New EU Guidelines Provide Insights On Global AI Regulation

By **Kevin Benedicto** (July 24, 2024)

Kevin Benedicto

On June 3, the European Data Protection Supervisor issued its first guidelines regarding generative artificial intelligence.[1]

These apply to European Union government institutions, pursuant to EU Regulation 2018/1725. This regulation governs the protection of personal data by EU government institutions, bodies, offices and agencies, authorizing the supervisor as the institutions' independent data protection authority.

Although these guidelines apply only to EU governmental bodies, they provide insight into how the supervisor may approach generative AI going forward.

In light of the recently passed EU Artificial Intelligence Act, coming into force in the coming years,[2] and the intensifying global trend toward AI regulation, the guidelines offer a glimpse into what could be the next phase of AI regulation in Europe, the U.K., the U.S. and other regions.

To clarify, generative AI refers to advancements in computer deep learning models that are designed to produce a wide and general variety of outputs, capable of a range of tasks and applications, such as generating text, image or audio.

The most common example of generative AI is large language models that are trained on massive amounts of text data. These can generate natural language responses to a wide range of inputs.[3]

Even as large language models and generative AI have experienced exponential growth, policymakers worldwide have raised questions about the potential risks of the technology and have raced to consider how to regulate them.

Framework and Principles

The guidelines aim to provide practical guidance on generative AI, while emphasizing that EU government institutions must ensure that personal data processing for AI complies with data protection obligations under EU law. The guidelines outline key principles for EU use of generative AI systems.

Trustworthy AI

The guidelines make it clear that EU government institutions are permitted to develop and deploy generative AI systems in their provision of public services. However, when personal data is processed, EU government institutions must comply with applicable EU data protection regulations. The guidelines note that "generative AI systems must be transparent, explainable, consistent, auditable and accessible."[4]

Personal Data Processing

The guidelines warn EU government institutions that generative AI systems ingest copious amounts of data, and that personal data processing can occur at various stages in generative AI deployment. The so-called web scraping technique used by many large language models may collect personal data without individuals' knowledge, and such data would be subject to EU data protection legislation.

The guidelines require EU government institutions to closely scrutinize AI systems that claim not to process personal data before deploying such systems.

Data Protection Officers and Impact Assessments

Even prior to the advent of generative AI, EU regulations required EU government institutions to appoint data protection officers responsible for advising on data protection obligations.

The guidelines hold data protection officers responsible for understanding details about any generative AI systems and advising EU government institutions on their use.

Additionally, the guidelines require EU government institutions to undertake regular and systematic monitoring regarding the risks associated with generative AI systems, including conducting in-depth data protection impact assessments and audits.

Lawful Data Processing

The guidelines remind EU government institutions that EU Regulation 2018/1725 only permits personal data processing if there is a valid legal purpose, such as acting in the public interest or in the exercise of their legal authority.

Obtaining individuals' consent of to allow personal data processing for generative AI purposes can be a legitimate purpose, provided consent is properly acquired.

Data Minimization and Accuracy

The EU has long employed a policy of data minimization, according to the guidelines requiring that personal data processing be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed."[5] The guidelines remind EU government institutions to use "well-structured datasets … that prioritize quality over quantity, following a properly supervised training process, and subject to regular monitoring."

Data accuracy is another key point. According to the guidelines, AI models "are still prone to inaccurate results that can have an impact on individuals' fundamental rights and freedoms," and the guidelines place the responsibility on EU government institutions to assess the data accuracy of any generative AI models they implement.[6]

Transparency and Individual Rights

The guidelines require that EU government institutions implementing generative AI must provide and update individuals with required information under EU regulations when using generative AI systems to process personal data. They must also comply with EU regulations on individual rights, providing individuals with options for access, rectification, erasure, objection and restriction of processing.

Avoiding Bias

Academic studies have shown that generative AI can produce images and text that perpetuate biases related to gender, race, political affiliation and more.[7]

The guidelines acknowledge that "artificial intelligence solutions tend to magnify existing human biases and possibly incorporate new ones, which can create new ethical challenges and legal compliance risks," and they ask EU government institutions to prioritize procedures and best practices to mitigate bias.[8]

Data Security

The guidelines warn EU government institutions to "exercise extreme caution and carry out detailed planning of all aspects related to IT security" given the potential new security risks caused by the implementation and adoption of such a new technology in generative AI.

EU AI Act Looms

The EU AI Act was adopted in May, introducing fresh regulations for all generative AI use in the EU. It is anticipated to be effective by August, with various provisions being fully enforceable within six to 36 months of the effective date.

For example, a ban on AI systems posing so-called unacceptable risks will apply six months after the EU AI Act entry into force, while new AI codes of practice that will bind companies using generative AI in the EU will apply nine months after.

The supervisor is the AI supervisory authority under the EU AI Act and will promulgate guidelines, recommendations and regulations under the act. While the guidelines apply only to EU government institutions and were not issued pursuant to its new authority under the legislation, the same principles will likely be present in future supervisor regulations implementing the act across the EU.

AI Regulations Around the World

Like the supervisor, regulators and policymakers worldwide are grappling with the explosive growth of generative AI and its impact, and are attempting to craft regulations and guidance around its use. A chief concern is balancing the risks and benefits of AI, and the impact that either light or heavy-handed regulation might have on the growing AI industry.

In the U.K., the previous government issued a framework for regulating AI, focusing on the core principles of safety, security and robustness, appropriate transparency and explainability, fairness, accountability and governance, plus contestability and redress.[9]

While the core principles echo that of the guidelines, the U.K. framework takes a decidedly less restrictive approach than the one outlined in the guidelines and the EU AI Act. Instead, it focuses on being proinnovation and foregoes any broad new AI legislation, instead focusing on existing regulations and voluntary measures by AI companies and developers.

By declining to codify the framework into law or to propose comprehensive AI legislation, the U.K. has diverged from the EU approach to AI thus far. It is unclear whether the recent change in the U.K. government will prompt any changes to this view.

Like the U.K., the U.S. lacks comprehensive legislation regulating generative AI, although President Joe Biden has issued a broad executive order on AI that directed a number of government agencies to develop a comprehensive framework on accountability and regulation of AI.[10]

Takeaways and Implications

The rapid expansion of generative AI continues unabated, prompting governments globally to accelerate their efforts to keep pace. The EU has moved quickly with comprehensive AI legislation in the EU AI Act, and with the issuance of its guidelines on

EU government institutions, continues to demonstrate a policy of strong and prescriptive regulation of AI that includes new legislation and a clear focus on individual rights and protections.

The former U.K. government took a divergent approach, favoring the use of existing regulations and voluntary industry compliance to prioritize innovation and investment from AI companies.

The U.S. approach is more fragmented and lands somewhere between the EU and the U.K., with a comprehensive executive order and some prescriptive state-level laws but no national legislation. Other countries are charting their paths as well.

With rapidly evolving changes, lawyers advising clients in the generative AI space and across industries making use of generative AI need to prepare accordingly. Compliance with data protection and regulatory requirements is more important than ever, and extra caution should be exercised when generative AI is being developed and used.

Organizations utilizing third-party generative AI services or models that handle personal data need to meticulously evaluate and demand transparency regarding the specifics of these systems. This is crucial, as regulatory entities, particularly within regions such as the EU, will hold organizations accountable for issues related to their use of generative AI.

Emerging technologies like AI present significant potential benefits, but also new risks as companies seek to comply with forthcoming regulations.

Kevin Benedicto is counsel at Redgrave LLP.

[1] https://www.edps.europa.eu/press-publications/press-news/press-releases/2024/edps-guidelines-generative-ai-embracing-opportunities-protecting-people_en. Press Release, "EDPS Guidelines on generative AI: embracing opportunities, protecting people." June 3, 2024. https://www.edps.europa.eu/press-publications/press-news/press-releases/2024/edps-guidelines-generative-ai-embracing-opportunities-protecting-people_en.

[2] EU AI Act: first regulation on artificial intelligence. June 6, 2024. https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence#next-steps-7.

[3] Generative AI and the EUDPR, First Orientations for ensuring data protection compliance when using Generative AI systems. European Data Protection Supervisor, June 3, 2024 ("EDPS Guidelines") at 4.

[4] EDPS Guidelines at 6.

[5] EDPS Guidelines at 14.

[6] EDPS Guidelines at 15.

[7] Nicoletti, L., & Bass, D. (2023, June 14).Humans are biased. Generative AI is even

worse. Bloomberg Technology + Equality.https://www.bloomberg.com/graphics/2023-generative-ai-bias; Heikkilä, M. (2023, August 8).AI language models are rife with different political biases.MIT Technology Review.https://www.technologyreview.com/2023/08/07/1077324/ai-language-models-are-rife-with-political-biases.

[8] EDPS Guidelines at 20.

[9] Secretary of State for Science, Innovation and Technology, A pro-innovation approach to AI regulation, August 3, 2023, available at https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach/white-paper#executive-summary.

[10] The White House, Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, October 30, 2023, available at https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/.