EDPS Orientations for ensuring data protection compliance when using Generative AI systems

Generative AI and the EUDPR

June 14, 2024

The European Data Protection Supervisor (EDPS) has released orientations (guidelines) on "Generative Artificial Intelligence and Personal Data Protection" to assist EU institutions, bodies, offices, and agencies (EUIs) with practical advice in complying with data protection laws when using generative AI. These orientations address core data protection principles and the challenges posed by generative AI. While generative AI offers various benefits, it also risks impacting fundamental rights and freedoms if not properly managed.

The EDPS orientations aim to ensure EUIs adhere to data protection obligations under the EUDPR for EUIs (Regulation 2018/1725), emphasizing the need for technological neutrality to remain relevant despite the rapid evolution of AI. These initial orientations mark the beginning of more comprehensive future guidance, reflecting ongoing developments in generative AI and its implications.

They have been drafted to cover as many scenarios and applications as possible and do not prescribe specific technical measures. Instead, they put an emphasis on the general principles of data protection that should help EUIs comply with the data protection requirements.

About generative AI

Generative AI is a specialized subset of AI and leverages machine learning models to produce a wide variety of outputs such as text, images, or audio.

The foundation models serve as the core architecture for more specialized generative AI systems. Foundation models, including large language models, are trained on extensive and diverse datasets, encompassing publicly available information, and can represent complex structures like images, audio, video, or language. Large language models, for instance, are trained on vast amounts of text data to generate natural language responses.

Generative AI applications are diverse, including code generation systems, virtual assistants, content creation tools, language translation engines, automated speech recognition, medical diagnosis systems, and scientific research tools.

The hierarchy within generative AI starts with the broad category, encompassing models designed to create content. Foundation models form the base, upon which more specialized models are built and fine-tuned for specific tasks or applications.

Generative AI is widely applicable, from consumer-oriented applications like ChatGPT to business-specific tools. EU institutions (EUIs) can develop, deploy, and use generative AI in public services, adhering to legal requirements and ensuring respect for fundamental rights.

Key points orientations

1. Applicability: Regular monitoring and controls should be applied throughout the AI lifecycle to determine personal data processing. Accountability and clear role definitions are crucial among various actors in the AI model supply chain.
2. Data Collection: Web scraping for, and processing of, personal data, even if publicly available, must comply with EU data protection laws, particularly data minimization.
3. Role of DPOs: Data protection officers should advise on compliance during the AI system's procurement, design, and implementation, including reviewing data-sharing agreements.
4. Data Protection Impact Assessment (DPIA): Required when high risks to individual rights are anticipated, especially with new technologies. Involve data subjects or their representatives in the DPIA process.
5. Automated Decision-Making: Generative AI might involve automated decision-making, falling under Article 24 of the Regulation if it includes profiling or individual assessments. Safeguards must be in place to ensure human intervention and protect individual rights.
6. Data Subject Rights and Security: EU organizations must ensure data subjects are informed about the processing of their data by generative AI systems and facilitate their rights. EUIs must be able to identify and address security risks.

Impact and actions

The EDPS orientations on Generative AI and Personal Data Protection underscore the critical importance of aligning EU institutions' use of generative AI with data protection laws.

Failure to do so risks infringing upon fundamental rights and freedoms, highlighting the need for proactive measures to mitigate potential negative impacts.

While the EDPS guidelines are specifically designed for EUIs, their relevance extends globally, providing a comprehensive approach to the responsible use of generative AI that can benefit any organization concerned with data protection and privacy.

Observing the key points in the orientations, provide a good starting point.