AI & Partners

Amsterdam - London - Singapore

EU AI Act

General-Purpose AI Code of Practice

Commitment Areas

February 2025

AI & Partners

AI & Partners

Amsterdam - London - Singapore

AI & Partners defends and extends the digital rights of users at risk around the world. By combining direct technical support, comprehensive policy engagement, global advocacy, grassroots professional services, regulatory interventions, and participating in industry groups such as AI Commons, we fight for fundamental rights in the artificial intelligence age.

This report was prepared by Sean Donald John Musch and Michael Charles Borrelli. For more information visit https://www.ai-and-partners.com/. All predictions, suggestions, analysis, projections, indications, and other material have been prepared on a 'best-efforts' basis.

Contact: Michael Charles Borrelli | Director | m.borrelli@ai-and-partners.com.

This report is an AI & Partners publication.

Contents

Introduction

The **General-Purpose AI Code of Practice (GPAI CoP)** establishes a structured approach for addressing the governance, transparency, and risk management challenges associated with general-purpose AI models. As AI systems become more advanced and widely adopted, ensuring responsible development and deployment is critical for both **upstream providers**—who build and refine these models—and **downstream companies**—who integrate them into end-user applications.

This report examines the commitments outlined in the GPAI CoP and their implications across the AI ecosystem. It focuses on how **upstream model providers** must comply with requirements related to **transparency, copyright, systemic risk management, and governance**. Additionally, it explores how **downstream organizations** are affected by these commitments, particularly in areas such as **AI safety, regulatory compliance, and operational risk mitigation**.

By analyzing each section of the GPAI CoP, this report provides **key insights into compliance obligations, best practices, and emerging challenges**. The findings draw on the expertise of **AI & Partners' specialists**, whose experience across global AI governance initiatives informs this assessment.

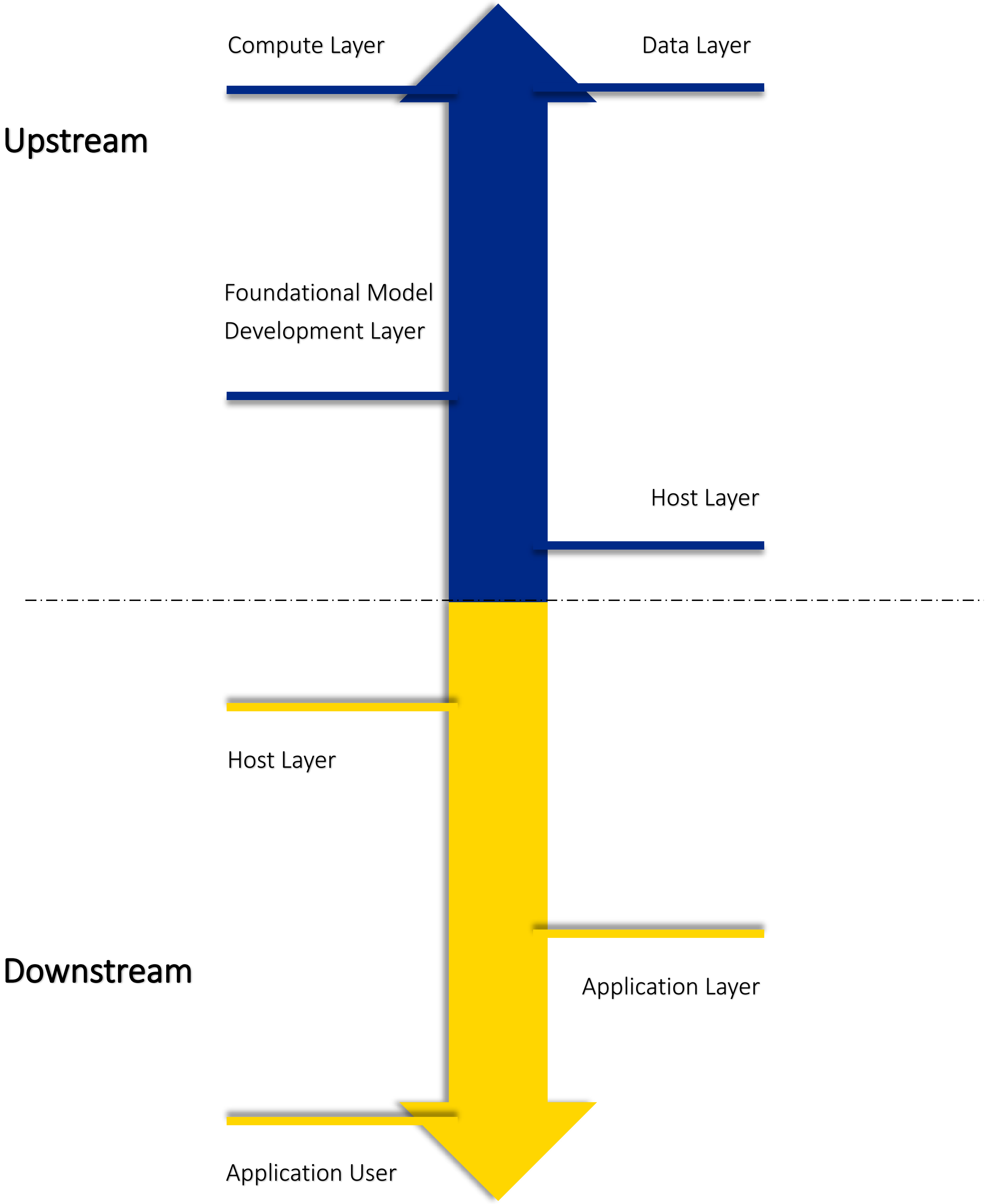
As regulatory frameworks, including the **EU AI Act**, continue to evolve, understanding the **supervisory responsibilities and technical safeguards required under the GPAI CoP** will be essential for organizations across industries. This report aims to equip stakeholders with **practical guidance on navigating these commitments**, fostering a responsible and legally compliant AI ecosystem.

Best regards,

Sean Musch

Founder/CEO

AI & Partners



Compute Layer

Data Layer

Upstream

Foundational Model Development Layer

Host Layer

Host Layer

Downstream

Application Layer

Application User

Frequently asked questions being asked about the General-Purpose AI Code of Practice

Why Are Regulations Necessary for General-Purpose AI Models?

Artificial intelligence has the potential to significantly benefit both society and the economy. General-purpose AI models are particularly crucial in this context, as they serve multiple functions and form the foundation for numerous AI applications used globally, including within Europe.

The AI Act seeks to ensure that general-purpose AI models are both secure and reliable.

To achieve this goal, it is essential that providers of general-purpose AI models possess a thorough understanding of their models throughout the AI value chain. This knowledge enables proper integration into downstream AI systems while also ensuring compliance with the AI Act. Specifically, providers must create and share technical documentation with the AI Office and downstream users, establish a copyright policy, and publish an overview of the training data. Additionally, providers whose models present systemic risks—either due to their advanced capabilities or their significant impact on the market—must inform the European Commission, evaluate and mitigate systemic risks, conduct model assessments, report major incidents, and maintain cybersecurity measures.

As a result of implementing these measures, the AI Act fosters innovation while ensuring safety and trustworthiness in AI development within Europe.

How are General-Purpose AI Models Defined?

According to the AI Act, a general-purpose AI model is one trained on extensive data, often using large-scale self-supervision, and capable of performing a broad range of tasks effectively, irrespective of its market placement. These models can integrate into various downstream applications and systems (Article 3(63)).

Further clarification is provided in Recital 98, which suggests that models trained with at least a billion parameters and substantial data at scale should be considered to exhibit broad generality. Recital 99 highlights that large generative AI models exemplify general-purpose AI models, given their ability to produce text, audio, images, and video across multiple applications.

Even within a single modality, such as text, audio, or visual data, a model can demonstrate broad functionality if its capabilities are sufficiently versatile. Models that have undergone fine-tuning or modifications to enhance performance for specific tasks may also meet these criteria. The AI Office, in collaboration with the Commission's Joint Research Centre, is working on further clarifications regarding what qualifies as a general-purpose AI model.

What are General-Purpose AI Models with Systemic Risk?

Systemic risks refer to large-scale threats arising from cutting-edge AI models or other models with a comparable impact (Article 3(65)). These risks may include facilitating the creation of harmful substances, loss of control over autonomous AI systems, or widespread misinformation and discrimination (Recital 110). Highly advanced models, as well as some models with significant reach and scalability, could present such risks.

The AI Act categorizes an AI model as posing systemic risk if it is one of the most advanced at a given time or has an equivalent impact (Article 51(1)). This classification is subject to change as technology evolves and society adapts.

To define the most advanced models, the AI Act establishes an initial benchmark of 10^25 floating-point operations (FLOP) for training (Article 51(1)(a) and (2)), a process estimated to cost tens of millions of euros. The AI Office will monitor industry developments, and the Commission may adjust this threshold through delegated acts (Article 51(3)). Furthermore, models that do not meet this threshold but have a significant impact—determined by factors such as user base, scalability, and access to key tools—may also be classified as posing systemic risk (Article 51(1)(b), Annex XIII).

The AI Office will provide additional guidance on this classification based on research from the Joint Research Centre.

Who Qualifies as a Provider of General-Purpose AI Models?

The AI Act's regulations apply to any entity placing general-purpose AI models on the European market, regardless of whether they are based within the EU or abroad (Article 2(1)(a)).

A provider is defined as any individual, organization, public authority, or agency that develops or commissions the development of a general-purpose AI model and makes it available, whether commercially or free of charge (Article 3(3)).

Placing a model on the market entails making it accessible in the EU for commercial use (Article 3(9) and (10)). Even if a provider integrates the AI model into their own system before public release, it is still considered placed on the market unless its use is strictly internal and does not impact individuals' rights or pose systemic risks (Recital 97).

What are the Provider Obligations Under the AI Act?

Starting August 2, 2025, providers of general-purpose AI models must comply with the AI Act (Article 113(b)). For models introduced before this date, transitional rules apply (Article 111(3)).

Providers must:

- Document technical details and share them with the AI Office and relevant authorities (Article 53(1)(a)).
- Provide information to downstream users (Article 53(1)(b)).
- Establish a policy ensuring compliance with copyright laws (Article 53(1)(c)).
- Publish a detailed summary of training data used (Article 53(1)(d)).

The General-Purpose AI Code of Practice will offer further guidance on transparency and copyright obligations (Working Group 1).

Providers of AI models with systemic risk have additional responsibilities under Article 55, including assessing and mitigating risks, conducting evaluations, tracking and reporting incidents, and ensuring cybersecurity.

The Code of Practice will also elaborate on these obligations through working groups dedicated to systemic risk assessment, technical mitigation, and governance (Working Groups 2, 3, and 4).

How does this Affect Open-Source AI Models?

Certain obligations do not apply to open-source models if their parameters, including weights, architecture details, and usage guidelines, are publicly accessible. However, this exemption does not extend to models classified as posing systemic risk (Article 53(2)).

Regardless of open-sourcing, providers of systemic risk models must adhere to AI Act obligations. Since risk mitigation becomes more challenging after an open-source release, providers should evaluate risks before publishing their models (Recital 112).

The General-Purpose AI Code of Practice will address compliance requirements for open-source models.

What is the General-Purpose AI Code of Practice?

The AI Act mandates a General-Purpose AI Code of Practice to clarify how providers can meet regulatory requirements (Article 56). Facilitated by the AI Office, this initiative includes input from nearly 1,000 stakeholders, member states, and international observers.

The Code will define best practices for compliance with obligations in Articles 53 and 55, including notification requirements for providers whose models meet systemic risk criteria (Article 52(1)).

While the Code provides implementation guidance, it does not modify legal definitions or enforcement mechanisms, which remain under the AI Office's authority.

What are the Enforcement and Legal Implications?

The AI Office oversees compliance with provider obligations (Article 88) and supports national regulators in enforcing AI system requirements (Article 75). The Office has authority to:

- Request information (Article 91).
- Conduct model evaluations (Article 92).
- Require providers to implement risk mitigations or withdraw models from the market (Article 93).
- Impose fines up to 3% of global annual revenue or 15 million euros (whichever is higher) (Article 101).

Once finalized and approved via an implementing act, the Code of Practice will serve as a compliance benchmark under the AI Act, although alternative compliance pathways will remain available.

The Code will also be subject to periodic updates, reflecting technological and regulatory developments.

EUROPEAN ARTIFICIAL INTELLIGENCE OFFICE

Commitments by Providers of General-Purpose AI Models

Transparency

Upstream

GPAI model providers must comply with the **EU AI Act** and the **General-Purpose AI Code of Practice** by prioritizing transparency, accountability, and regulatory adherence. This entails documenting and disclosing essential details about their models, including:

- **Training data sources** to provide insight into provenance and potential biases.
- **Intended uses and limitations** to prevent misuse and ensure responsible deployment.
- **Performance evaluations** to demonstrate compliance with risk management frameworks.

Transparency commitments are critical in **ensuring regulatory compliance and mitigating AI-related risks**, particularly those linked to misinformation, bias, and systemic vulnerabilities. By maintaining **comprehensive and up-to-date technical documentation**, upstream providers enable downstream developers to integrate GPAI models responsibly while establishing a **clear chain of accountability**.

However, these commitments present **operational and competitive challenges**. Striking a balance between transparency and **intellectual property protection** remains a key concern, as excessive disclosure could compromise proprietary AI technologies. At the same time, compliance requirements—such as model explainability and risk classification—can be **resource-intensive, particularly for smaller AI developers**.

Despite these challenges, robust transparency practices **enhance market credibility**. Companies that proactively adhere to rigorous documentation and reporting standards **gain a trust advantage**, fostering stronger relationships with regulators, customers, and AI ecosystem partners.

Companies leveraging GPAI models in end-user applications **rely on upstream transparency commitments** to ensure safe, lawful, and ethical AI deployments. **Clear, structured model documentation** is essential for downstream AI developers to:

- **Understand model capabilities and limitations** to avoid unintended consequences.
- **Identify potential biases and risks** that could affect AI-driven decision-making.
- **Ensure compliance with AI Act obligations**, particularly in high-risk applications.

Inadequate documentation from upstream providers exposes downstream companies to **operational, legal, and reputational risks**. **Unexpected model behaviour, regulatory non-compliance, and liability concerns** may arise if AI provenance, risk factors, or intended use cases are unclear. This is particularly crucial for **high-risk sectors**, such as **healthcare, finance, and law enforcement**, where AI-driven errors can have severe consequences.

However, transparency obligations also introduce **compliance burdens** for downstream users. If documentation is overly **technical, inconsistent, or insufficiently standardized**, smaller firms and non-technical teams may struggle to interpret AI model constraints, leading to potential **misuse.**

By **prioritizing transparency and compliance**, downstream companies can **build trust, mitigate risks, and strengthen their position** in an increasingly regulated AI landscape.

Downstream

Copyright

Upstream

General-Purpose AI (GPAI) model providers must comply with **copyright policies under the EU AI Act** and the **General-Purpose AI Code of Practice**, ensuring their training data respects **intellectual property (IP) rights**. These obligations align with **Directive (EU) 2019/790**, which governs copyright in the digital single market, requiring providers to::

- **Identify and document training data sources** to verify compliance with copyright laws.
- **Ensure proper licensing agreements** for copyrighted materials incorporated into AI models.
- **Implement opt-out mechanisms** that allow rightsholders to exclude their content from AI training datasets.
- **Disclose whether copyrighted materials were used in training** and provide transparency in model provenance.

While these commitments enhance **trust and accountability**, they introduce **significant challenges** for upstream providers. Balancing **transparency with trade secret protection** is complex, as excessive disclosure may expose proprietary methods to competitors. Additionally, **copyright compliance varies across jurisdictions**, requiring **legal adaptability** and investment in **automated rights management technologies**.

Copyright constraints can also **affect model performance**, as access to high-quality, diverse training data may become restricted. However, **proactively addressing copyright concerns**—such as by adopting robust **data governance frameworks** and collaborating with rightsholders—can help GPAI providers **build trust with regulators, reduce litigation risks, and strengthen their market position**.

Downstream

Downstream companies that **deploy GPAI models** in end-user applications must ensure **compliance with copyright laws** to avoid unintended infringement. **Transparency from upstream providers** is critical in determining whether AI-generated outputs adhere to **intellectual property regulations**. Companies in sectors such as **media, advertising, publishing, and content creation** must take extra precautions to:

- **Verify the copyright status of AI-generated content** before commercial use.
- **Confirm that upstream models adhere to licensing agreements** and rights reservations.
- **Implement safeguards** to prevent end-users from generating infringing content.

However, copyright compliance poses **operational and financial burdens** for downstream companies. If **training data documentation from upstream providers is insufficient**, businesses may need to **conduct independent due diligence**, increasing **legal costs and complexity**. Moreover, **uncertainty around copyright ownership of AI-generated content** may require companies to **adapt business models**, incorporating **licensing fees or content restrictions** to mitigate risks.

For **creative industries**, these policies introduce both **risks and opportunities**. While licensing costs and legal constraints may **limit automation-driven efficiencies**, businesses that **proactively establish AI copyright compliance frameworks** will gain a **competitive advantage**, ensuring long-term viability in an increasingly regulated market.

Commitments by Providers of General-Purpose AI Models With Systemic Risk

Framework

Upstream

Providers of **GPAI models classified as having systemic risk** under the **EU AI Act** must adhere to **Commitments 3-6** of the **General-Purpose AI Code of Practice**. These commitments concern:

- **Risk taxonomy development** to categorize and assess potential threats posed by AI models.
- **Implementation of safety frameworks** to minimize unintended harmful consequences.
- **Comprehensive model reporting** to ensure transparency in AI operations.

To comply, upstream providers must engage in **continuous risk assessment, adversarial testing, and extensive documentation** of systemic risks. This includes monitoring **cybersecurity threats, large-scale misinformation risks, and AI misuse in critical applications** such as defence, finance, and public services.

However, these obligations introduce **significant regulatory and operational challenges**. Providers must **balance innovation with compliance**, as overly restrictive regulations may **slow AI advancements**, while insufficient oversight could **expose them to severe legal liabilities**. Additionally, systemic risk frameworks often require **collaboration with regulators, independent auditors, and third-party assessors**, increasing both **compliance costs and administrative burdens**.

Despite these challenges, **proactively managing systemic risks** strengthens market credibility and regulatory trust. Companies that invest in **robust AI safety measures, risk mitigation strategies, and transparent compliance reporting** will be better positioned to navigate the evolving AI regulatory landscape while fostering public confidence in their technologies.

Downstream companies deploying **General-Purpose AI models with systemic risk** into end-user applications must **navigate complex compliance challenges** to ensure responsible AI usage. Commitments **3-6** of the **General-Purpose AI Code of Practice** require them to:

- **Understand and assess AI-driven risks** associated with deployed models.
- **Implement mitigation strategies** to prevent algorithmic bias, cybersecurity vulnerabilities, and misuse.
- **Ensure compliance with regulatory and industry-specific guidelines** to minimize liability.

A key challenge for downstream companies is **their reliance on upstream providers** for accurate risk disclosures and compliance documentation. If transparency is lacking, **legal uncertainties and operational risks** may arise, potentially leading to **regulatory fines, reputational damage, and ethical concerns**.

However, systemic risk management demands **significant resources**. Companies may need to **create new compliance functions, hire AI risk specialists, and integrate risk mitigation tools** into existing workflows. This poses **a substantial burden on SMEs and startups**, which may lack the necessary expertise and funding to meet stringent AI compliance requirements.

In proactively **managing AI risks and regulatory obligations**, downstream companies can **enhance trust, reduce liability, and strengthen their ability to deploy AI models responsibly** in an increasingly regulated environment.

Downstream

Risk Assessment

Upstream

Under **Commitments 7-10** of the **General-Purpose AI Code of Practice**, upstream providers of **General-Purpose AI (GPAI) models with systemic risk** must establish robust **risk identification, analysis, evaluation, and evidence collection** frameworks. These commitments require providers to systematically assess and document risks related to:

- **Capability-based threats** (e.g., autonomous adaptation and self-learning risks).
- **Deployment vulnerabilities** (e.g., cybersecurity threats, adversarial attacks).
- **Societal risks** (e.g., misinformation, discrimination, and public safety concerns).

To comply, upstream providers must develop **structured risk identification frameworks**, categorizing risks based on **severity, likelihood, and potential harm**. This includes conducting:

- **Comprehensive risk analyses** to evaluate potential model misuse and unintended consequences.
- **Ongoing risk evaluations** to determine whether mitigation measures are sufficient or need improvement.

Compliance with these commitments may require partnerships with **third-party assessors, regulatory agencies, and AI governance bodies**, increasing both **costs and development timelines**. However, **proactively investing in risk management** strengthens regulatory trust, reduces liability exposure, and enhances the overall **safety and reliability of AI deployments**.

For **downstream companies integrating GPAI models with systemic risk**, **Commitments 7-10** serve as critical **compliance guardrails**, ensuring AI deployments are **safe, transparent, and accountable**. These commitments influence how companies:

- **Identify and assess AI-related risks** before implementation.
- **Mitigate biases, security vulnerabilities, and systemic failures.**
- **Document and report risk management efforts** to regulators and stakeholders.

A primary challenge for downstream users is **dependency on upstream providers** for accurate and comprehensive risk disclosures. If upstream documentation is **incomplete, overly technical, or inconsistent**, companies may struggle to:

- **Evaluate model reliability** and its suitability for high-stakes applications.
- **Ensure compliance with sector-specific regulations**, particularly in **finance, healthcare, and critical infrastructure**.

To meet risk assessment requirements, downstream companies should integrate **AI-specific governance frameworks** into their compliance processes Additionally, downstream companies may be required to **document their own risk evaluations and mitigation actions**, which could **increase operational burdens**—particularly for SMEs with limited compliance resources.

Downstream

Technical Risk Mitigation

Upstream

Under **Commitments 11-13** of the **General-Purpose AI Code of Practice**, upstream providers of **GPAI models classified as having systemic risk** must implement **comprehensive technical risk mitigation strategies**. These require, at the minimum:

- **Safety mitigations** (Commitment 11) to prevent unintended model behaviours and misuse.
- **Security mitigations** (Commitment 12) to protect against cyber threats and adversarial attacks.

To comply, upstream providers must adopt **state-of-the-art security and safety measures** that:

- **Harden AI models against adversarial manipulation and cyber threats.**
- **Enhance model robustness** to minimize vulnerabilities in high-risk applications.

However, these obligations introduce **significant technical and operational costs**. Ensuring compliance may necessitate:

- **Advanced testing infrastructures** to assess model vulnerabilities.
- **Dedicated security teams** to monitor AI integrity and performance.

For providers of **open-source or widely distributed AI models**, enforcing **security safeguards** is particularly challenging, as they have **limited control over how their models are fine-tuned or deployed downstream**. Nonetheless, **proactively addressing security and safety risks** will help providers build **trust with regulators, and reduce legal exposure.**

Downstream companies integrating **GPAI models with systemic risk** must ensure that **upstream safety and security measures** align with their specific **regulatory and operational needs**. **Commitments 11-13** influence how companies:

- **Evaluate AI reliability and security before deployment.**
- **Protect sensitive user data and ensure AI integrity.**
- **Mitigate operational risks linked to adversarial threats and misuse.**

A major challenge for downstream users is **understanding and implementing upstream security safeguards**. If AI providers do not offer **clear, standardized documentation**, companies may struggle to:

- **Assess risks and identify security vulnerabilities.**
- **Ensure compliance with industry and regulatory frameworks.**
- **Implement appropriate safety measures for high-stakes applications.**

To meet compliance expectations, downstream businesses must establish **AI security protocols** that may include:

- **Independent security audits** to verify AI safety before deployment.
- **Adversarial testing** to assess the resilience of AI models against external threats.

Despite these challenges, **investing in robust safety and security practices** offers a **competitive advantage**.

Downstream

Governance Risk Mitigation

Upstream

Commitments 14-21 of the General-Purpose AI Code of Practice focus on governance risk mitigation for providers of GPAI models with systemic risk. These commitments establish key accountability mechanisms, including internal governance structures (Commitment 14), adherence to risk frameworks (Commitment 15), external assessments (Commitment 16), serious incident reporting (Commitment 17), whistleblower protections (Commitment 18), regulatory notifications (Commitment 19), documentation (Commitment 20), and public transparency (Commitment 21).

To comply, GPAI providers must implement structured governance frameworks that clearly assign responsibility for systemic risk management within their organizations. They must also conduct continuous risk assessments, maintain detailed documentation, and demonstrate compliance with evolving regulations. External audits and serious incident reporting require providers to engage proactively with regulators and third-party assessors whenever significant AI risks arise, ensuring greater oversight and accountability.

Key considerations for upstream providers:

- Internal Accountability: Organizations must designate responsible teams or executives for systemic risk governance.
- Proactive Risk Management: Regular external audits and third-party assessments help validate risk mitigation efforts.

These commitments introduce complex operational and regulatory challenges for AI developers. Establishing governance structures requires legal expertise, cross-functional collaboration, and ongoing risk monitoring to ensure alignment with regulatory expectations.

For downstream companies, Commitments 14-21 shape compliance expectations for AI-integrated applications, emphasizing governance, transparency, and risk mitigation. These commitments mandate that organizations actively monitor AI behaviour, document risk management efforts, and engage with regulators in the event of AI-related incidents.

A critical challenge for downstream organizations is their reliance on upstream providers for detailed risk disclosures, external audits, and compliance documentation. If GPAI model providers fail to provide transparent governance structures and risk assessments, downstream companies may struggle to assess AI-related risks, increasing their exposure to regulatory penalties, legal liabilities, and reputational harm.

Key considerations for downstream companies:

- Dependence on Upstream Providers: Organizations must ensure they receive comprehensive risk documentation and compliance disclosures from GPAI providers.
- Sector-Specific Compliance Needs: Companies in regulated industries must implement AI risk management frameworks tailored to legal and ethical requirements.

To mitigate these risks, downstream users must implement internal AI governance policies that align with sector-specific compliance requirements. This includes adopting AI risk management frameworks, establishing serious incident reporting mechanisms, and ensuring whistleblower protections for employees.

Downstream

Calls to action

Upstream

Enhance Transparency and Documentation

Ensure all AI models include clear, standardized documentation covering training data sources, model capabilities, limitations, and intended use cases. This will help downstream providers comply with the EU AI Act and mitigate risks related to misinformation, bias, and misuse.

Implement Robust Risk Assessment Frameworks

Adopt and continuously refine systemic risk identification and mitigation strategies, including adversarial testing, red-teaming, and bias detection. Proactively engage with regulators to demonstrate compliance with evolving AI safety standards.

Strengthen Security and Copyright Compliance

Integrate safeguards against intellectual property infringement, data leakage, and adversarial manipulation.

Collaborate with Regulators and Industry Stakeholders

Engage in proactive discussions with regulatory bodies, civil society, and industry partners to shape best practices for AI governance.

Support Downstream Users with Compliance Resources

Provide user-friendly compliance tools, API-level risk disclosures, and technical support to help downstream companies navigate regulatory challenges. Offer educational materials and best-practice guidelines tailored to SMEs and high-risk sectors.

Downstream

Conduct Comprehensive AI Risk Assessments

Evaluate the risks associated with deployed AI models, including potential biases, security vulnerabilities, and regulatory obligations. Establish internal AI governance frameworks that align with industry and legal standards.

Demand Transparency from Upstream Providers

Require detailed technical documentation, risk disclosures, and regulatory compliance assurances from AI model providers. Ensure that upstream partners adhere to ethical AI commitments before integrating their models into business applications.

Develop AI Literacy and Compliance Strategies

Train employees on AI-related risks, regulatory obligations, and ethical considerations.

Monitor and Report AI-Related Incidents

Establish processes for tracking AI-driven decisions, flagging anomalies, and reporting compliance breaches.

Adopt Ethical AI Practices for Competitive Advantage

Differentiate by embedding fairness, accountability, and transparency into AI applications. Companies that prioritize responsible AI development will gain trust from consumers, regulators, and business partners, strengthening their market position.

Conclusion

The implementation of both the EU AI Act and the General-Purpose AI Code of Practice marks a significant milestone in the regulation of artificial intelligence, setting a precedent for responsible AI governance worldwide. As organizations and policymakers navigate this evolving landscape, the past six months have demonstrated both the challenges and opportunities that arise from enforcing a comprehensive regulatory framework.

One of the key takeaways from the Act's early implementation is the importance of adaptability. While the regulations establish clear guidelines for AI developers, businesses, and governments, real-world application has highlighted the need for continuous dialogue between regulators, industry stakeholders, and civil society. The ability to adjust enforcement mechanisms, provide targeted support for SMEs, and streamline compliance processes will be critical to ensuring the Act's long-term success.

Transparency and accountability have emerged as central themes in AI governance. The commitment areas outlined in the Code of Practice emphasize the role of AI providers in maintaining clear documentation, mitigating systemic risks, and fostering ethical AI use. These principles are not only regulatory necessities but also crucial drivers of public trust in AI-driven technologies. Companies that prioritize compliance and responsible AI practices will likely benefit from greater consumer confidence and market credibility.

However, the Act's implementation has also underscored the difficulties in harmonizing AI regulations across different sectors and Member States. Variability in national enforcement strategies, resource constraints among regulators, and the evolving nature of AI technology pose ongoing challenges. Addressing these concerns will require enhanced collaboration, standardized compliance mechanisms, and proactive engagement from all stakeholders.

Looking ahead, the success of the EU AI Act will depend on a balanced approach that fosters both innovation and regulatory oversight. As AI continues to shape industries such as healthcare, finance, and public administration, ensuring that ethical considerations remain at the forefront will be crucial. The lessons learned from early adoption will serve as a foundation for refining AI governance models, both within the EU and globally.

Ultimately, the EU AI Act and the Code of Practice present a landmark opportunity to align technological progress with societal values. Working together it is possible to embrace a future where AI is transparent, accountable, and beneficial to all, policymakers, businesses, and communities can collectively shape a responsible and sustainable AI ecosystem.

About AI & Partners

AI & Partners – 'AI That You Can Trust'

At AI & Partners, we're here to help you navigate the complexities of the EU AI Act, so you can focus on what matters—using AI to grow your business. We specialize in guiding companies through compliance with tailored solutions that fit your needs. Why us? Because we combine deep AI expertise with practical, actionable strategies to ensure you stay compliant and responsible, without losing sight of your goals. With our support, you get AI you can trust—safe, accountable, and aligned with the law.

To find out how we can help you, email contact@ai-and-partners.com or visit https://www.ai-and-partners.com.

Contacts

Sean Donald John Musch, CEO/Founder, s.musch@ai-and-partners.com

Michael Charles Borrelli, Director, m.borrelli@ai-and-partners.com

Authors

Sean Donald John Musch, CEO/Founder

Michael Charles Borrelli, Director

References

European Parliament and The Council of the European Union, (2024), 2024/1689 Regulation (EU) 2024/1689 of the European Parliament and of The Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), accessible at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401689 (last accessed 15th February 2025)

EU Artificial Intelligence Act, (2024), 'The EU Artificial Intelligence Act: Up-to-date developments and analyses of the EU AI Act', accessible at: https://artificialintelligenceact.eu/ (last accessed 15th February 2025)

European Commission, (2025), 'General-Purpose AI Code of Practice', accessible at: https://digital-strategy.ec.europa.eu/en/policies/ai-code-practice (last accessed 15th February 2025)

Important notice

This document has been prepared by AI & Partners B.V. for the sole purpose of enabling the parties to whom it is addressed to evaluate the capabilities of AI & Partners B.V. to supply the proposed services.

Other than as stated below, this document and its contents are confidential and prepared solely for your information, and may not be reproduced, redistributed or passed on to any other person in whole or in part. If this document contains details of an arrangement that could result in a tax or National Insurance saving, no such conditions of confidentiality apply to the details of that arrangement (for example, for the purpose of discussion with tax authorities). No other party is entitled to rely on this document for any purpose whatsoever and we accept no liability to any other party who is shown or obtains access to this document.

This document is not an offer and is not intended to be contractually binding. Should this proposal be acceptable to you, and following the conclusion of our internal acceptance procedures, we would be pleased to discuss terms and conditions with you prior to our appointment. Images used throughout the document have either been produced in-house or sourced from publicly available sources (see **References** for details).

AI & Partners B.V. is the Dutch headquarters of AI & Partners, a global professional services firm. Please see https://www.ai-and-partners.com/ to learn more about us.

Designed and produced by AI & Partners B.V.