AI & Partners

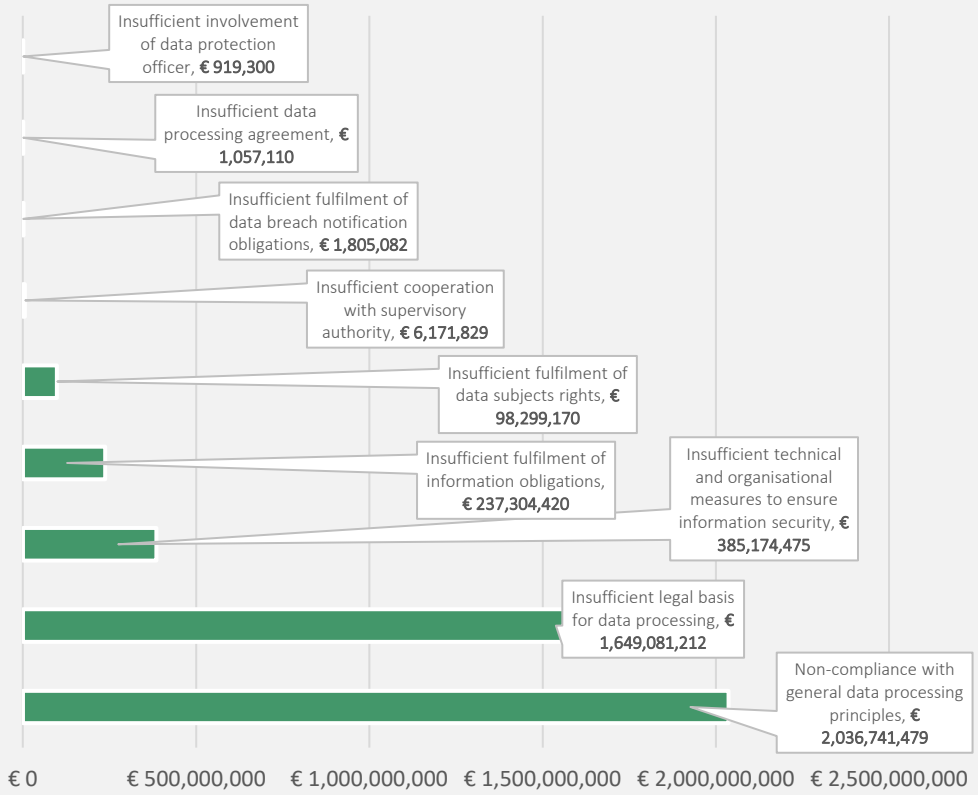
Amsterdam - London - Singapore

Fines and Penalties

Predicting EU AI Act enforcement action

March 2024

Key GDPR Enforcement Insights



Predicting EU AI Act Fines Based on GDPR Enforcement Data

Recital 84 of the EU AI Act states that, in order to strengthen and harmonise administrative penalties for infringement of this Regulation, the upper limits for setting the administrative fines for certain specific infringements should be laid down.

01 Principles-Based Fines

Similar to the GDPR, potential fines under the EU AI Act may be imposed for non-compliance with regulatory principles. This suggests a continued emphasis on fundamental principles such as transparency, fairness, and accountability in AI systems.

02 Legal and Ethical AI Basis

Fines for insufficient legal basis for data processing in GDPR imply that the EU AI Act may require a clear and justifiable legal and ethical basis for AI system-based activities. This could involve adherence to ethical guidelines and compliance with specific legal requirements for AI applications.

03 Security Measures for AI Systems

The fines related to insufficient technical and organizational measures for information security in GDPR suggest that the EU AI Act may include provisions requiring robust security (and other) measures specific to AI systems. This could encompass measures to ensure the integrity, confidentiality, and availability of AI-generated data or outputs.

04 Information Transparency in AI

Fines associated with insufficient fulfilment of information obligations and data subjects' rights in GDPR imply that the EU AI Act may demand transparency and clear communication about AI systems' functioning and impact on individuals' fundamental rights. This may involve informing users about the use of AI algorithms and providing them with meaningful insights into how they interact with AI systems.

05 Regulatory Cooperation for AI Governance

Fines for insufficient cooperation with supervisory authorities in GDPR indicate that the EU AI Act may encourage active collaboration with regulatory bodies for effective AI governance. Organizations may be required to work closely with supervisory authorities to address concerns and ensure compliance with AI-related regulatory obligations.

Violation Mapping

GDPR	EU AI Act
Art. 5, 9, 13, 24 (1), 28, 32: Non-Compliance with general data processing principles	**R.27**: Non-Compliance with general principles applicable to all AI systems
Art. 5, 6, 9, 58: Insufficient legal basis for data processing	**Art. 99**: Insufficient technical and organisational measures to ensure training of models
Art. 5, 12, 15, 25, 32: Insufficient technical and organisational measures to ensure information security	
Art. 5, 12, 13, 25: Insufficient fulfilment of information obligations	**Art. 50**: Insufficient fulfilment of information obligations
Art. 7, 12, 15, 17, 32, 33, 34: Insufficient fulfilment of data subjects' rights	**Art. 59**: Insufficient fulfilment of individuals' fundamental rights
Art. 31, 37, 58: Insufficient cooperation with supervisory authority	**Art. 77**: Insufficient cooperation with supervisory authority
Art. 5, 28, 15, 33, 34: Insufficient fulfilment of data breach notification obligations	**Art. 73**: Insufficient fulfilment of breach notification obligations
Art. 5, 12, 13, 24, 26, 28: Insufficient data processing agreement	
Art. 13, 37, 38, 39: Insufficient involvement of data protection officer	**Art. 14**: Insufficient involvement of human oversight

Principles

Principles-Centric Approach in EU AI Act

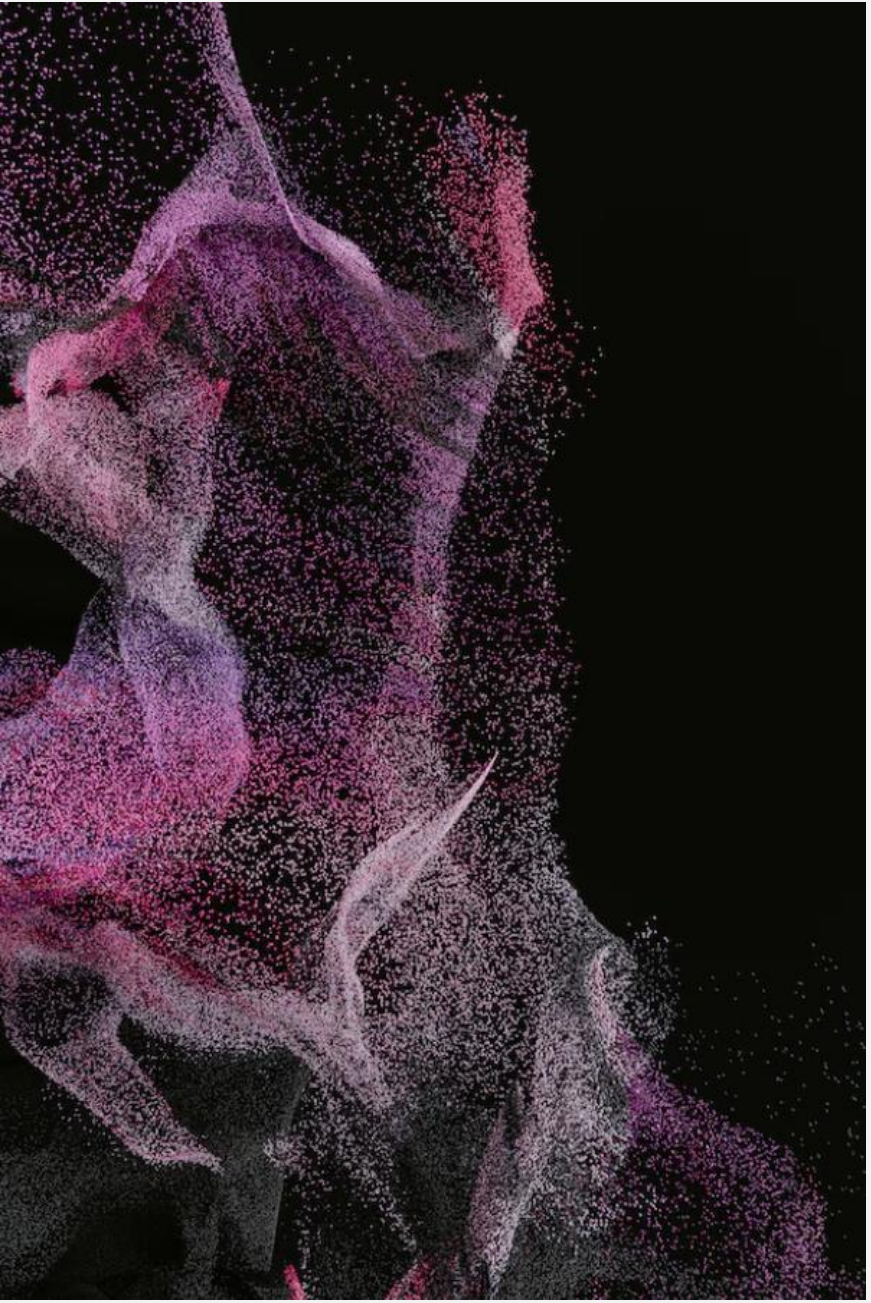
Fines for non-compliance with general data processing principles under the GDPR suggest that the EU AI Act may adopt a principles-centric approach, emphasizing adherence to foundational principles such as transparency, fairness, and accountability in the development and deployment of AI systems. Entities engaged in AI activities may be required to integrate these principles into their AI processes to ensure ethical and responsible AI use.

Holistic Governance for AI Ethics

Potential fines under the EU AI Act for violations related to general data processing principles indicate a need for holistic governance of AI ethics. This suggests that organizations developing or deploying AI systems might be obligated to implement comprehensive strategies that prioritize ethical considerations throughout the AI lifecycle, from design and development to deployment and ongoing use.

User-Centric AI Design and Communication

Fines associated with non-compliance with general data processing principles imply that the EU AI Act could prioritize user-centric AI design and communication. Organizations may be required to ensure clear and understandable communication with users about how AI systems process their data. This could involve transparent disclosure of AI algorithms, purposes of data processing, and mechanisms for user consent, enhancing transparency and trust in AI technologies.



Data Processing

Ethical and Legal Foundation in AI Governance

Fines for insufficient legal basis for data processing under the GDPR suggest that the EU AI Act may prioritize establishing a robust ethical and legal foundation for AI governance. This indicates a potential requirement for organizations to clearly define and justify the legal basis for their AI activities, emphasizing compliance with ethical guidelines and legal frameworks specific to AI.

Clear Legal Justification for AI Processing

Potential fines under the EU AI Act for insufficient legal basis hint at the necessity for organizations to provide clear and justifiable legal grounds for their AI processing activities. This may involve specific provisions outlining acceptable legal bases for various AI applications, reinforcing the importance of transparency and legal compliance in AI development and deployment.

Risk Mitigation through Legal Compliance

Fines associated with insufficient legal basis for data processing in GDPR imply that the EU AI Act could stress the importance of mitigating risks through legal compliance. Organizations engaged in AI activities may need to proactively assess and justify the legal basis for their AI processing to reduce the risk of fines, promoting responsible and legally sound AI practices.

Technical and Organisational Measures

Rigorous Security Frameworks for AI Systems

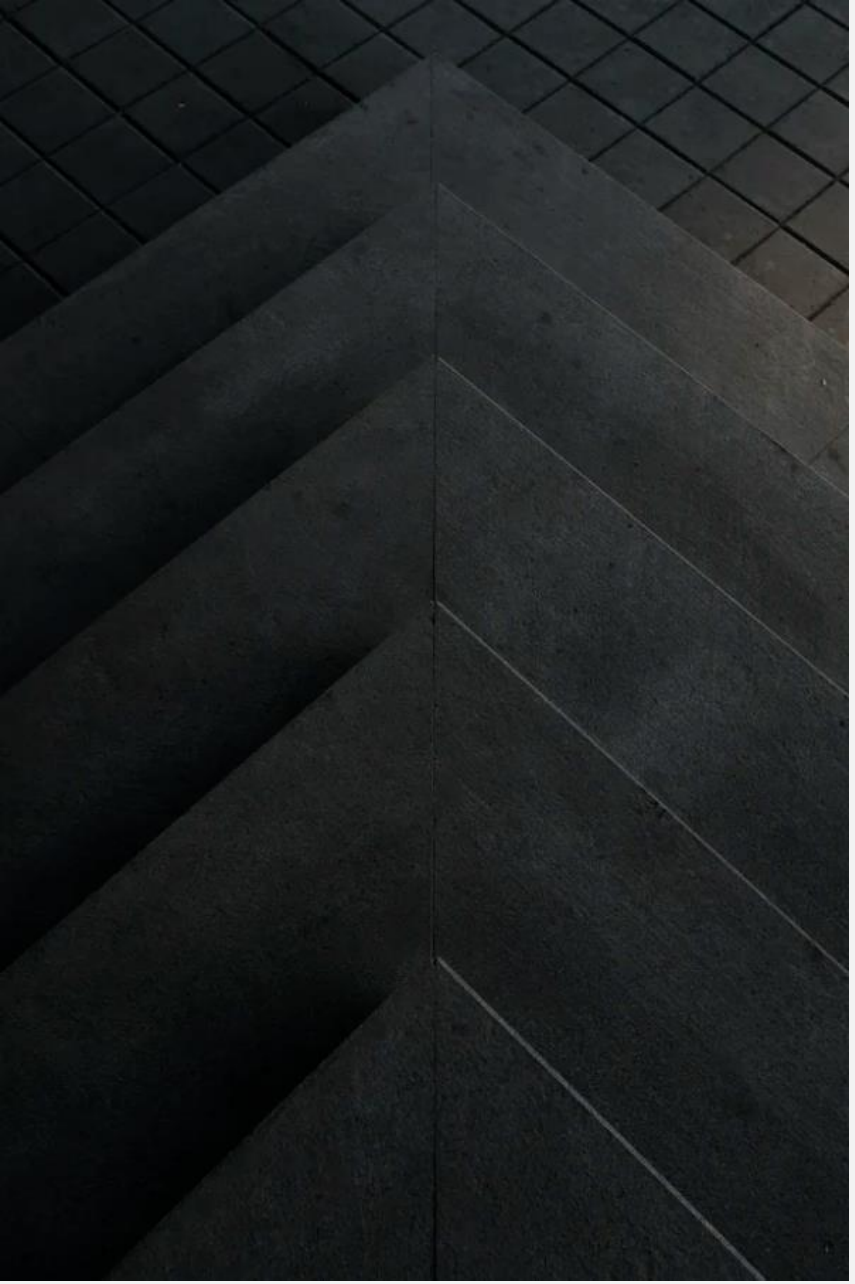
Fines for insufficient technical and organizational measures in the GDPR suggest that the EU AI Act may demand rigorous security frameworks for AI systems. Organizations involved in AI development may be required to implement robust technical and organizational measures to ensure the integrity, confidentiality, and resilience of AI-related data, safeguarding against potential vulnerabilities and cyber threats.

AI-Specific Security Guidelines and Standards

Potential fines under the EU AI Act for insufficient technical and organizational measures imply a need for AI-specific security guidelines and standards. This may involve the development and adherence to industry-recognized practices tailored to the unique challenges posed by AI technologies, ensuring a comprehensive and effective security posture.

Proactive Risk Mitigation in AI Development

Fines associated with insufficient technical and organizational measures indicate that the EU AI Act could prioritize proactive risk mitigation in AI development. Organizations may be required to integrate security measures throughout the AI development lifecycle, from design to deployment, emphasizing a proactive approach to identify and address potential security risks, fostering a secure and trustworthy AI ecosystem.



Information Obligations

Transparent Communication in AI Practices

Fines for insufficient fulfilment of information obligations under the GDPR suggest that the EU AI Act may stress the importance of transparent communication in AI practices. Organizations involved in AI development might be required to provide clear and accessible information to individuals about how AI systems process their data, fostering transparency and informed decision-making.

User Empowerment through AI Information

Potential fines under the EU AI Act for insufficient fulfilment of information obligations imply a focus on user empowerment. This suggests that organizations may need to empower individuals by providing comprehensive information about AI processes, enabling users to understand and exercise control over the use of their data in AI applications.

Ethical AI Disclosure Requirements:

Fines associated with insufficient fulfilment of information obligations indicate that the EU AI Act could introduce ethical AI disclosure requirements. Organizations may be obligated to disclose information about the ethical considerations, decision-making processes, and potential impacts of AI systems, ensuring transparency and accountability in the deployment of AI technologies.

Data Subjects

Enhanced Individual Empowerment

Fines for insufficient fulfilment of data subjects' rights under the GDPR suggest that the EU AI Act may prioritize enhanced empowerment of individuals. This implies that organizations engaged in AI activities may be obligated to uphold and facilitate the exercise of individuals' fundamental rights, such as human dignity, right to life, right to integrity of the person, ensuring a heightened level of control and agency over the development, deployment and/or use of AI systems.

AI-Specific Data Subject Protections

Potential fines under the EU AI Act for insufficient fulfilment of data subjects' rights indicate a need for AI-specific data subject protections. This may involve provisions tailored to the unique challenges posed by AI technologies, ensuring that individuals have effective mechanisms to assert their rights in the context of AI-generated or processed data.

Transparent AI Decision-Making Processes

Fines associated with insufficient fulfilment of data subjects' rights suggest that the EU AI Act could emphasize transparent AI decision-making processes. Organizations might be required to provide clear information about the logic, significance, and potential consequences of automated decisions, enabling individuals to understand and challenge the outcomes, fostering transparency and fairness in AI-driven processes.

Supervisory Authority

Regulatory Collaboration and Oversight

Fines for insufficient cooperation with supervisory authority under the GDPR suggest that the EU AI Act may stress the importance of regulatory collaboration and oversight in the realm of artificial intelligence. This implies that organizations involved in AI activities may be required to actively engage with and cooperate with supervisory authorities, fostering a collaborative approach to address regulatory concerns and ensuring effective oversight of AI applications.

Proactive Engagement in AI Governance

Potential fines under the EU AI Act for insufficient cooperation indicate a need for proactive engagement in AI governance. This may involve organizations taking a proactive stance in collaborating with regulatory bodies, providing timely and comprehensive information, and actively participating in discussions to address potential challenges and ensure alignment with evolving AI regulations.

Responsive Approach to Regulatory Inquiries

Fines associated with insufficient cooperation with supervisory authorities suggest that the EU AI Act could mandate a responsive approach to regulatory inquiries. Organizations might be required to promptly and transparently respond to inquiries from supervisory authorities, demonstrating a commitment to regulatory compliance and fostering an environment of openness and accountability in the development and deployment of AI technologies.

Data Breach

Timely and Transparent Breach Reporting

Fines for insufficient fulfilment of data breach notification obligations under the GDPR suggest that the EU AI Act may emphasize the importance of timely and transparent reporting of AI-related breaches. This implies that organizations involved in AI activities might be obligated to promptly notify authorities and affected parties about breaches, ensuring swift responses to mitigate potential harms and uphold accountability in the AI ecosystem.

AI-Specific Breach Protocols

Potential fines under the EU AI Act for insufficient breach notification suggest the need for AI-specific breach protocols. This could involve defining clear procedures and timelines for reporting data breaches related to AI systems, recognizing the unique challenges and risks posed by AI technologies and ensuring a tailored and effective response.

Enhanced Regulatory Oversight in AI Security

Fines associated with insufficient fulfilment of breach notification obligations indicate that the EU AI Act may introduce enhanced regulatory oversight in AI security. Organizations might be required to demonstrate not only the fulfilment of notification obligations but also proactive measures to prevent, detect, and respond to data breaches in AI applications. This fosters a robust regulatory framework to address emerging security concerns in the dynamic field of artificial intelligence.

Data Processing Agreement

Robust Contractual Frameworks for AI System Activities

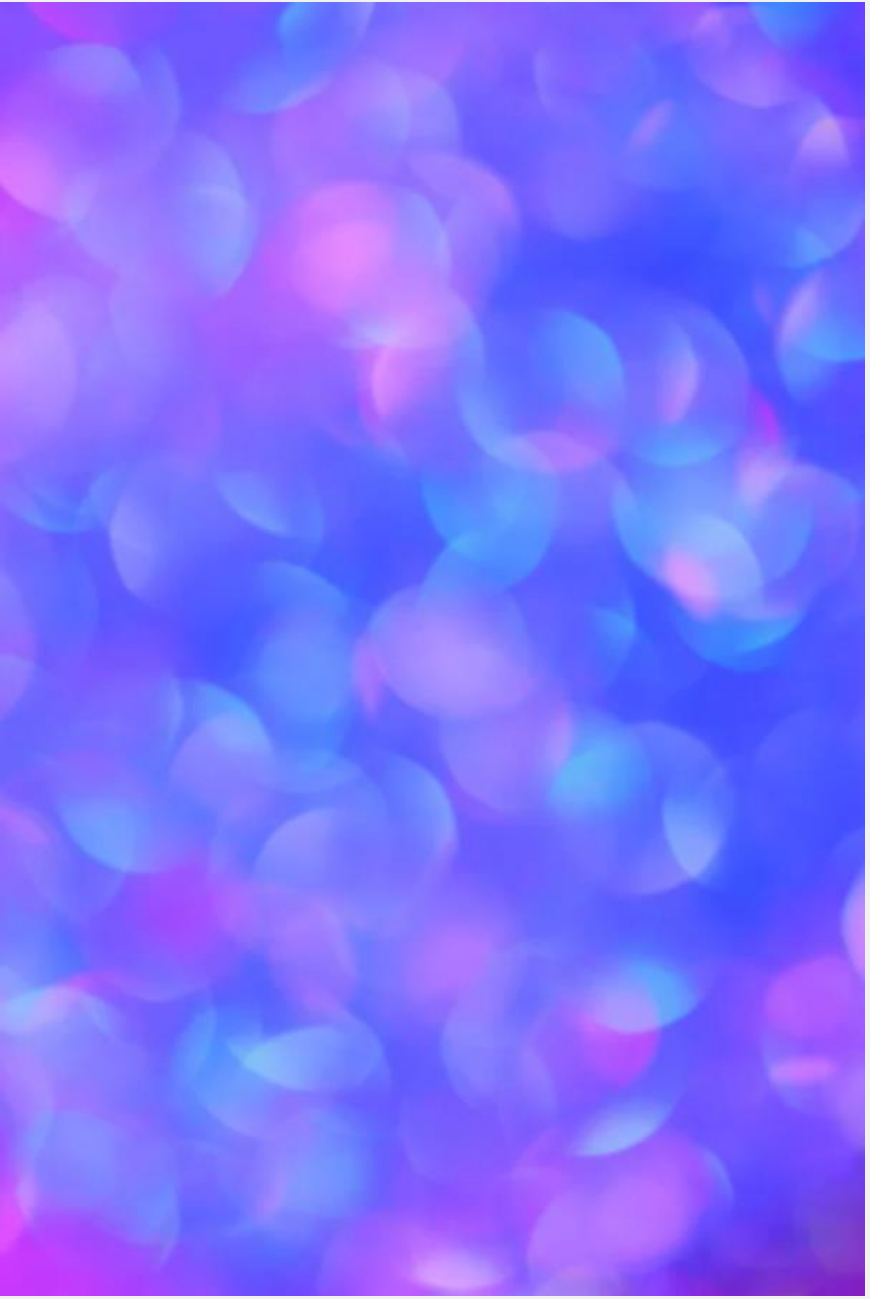
Fines for insufficient data processing agreements under the GDPR suggest that the EU AI Act may emphasize the need for robust contractual frameworks specific to AI system activities. Organizations engaged in AI activities might be required to establish clear, comprehensive agreements defining the terms of AI system activities, such as deployment, ensuring compliance with legal and ethical standards, and addressing the unique challenges associated with AI technologies.

AI-Specific Agreement Requirements

Potential fines under the EU AI Act for insufficient data processing agreements imply the introduction of AI-specific agreement requirements. This could involve specifying detailed provisions addressing the intricacies of AI system activities, including algorithmic transparency, data ownership, and the ethical considerations associated with AI applications.

Legal Safeguards for AI Data Handling

Fines associated with insufficient data processing agreements indicate that the EU AI Act may mandate legal safeguards for AI data handling. Organizations might be obligated to establish agreements that not only comply with general data protection principles but also incorporate specific provisions to safeguard data when processed by AI systems. This ensures responsible and lawful AI practices while providing clarity and protection for all parties involved.



Data Protection Officer

Mandatory Role of Data Protection Officer in AI Governance

Fines for insufficient involvement of a data protection officer (DPO) under the GDPR suggest that the EU AI Act may mandate a crucial role for DPOs in AI governance. Organizations involved in AI activities might be required to ensure active and meaningful participation of DPOs, emphasizing their role in overseeing AI processes, mitigating risks, and ensuring compliance with data protection regulations specific to AI.

AI-Specific Expertise for Data Protection Officers

Potential fines under the EU AI Act for insufficient DPO involvement imply a need for AI-specific expertise among DPOs. This could involve organizations appointing DPOs with specialized knowledge in AI technologies, ensuring they can effectively navigate the unique challenges and ethical considerations associated with AI-driven data processing.

Proactive DPO Engagement in AI Ethical Oversight

Fines associated with insufficient DPO involvement suggest that the EU AI Act may encourage proactive engagement of DPOs in AI ethical oversight. DPOs might be required to actively assess and monitor the ethical implications of AI systems, ensuring that organizations adhere to ethical guidelines and principles throughout the development and deployment of AI technologies.

Contact Details

AI & Partners

Amsterdam - London - Singapore

Email

contact@ai-and-partners.com

Phone

+44(0)7535 994 132

Website

https://www.ai-and-partners.com/

Social Media

LinkedIn: https://www.linkedin.com/company/ai-&-partners/
Twitter: https://twitter.com/AI_and_Partners

AI & Partners

Amsterdam - London - Singapore

Thank You!

Disclaimer

This Presentation may contain information, text, data, graphics, photographs, videos, sound recordings, illustrations, artwork, names, logos, trade marks, service marks, and information about us, our lines of services, and general information may be provided in the form of documents, podcasts or via an RSS feed (“the Information”).

Except where it is otherwise expressly stated, the Information is not intended to, nor does it, constitute legal, accounting, business, financial, tax or other professional advice or services. The Information is provided on an information basis only and should not be relied upon. If you need advice or services on a specific matter, please contact us using the contact details for the relevant consultant or fee earner found on the Presentation.

The Presentation and Information is provided “AS IS” and on an “AS AVAILABLE” basis and we do not guarantee the accuracy, timeliness, completeness, performance or fitness for a particular purpose of the Presentation or any of the Information. We have tried to ensure that all Information provided on the Presentation is correct at the time of publication. No responsibility is accepted by or on behalf of us for any errors, omissions, or inaccurate information on the Presentation. Further, we do not warrant that the Presentation or any of the Information will be uninterrupted or error-free or that any defects will be corrected.

Although we attempt to ensure that the Information contained in this Presentation is accurate and up-to-date, we accept no liability for the results of any action taken on the basis of the Information it contains and all implied warranties, including, but not limited to, the implied warranties of satisfactory quality, fitness for a particular purpose, non-infringement, compatibility, security, and accuracy are excluded from these Terms to the extent that they may be excluded as a matter of law.

In no event will we be liable for any loss, including, without limitation, indirect or consequential loss, or any damages arising from loss of use, data or profits, whether in contract, tort or otherwise, arising out of, or in connection with the use of this Presentation or any of the Information.