Key Issue: The Code of Practice for GPAI Providers (Code), intended to streamline compliance with the AI Act, risks making overly prescriptive, unnecessary and possibly dangerous rules. This will hamper Europe's ability to innovate and grow through the adoption of AI tools.

Background: The Code was called for in the AI Act to provide a mechanism for providers of General Purpose AI models to demonstrate compliance with the AIA. The Code is being developed under the auspices of the AI Office in the European Commission through a series of working groups led by members of civil society. The drafters of the code published the second of four expected drafts in December and the Code should be finalized by April ahead of a compliance deadline in August.

There are significant and serious concerns that the current draft of the Code will limit the ability to develop and deploy AI in Europe. The Code was envisioned as a means of compliance with the AI Act. However, it demonstrates a continued attempt to introduce compliance obligations that go far beyond what was called for in the AI Act including ideas that were debated and rejected during the legislative process. This includes disproportionate disclosure of proprietary information and the imposition of legally and technically unsound safety requirements. This is an unnecessary compliance burden, particularly for sectors that develop or fine-tune models, or already have a comprehensive product safety and approvals regime in place, e.g automotive, manufacturing, chemicals, pharma, banking, insurance, etc.

Scope Creep: The Code significantly exceeds the AI Act's scope and EU copyright law, including measures that lack a legal basis and contradict legislative agreements. Key issues include:

- **Copyright Policy:** The Code mandates compliance with unworkable third-party opt-outs, and unclear due diligence on dataset acquisitions, creating substantial liability risk. Copyright provisions risk applying extraterritorially, causing significant compliance burdens.
- **Risk Assessments:** Mandatory third-party risk assessments contradict the AI Act's risk-based approach, potentially exposing sensitive IP and creating bottlenecks. Independent testing should be preferred. The taxonomy of risks should reflect risks that can be effectively mitigated at the model level to avoid confusion along the AI value chain.

Recommendation: The code should respect the boundaries of the AI Act and copyright law. Provisions should be workable. Opt-outs and due diligence should be subject to 'reasonable efforts'. Extraterritorial effects should be excluded.

Excessive Demands: The Code's disclosure requirements risk breaching IP, trade secrets, and creating security risks. Specific issues include:

- **Model Parameters, compute and energy consumption:** The Code requires granular parameter counts, detailed disclosure of training infrastructure and its energy use. This is disproportionate given the policy objective, and would create security vulnerabilities.
- **Transparency:** Public transparency requirements are excessive, creating security risks and going beyond the AI Act. Reports to be drafted and released every 6

months keeps essential personnel away from core business. Excessive disclosure of proprietary information might lead to economic damage, compromised model integrity as well as cyber and privacy risks.

- **Information on data used for training** is concerningly prescriptive and risks exposing trade secrets and unnecessary burdens (specifics of data licensing agreements, data acquisition and processing, methods for addressing harmful content not just what data was used for training). Potentially including fine-tuning by downstream deployers, and further development of models.
- **Template on training data**: Summary disclosures jeopardize confidential business data and trade secrets (e.g. detailed information on training datasets), model security, and are technically infeasible (previous models' time of data collection).
- **KPI's distracting from innovation and safety:** Excessive demands tie up valuable resources to source, draft and release reports instead of working on core safety and business. The Code prescribes KPIs that set perverse incentives and would distract from real model safety.

Recommendation: Transparency requirements should be proportionate, necessary and bound to an explicit objective in the AI Act. Overarching policy objectives, like trade secret protection, privacy, cyber security and information integrity, need to be referenced and respected throughout. Instead of precise counts, bands or categories are more appropriate to classify models. The template should also respect the boundaries of the AI Act, not jeopardize trade secrets or model safety, and be technically feasible. The KPIs to the objective of safety and transparency, without prescribing how to achieve that.

Economic Risk: These issues risk creating a bureaucratic obstacle, contradicting the Commission's goals of simplifying rules and encouraging innovation. In a time of low productivity growth and declining investment, overly complex regulations will hinder the EU's ability to compete globally and harness the potential of AI.

Recommendation: The Code needs to be significantly revised to align with the AI Act, reduce unnecessary burdens, and foster AI innovation. The AI Office, under the Executive Vice President for Tech Sovereignty, Security and Democracy, is leading the process and is expected to approve the draft Code by late April.