EDPS issues Guidelines on generative AI

The rapid advancement of generative AI technologies presents significant opportunities for innovation across various sectors.

18 June 2024

Understanding Generative AI

Generative AI refers to machine learning models designed to produce a wide array of outputs, such as text, images, and audio. These models, often built upon large foundation models like large language models (LLMs), require vast datasets for training. As a result, they can pose significant privacy and data protection risks, particularly when personal data is involved.

Compliance with EU Data Protection Laws

The EDPS orientations highlight several key principles and steps that EUIs must follow to ensure compliance with the EU General Data Protection Regulation (EU GDPR).

1. **Scope and Definitions:** The orientations emphasise the importance of understanding the various stages of generative AI system development, from data collection to model deployment, and the potential involvement of personal data at each stage.

2. **Data Protection Officers (DPOs):** DPOs play a crucial role in advising and overseeing compliance with data protection regulations during the development and deployment of generative AI systems. Their involvement is essential to ensure transparency, accountability, and adherence to data protection principles.

3. **Data Protection Impact Assessments (DPIAs):** Before deploying generative AI systems, EUIs must conduct DPIAs to assess and mitigate potential risks to individuals' rights and freedoms. This includes documenting all processing activities and ensuring continuous monitoring and reassessment of risks.

4. **Lawfulness of Processing:** The processing of personal data must have a valid legal basis under the Regulation. This includes obtaining consent, fulfilling contractual obligations, or performing tasks in the public interest. Special categories of data require additional safeguards and specific legal bases.

5. **Data Minimisation and Accuracy:** EUIs must ensure that personal data collected and processed is adequate, relevant, and limited to what is necessary for the intended purpose. Maintaining data accuracy throughout the AI system's lifecycle is critical to avoid erroneous or biased outcomes.

6. **Transparency and Individual Rights:** Individuals must be informed about how their data is processed by generative AI systems. This includes providing clear and comprehensive information

on data processing activities and ensuring individuals can exercise their rights to access, rectification, erasure, and objection.

7. **Automated Decision-Making:** When generative AI systems are used for automated decision-making, EUIs must ensure that individuals have the right to obtain human intervention, express their views, and contest decisions. This is particularly important for decisions with significant impacts on individuals' lives.

8. **Fair Processing and Avoiding Bias:** To prevent discrimination and unfair treatment, EUIs must implement measures to detect and mitigate biases in AI systems. This includes ensuring diverse and representative training datasets and ongoing monitoring of AI outputs for fairness.

9. **Data Security:** Robust security measures must be in place to protect personal data processed by generative AI systems. This includes addressing specific AI-related vulnerabilities and ensuring continuous assessment and improvement of security practices.

Conclusion

The EDPS orientations serve as a preliminary framework to help EUIs navigate the complexities of generative AI while ensuring compliance with data protection regulations. As AI technologies evolve, these guidelines will be updated and refined to address emerging challenges and support the responsible use of AI.

Sign up to get the latest legal know-how delivered straight to your inbox.

This document (and any information accessed through links in this document) is provided for information purposes only and does not constitute legal advice. Professional legal advice should be obtained before taking or refraining from any action as a result of the contents of this document.