining operational efficiency and competitive positioning across jurisdictions.

## Looking Ahead: Navigating Uncertainty and Opportunity

### Regulatory Evolution and Enforcement

The AI regulatory landscape is evolving rapidly, with the European Commission developing supplementary guidance and the AI Office already preparing for enforcement responsibilities. We anticipate that early enforcement actions will signal regulatory expectations and shape market behaviour, making early positioning decisions increasingly important.

From a technological perspective, AI capabilities continue to advance at an unprecedented pace, with the potential to outstrip current frameworks. The coming wave of emerging technologies (including quantum computing, neuromorphic systems, and advanced robotics) compound the issue for market participants, necessitating new approaches to governance and compliance that current frameworks can't address.

The Code's principles-based approach provides some flexibility for technological evolution, but companies must build adaptive capabilities, rather than point solutions, that can respond to changing requirements and emerging risks. When so much around the future of AI is uncertain, successful implementation requires balancing innovation momentum with regulatory compliance and stakeholder expectations. From this perspective, horizon scanning for regulatory developments is crucial, and in-scope organisations stand to gain a significant competitive advantage from developing relationships with regulators and industry associations in an increasingly complex compliance environment.

*We would like to thank Elliot Luke for their assistance with this alert.*

This informational piece, which may be considered advertising under the ethical rules of certain jurisdictions, is provided on the understanding that it does not constitute the rendering of legal advice or other professional advice by Goodwin or its lawyers. Prior results do not guarantee similar outcomes.

## CONTACTS

### Kaitlin Betancourt

Partner

kbetancourt@goodwinlaw.com  
New York | +1 212 813 8936

### Gretchen Scott

Partner

gscott@goodwinlaw.com  
London | +44 (0)20 7447 4292

### Joseph Ndep

Associate

jndep@goodwinlaw.com  
London | +44 (0)20 7681 1529

