POLITIS & PARTNERS

Law Firm

EDPB OPINION ON AI MODELS AND PERSONAL DATA PROCESSING

On December 17, 2024, the European Data Protection Board (EDPB) issued Opinion 28/2024 (the **"Opinion"**) in response to a request from the Irish supervisory authority regarding AI models and personal data. This landmark document tackles fundamental issues at the intersection of AI development and GDPR compliance, providing essential guidance for organizations seeking to innovate responsibly. Below, we delve into the Opinion's key points and its implications.

Balancing Innovation and Privacy

AI technologies are transformative, offering significant benefits across industries. However, their power to process vast amounts of data raises pressing questions about compliance with data protection regulations. The EDPB emphasizes that while the GDPR supports responsible innovation, this must be grounded in the protection of fundamental rights.

The EDPB's accompanying announcement underscores the Board's commitment to fostering responsible AI while ensuring privacy. It highlights that GDPR's principles not only safeguard data protection but also promote innovation by providing a clear legal framework. As emphasized by the EDPB, AI innovation and fundamental rights can coexist, provided organizations adopt transparent and ethical practices.

Central to the Opinion is the debate over whether AI models trained on personal data can ever be considered "anonymous." The EDPB concludes that such claims must be rigorously assessed on a case-by-case basis. An AI model's anonymity depends on the residual risks of identifying individuals, both directly and indirectly, through methods reasonably likely to be used. Organizations bear the burden of demonstrating that the likelihood of re-identification is negligible, which necessitates detailed documentation and robust risk-mitigation measures.

[1]OJ L 302, 17.11.2009, p. 32–96

Legal Basis for Processing: The Role of Legitimate Interest

When AI models involve personal data, organizations often rely on legitimate interest as a legal basis for processing. The EDPB reiterates that legitimate interest is neither a default nor a superior basis; it must be justified through a meticulous three-step assessment:

1. **Identifying the Legitimate Interest:** The interest must be lawful, clearly articulated, and real (not speculative). Examples include developing conversational agents or enhancing cybersecurity.
2. **Assessing Necessity:** The processing must be necessary to achieve the stated interest, with no less intrusive means available. This includes adhering to data minimization principles and evaluating the proportionality of the data used.
3. **Balancing Test:** The legitimate interest must not override the data subjects' rights and freedoms. Transparency, reasonable expectations, and the specific context of data collection are critical factors. For example, the origin of the data (e.g., publicly available sources) and the nature of the relationship between the controller and data subject significantly influence this assessment.

The EDPB emphasizes that the complexity of AI technologies, such as large language models (LLMs), often makes it difficult for individuals to foresee how their data might be processed. This places a heightened responsibility on organizations to provide clear, accessible, and meaningful information.

Consequences of Unlawful Processing

A particularly noteworthy section of the Opinion addresses the implications of unlawful data processing during the development of AI models. The EDPB explores three scenarios:

Scenario 1: Same Controller, Subsequent Processing

When the same controller unlawfully processes personal data during development and later uses the AI model for deployment, supervisory authorities must assess whether the two phases serve distinct purposes. If so, they may constitute separate processing activities, and the legality of the initial processing could directly affect the subsequent use. For instance, a lack of legal basis during development might invalidate future operations reliant on the same dataset.

Scenario 2: Transfer to a Different Controller

In cases where an AI model containing personal data is transferred to another controller for deployment, the new controller must verify compliance with GDPR. This includes determining whether the model was developed lawfully and assessing associated risks. The due diligence process should examine the source of the personal data, the legality of the original processing, and the measures implemented to mitigate risks.

Scenario 3: Post-Anonymization Use

If personal data was unlawfully processed during development but subsequently anonymized, the model's deployment may avoid GDPR applicability, provided it no longer involves personal data. However, if new personal data is processed during deployment, the GDPR applies to these activities. In this scenario, the lawfulness of the initial processing does not necessarily impact subsequent operations if anonymization is robust and demonstrable.

These scenarios highlight the importance of integrating compliance into every stage of AI development and deployment, from initial data collection to operational use.

Mitigating Risks and Ensuring Compliance

The EDPB provides a range of strategies for organizations to mitigate risks and demonstrate accountability:

1. **Privacy-Preserving Techniques:** Implement methods such as differential privacy to minimize the risk of re-identification.
2. **Data Minimization:** Limit data collection to what is strictly necessary for the model's purpose.
3. **Thorough Documentation:** Maintain detailed records of processing activities, technical measures, and risk assessments.
4. **Transparency:** Clearly communicate to data subjects how their data is used, especially in cases involving automated decision-making or profiling.
5. **Impact Assessments:** Conduct Data Protection Impact Assessments (DPIAs) to evaluate risks, particularly when processing is likely to result in high risks to individuals.

The EDPB emphasizes that the complexity of AI technologies, such as large language models (LLMs), often makes it difficult for individuals to foresee how their data might be processed. This places a heightened responsibility on organizations to provide clear, accessible, and meaningful information.

Conclusion: A Call for Ethical Innovation

The EDPB's Opinion underscores a fundamental message: the pursuit of AI innovation must be paired with a deep commitment to privacy and data protection. Organizations are not only bound by regulatory obligations but also by an ethical imperative to respect individuals' rights. By embedding data protection principles into their AI systems from the outset, organizations can build trust and pave the way for sustainable technological progress.

For businesses ready to embrace this responsibility, the rewards include not just compliance but the opportunity to lead in a future defined by ethical innovation.

For more information, please contact:

Emmanouil Savoidakis
Partner
E: esavoidakis@politispartners.gr

Kassiani Skamagka
Junior Associate
E: kskamagka@politispartners.gr

14, SOLONOS STR.
106 73, ATHENS, GREECE

Tel.: +30 210 7297252
Email: info@politispartners.gr
Web: www.politispartners.gr

POLITIS & PARTNERS
Law Firm