AI & Partners

Amsterdam - London - Singapore

EU AI Act

AI Regulation

Impact on Data Protection

May 2025

AI & Partners

Sean Musch, AI & Partners

Michael Borrelli, AI & Partners

Charles Kerrigan, CMS UK

Enzo di Taranto Capozzi, Global Sustainability Thought Leader

Peter Slattery, MIT

AI & Partners

Amsterdam - London - Singapore

AI & Partners defends and extends the digital rights of users at risk around the world. By combining direct technical support, comprehensive policy engagement, global advocacy, grassroots professional services, regulatory interventions, and participating in industry groups such as AI Commons, we fight for fundamental rights in the artificial intelligence age.

This report was prepared by Sean Donald John Musch and Michael Charles Borrelli. For more information visit https://www.ai-and-partners.com/.

Contact: Michael Charles Borrelli | Director | m.borrelli@ai-and-partners.com.

This report is an AI & Partners publication.

Contents

Introduction

As artificial intelligence continues to reshape industries, the need for robust regulatory frameworks to safeguard data privacy has never been more critical. Emerging AI regulations, including the EU AI Act and updates to GDPR enforcement, aim to ensure that AI systems operate transparently, ethically, and in compliance with stringent data protection standards. These regulatory measures impose new obligations on organizations, requiring them to assess AI risks, implement accountability mechanisms, and enhance data governance practices.

This report examines the intersection of AI regulation and data protection, offering insights into how evolving legal frameworks shape AI deployment. From mandatory impact assessments to data minimization requirements, AI governance now demands a proactive approach to mitigating privacy risks and ensuring compliance. Organizations must navigate complex regulatory landscapes to maintain consumer trust and avoid significant penalties.

With increasing scrutiny from global regulators, businesses must demonstrate AI governance maturity by integrating privacy-preserving technologies, enhancing transparency, and adopting responsible AI practices. Effective compliance strategies not only reduce legal exposure but also strengthen consumer confidence in AI-driven systems.

Whether you are an AI developer, enterprise leader, or policymaker, this report provides strategic guidance on aligning AI operations with emerging data protection regulations. At AI & Partners, we are committed to supporting organizations in building AI systems that prioritize privacy, security, and regulatory compliance in an increasingly complex legal environment.

Best regards,

Sean Musch

Founder/CEO

AI & Partners

Key questions being asked about AI Regulation Impact on Data Protection

What is the primary objective of AI regulation in the context of data protection?

The primary objective of AI regulation concerning data protection is to ensure that AI systems operate transparently, fairly, and in compliance with privacy laws. Regulations aim to mitigate risks associated with automated decision-making, prevent misuse of personal data, and uphold individuals' rights under established legal frameworks such as the GDPR. By enforcing accountability and requiring organizations to implement safeguards like data minimization, impact assessments, and user consent mechanisms, these regulations ensure that AI-driven technologies remain ethical and do not compromise privacy or fundamental rights. AI regulations also help foster consumer trust in automated processes.

How does AI regulation impact businesses that rely on AI-driven data processing?

AI regulation imposes new compliance requirements on businesses, necessitating the implementation of robust data governance practices. Companies must ensure that AI models do not engage in discriminatory practices, properly handle personal data, and provide clear explanations for automated decisions. Non-compliance can result in penalties and reputational damage. Businesses also need to implement bias mitigation strategies, conduct fairness audits, and integrate privacy-by-design principles in AI development. By following these regulations, businesses can avoid legal challenges, enhance customer trust, and develop AI systems that align with ethical and legal expectations while maintaining operational efficiency.

What are the key legal frameworks governing AI and data protection?

The key legal frameworks include the General Data Protection Regulation (GDPR), the EU AI Act, and various national-level regulations that dictate how AI systems should process data responsibly. These laws emphasize principles such as data minimization, user consent, and accountability in AI operations. Additionally, sector-specific laws, such as the U.S. AI Bill of Rights and China's AI governance guidelines, establish AI-specific compliance standards. Organizations operating internationally must navigate different jurisdictional requirements, ensuring AI-driven applications adhere to both regional and global legal frameworks while maintaining high standards for ethical and secure data processing.

What challenges do organizations face in complying with AI regulations?

Organizations encounter challenges such as adapting AI models to ensure fairness and transparency, maintaining detailed documentation for regulatory audits, and managing data access rights. Additionally, companies must stay updated with evolving laws and implement technical safeguards to mitigate data privacy risks. The complexity of AI algorithms often makes it difficult to provide clear explanations for automated decisions. Furthermore, small and medium enterprises (SMEs) may struggle with the costs of compliance, as implementing AI risk management frameworks requires substantial investments in legal expertise, data governance policies, and robust monitoring systems to prevent regulatory violations.

How do AI regulations affect automated decision-making and consumer rights?

AI regulations mandate that automated decision-making systems be interpretable and accountable. Consumers must be informed when AI-driven decisions affect their rights, such as loan approvals or hiring processes. Individuals also have the right to contest AI decisions and request human intervention in certain cases. Organizations must implement mechanisms to ensure explainability, fairness, and non-discrimination in AI outcomes. The ability to appeal AI-generated decisions ensures that individuals maintain agency over their personal data, while regulatory bodies enforce standards that prevent harmful biases and protect consumers from opaque, unaccountable AI-driven processes.

What role do data protection officers (DPOs) play in AI regulation compliance?

DPOs oversee AI governance policies, ensuring compliance with data protection laws. Their responsibilities include conducting data protection impact assessments, advising on AI ethics, and liaising with regulatory authorities to address compliance concerns. DPOs also help organizations implement AI risk management frameworks, oversee data retention and deletion policies, and ensure AI models align with evolving legal requirements. Their role is critical in balancing AI innovation with ethical responsibility, as they bridge the gap between technological advancements and legal obligations, ensuring organizations mitigate AI risks while maintaining transparency and accountability in data-driven operations.

How does AI regulation influence innovation and technological advancements?

While AI regulations introduce compliance challenges, they also encourage ethical AI development. By establishing clear legal boundaries, regulations foster public trust in AI technologies, leading to sustainable innovation and wider AI adoption in sectors such as healthcare, finance, and government services. Regulations incentivize the creation of fair, unbiased AI models, compelling organizations to invest in ethical AI practices. While compliance can be resource-intensive, businesses that integrate responsible AI principles gain a competitive advantage, as consumers and regulatory bodies increasingly favor transparent, secure, and accountable AI solutions that protect user rights and privacy.

What penalties exist for non-compliance with AI data protection regulations?

Non-compliance can result in significant fines, legal action, and operational restrictions. For instance, under GDPR, businesses may face fines of up to 4% of their global annual revenue. Regulatory bodies can also mandate corrective actions, such as modifying AI systems or ceasing certain data processing activities. Additional penalties may include reputational harm, loss of consumer trust, and increased scrutiny from authorities. Organizations that fail to comply with AI regulations risk losing market access and may face stricter oversight, requiring them to invest in substantial remediation efforts to regain compliance and restore credibility.

How can businesses proactively prepare for AI regulations?

Businesses should implement AI governance frameworks, conduct regular compliance audits, and establish transparency mechanisms for AI-driven decisions. Additionally, investing in staff training and ethical AI design can help organizations align with regulatory requirements and mitigate compliance risks. Establishing cross-functional compliance teams and collaborating with legal experts can further strengthen AI governance efforts. By integrating privacy-by-design principles, companies can ensure AI systems comply with data protection laws from inception. Staying informed about evolving regulatory landscapes and engaging with industry-wide AI governance initiatives helps businesses remain proactive in managing legal and ethical AI challenges.

What future trends can we expect in AI regulation and data protection?

Future AI regulations are likely to introduce stricter requirements for AI accountability, increased emphasis on explainability, and enhanced consumer protections. Policymakers may also focus on international harmonization of AI laws to ensure consistent data protection standards across jurisdictions. Additionally, regulations will likely address emerging AI risks such as deepfake misuse, generative AI accountability, and algorithmic discrimination. Companies that prioritize ethical AI development and transparency will be better positioned to adapt to these regulatory shifts, gaining a competitive edge by fostering public trust and demonstrating compliance with evolving global AI governance frameworks.

Understanding Impact of AI Regulation on Data Protection

GDPR Application

What is the Impact?

AI significantly challenges data protection principles under the GDPR by increasing the likelihood of re-identification of anonymized or pseudonymized data and enabling the inference of new personal data. This enhances risks to privacy, as individuals may be identified or profiled based on seemingly non-personal data. Consequently, GDPR provisions such as legal basis requirements, data subject rights, and safeguards for automated processing become increasingly relevant.

How is it relevant?

AI-driven data processing makes personal data more dynamic and context-dependent. The GDPR's definition of personal data extends to identifiable and inferred information, meaning AI techniques can transform previously non-personal data into personal data. This affects compliance, requiring stricter security measures, transparency obligations, and regulatory oversight to prevent unauthorized re-identification and mitigate profiling risks.

Why does it arise?

The issue arises due to AI's capacity to analyze large datasets, detect correlations, and infer information beyond what was originally provided. Advances in machine learning and big data analytics have made it easier to associate disparate data points with individuals, undermining traditional anonymization techniques. As AI becomes more sophisticated, the GDPR's conceptual framework must adapt to ensure robust data protection and prevent misuse of inferred or re-identified data.

Data Protection Principles

What is the Impact?

AI and big data challenge key GDPR principles, particularly transparency, fairness, purpose limitation, data minimisation, accuracy, and storage limitation. The complexity of AI-driven processing makes it harder to ensure compliance, leading to risks such as opaque decision-making, potential discrimination, repurposing of data, excessive data retention, and inaccuracies affecting individuals.

How is it relevant?

AI-driven data processing raises concerns about accountability, lawful processing, and individual rights. Transparency is essential for ensuring that individuals understand how their data is used. Purpose limitation and minimisation principles are at odds with AI's tendency to repurpose and process large datasets unpredictably. Accuracy and fairness are crucial in AI-driven profiling to prevent biases and ensure reliable outcomes. Storage limitations also conflict with AI's need for vast historical data.

Why does it arise?

The issues stem from AI's inherent characteristics—complexity, opacity, data dependency, and predictive nature. AI models require extensive data for training, often leading to repurposing beyond original collection intents. Automated decision-making and profiling can result in unfair or biased outcomes if not carefully regulated. Additionally, balancing AI innovation with GDPR's strict data protection requirements creates an ongoing regulatory challenge.

Legal Bases

What is the Impact?

AI regulation, particularly under the GDPR, imposes strict conditions on the processing of personal data, limiting AI applications that rely on large datasets. The necessity of a legal basis for AI-driven data processing introduces compliance challenges, particularly concerning consent, legitimate interest, and repurposing of data. Additionally, AI amplifies risks related to sensitive data, including re-identification and inferred profiling, necessitating stronger safeguards.

How is it relevant?

This issue is central to balancing technological advancement with individual privacy rights. The constraints imposed by GDPR impact AI development in sectors such as healthcare, finance, and marketing, where personal data is integral to innovation. Moreover, the distinction between statistical and profiling-based processing influences the legality of AI-driven decision-making, shaping industry practices and ethical considerations.

Why does it arise?

The challenge stems from AI's ability to process vast amounts of data beyond the original purpose of collection, often without explicit user consent. The GDPR's principles of purpose limitation and data minimization conflict with AI's data-driven nature. Furthermore, AI's capability to infer sensitive information from non-sensitive data raises concerns about discrimination, transparency, and individual control over personal information.

Transparency

What is the Impact?

AI regulation significantly affects data protection by imposing transparency requirements on AI-driven data processing. The GDPR mandates that individuals be informed about how their data is processed, especially in AI-based decision-making. This includes explaining the logic behind automated decisions, potential consequences, and safeguards. However, AI's complexity, particularly in machine learning models, makes full transparency difficult, limiting individuals' ability to understand or challenge decisions affecting them.

How is it relevant?

Transparency is crucial for ensuring fairness, accountability, and trust in AI systems. Without clear explanations, individuals cannot assess whether AI decisions are biased, incorrect, or unjust. The challenge becomes more significant as AI models evolve dynamically, often repurposing data in unforeseen ways. The GDPR attempts to balance transparency with practical limitations, such as cases where providing information is disproportionate or technically infeasible.

Why does it arise?

The challenge arises from the inherent opacity of AI, particularly deep learning models, which do not easily lend themselves to human-readable explanations. While GDPR seeks to enforce explainability, current AI technology often lacks the capability to provide clear, accessible insights into its decision-making processes. Furthermore, companies may be reluctant to disclose proprietary algorithms, complicating regulatory compliance and oversight.

Data Subjects' Rights

What is the Impact?

AI affects data subjects' rights under GDPR, particularly concerning access, erasure, portability, and objection. AI-driven automated decision-making and profiling raise challenges in providing meaningful transparency and ensuring individuals can control their data effectively. The right to access (Article 15) is constrained by intellectual property protections, the right to erasure (Article 17) is complicated by inferred data, and the right to portability (Article 19) is unclear regarding system-tracked and inferred data. Additionally, AI heightens concerns around profiling, direct marketing, and statistical data processing, affecting the ability of individuals to object (Article 21).

How is it relevant?

AI's reliance on large datasets and automated profiling makes it difficult to ensure compliance with GDPR rights, potentially limiting individuals' ability to understand, challenge, or control the use of their personal data. Transparency obligations and access rights are limited by AI's complexity, while the persistence of inferred data challenges the feasibility of data erasure. The right to object to AI-driven profiling is particularly significant in marketing and research contexts, impacting individuals' autonomy over how their data is used.

Why does it arise?

The issues stem from AI's data-driven nature, the opacity of algorithmic decision-making, and the tension between data protection rights and practical implementation. AI models generate inferred data that may not be considered "personal data" under GDPR, yet significantly impact individuals. Additionally, businesses and researchers rely on AI-based profiling and automated decision-making, leading to conflicts between commercial interests, innovation, and privacy protections. The challenge lies in balancing transparency, individual rights, and the complexity of AI systems.

Automated Decision-Making

What is the Impact?

AI regulation reinforces Article 22 GDPR by imposing stricter oversight on automated decision-making processes, particularly those with legal or similarly significant effects on individuals. It mandates transparency, human oversight, and justification for AI-driven decisions, reducing risks of bias, unfairness, and data misuse. However, compliance obligations may limit certain AI applications and increase regulatory complexity for businesses.

How is it relevant?

Article 22 GDPR grants individuals rights over automated decision-making, restricting AI systems that operate without meaningful human intervention. AI regulations, such as the EU AI Act, complement these protections by setting stricter risk-based requirements, ensuring that high-risk AI applications align with data protection principles like fairness, explainability, and accountability.

Why does it arise?

Automated decision-making can have profound consequences on individuals' rights, from credit scoring to hiring and law enforcement. The potential for bias, discrimination, and lack of transparency in AI systems has driven regulators to strengthen safeguards under Article 22. As AI becomes more sophisticated, additional governance measures are necessary to ensure compliance with fundamental rights and prevent harm.

Privacy-by-Design

What is the Impact?

AI regulation strengthens privacy by design by requiring organizations to integrate data protection measures at the core of AI systems. This impacts automated decision-making (Article 22 GDPR), mandating transparency, human oversight, and safeguards against bias. Stricter obligations under the EU AI Act and GDPR limit excessive data processing and enhance individuals' control over their data.

How is it relevant?

Privacy by design ensures AI systems are lawful, fair, and transparent in processing personal data. As AI adoption grows, compliance with GDPR and AI regulations mitigates risks of discrimination, security breaches, and unlawful profiling. Businesses developing AI must embed privacy safeguards early to avoid regulatory penalties, reputational harm, and legal challenges.

Why does it arise?

The risks of AI-driven data processing—such as opacity, bias, and autonomy in decision-making—conflict with fundamental privacy rights. AI regulation emerges to close compliance gaps, enforce accountability, and balance innovation with ethical AI deployment. The regulatory focus on privacy by design stems from the need to protect individuals' rights in an AI-driven world.

Statistical Processing & Scientific Research

What is the Impact?

AI regulation, particularly the GDPR, enables statistical processing and scientific research by permitting data repurposing (Article 5(1)(b)) and providing safeguards (Article 89). While it facilitates big data analytics, it also imposes restrictions through data minimization, pseudonymization, and purpose limitation to protect individual privacy. The EU AI Act and GDPR collectively shape how AI systems process data for research while ensuring compliance with fundamental rights.

How is it relevant?

Statistical processing supports economic, technological, and scientific advancements, including AI-driven healthcare, market analysis, and policy optimization. GDPR provisions balance innovation with privacy protection, allowing controlled data reuse while preventing unauthorized access or discriminatory AI outcomes. Companies must navigate complex compliance requirements when leveraging AI for large-scale data analysis.

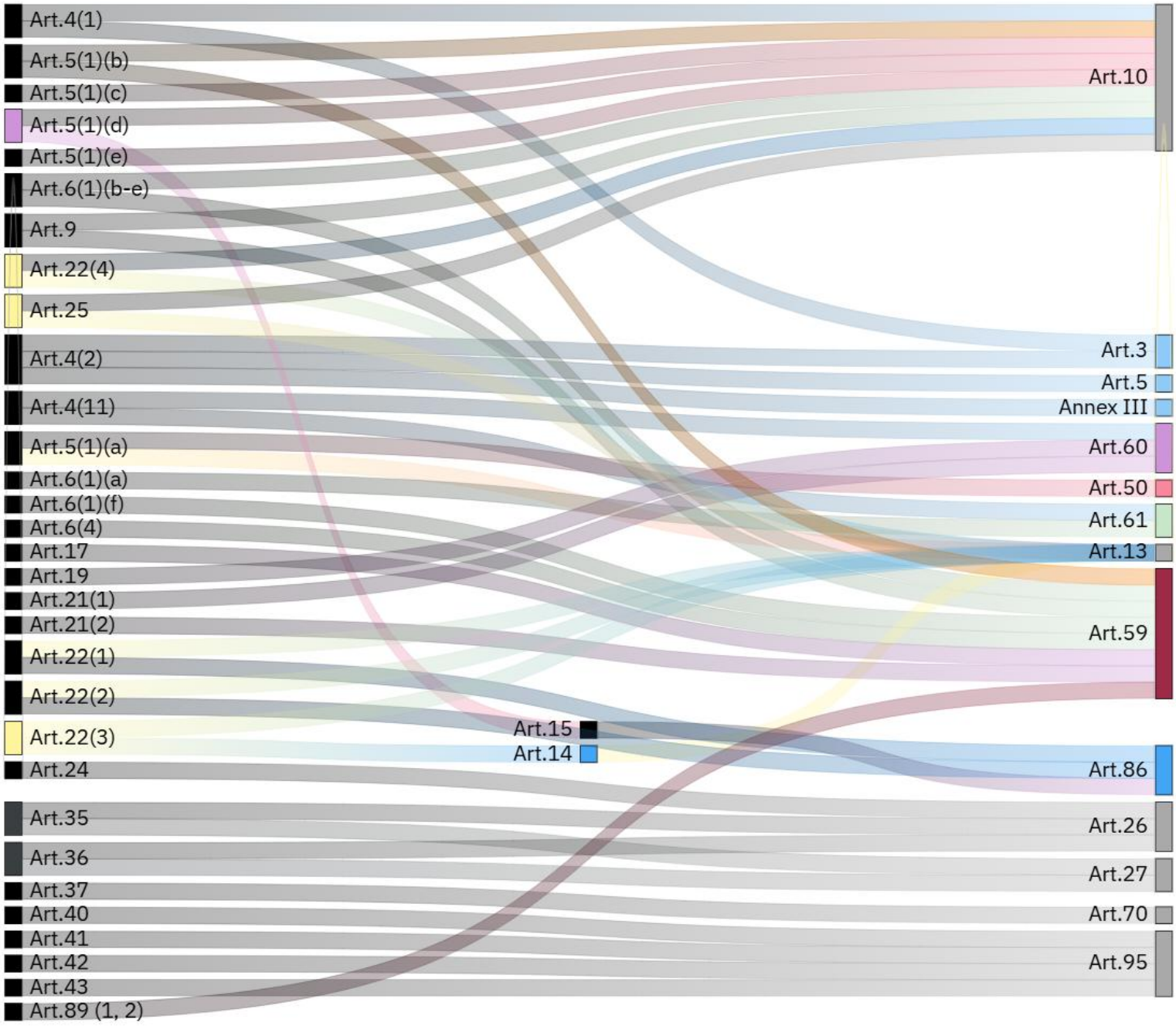
Why does it arise?

AI's ability to extract insights from vast datasets challenges traditional data protection principles like purpose limitation and data minimization. Regulatory frameworks arise to enable responsible data use while mitigating risks such as re-identification, bias, and unfair commercial exploitation. The EU's cautious approach reflects its commitment to both innovation and fundamental rights in AI governance.

Mapping GDPR to EU AI Act

GDPR

EU AI Act



GDPR		EU AI Act		
Reference	Title	Provision(s)	Explanation	Action
4(1):	Personal data (identification, identifiability, re-identification)	Articles **3** (Definitions) and **10** (Data and data governance)	**Alignment with GDPR**: The definition of personal data in the EU AI Act mirrors that of the GDPR, ensuring consistency in how personal data is treated across different regulations. This is crucial for maintaining the integrity of data protection standards when AI systems process personal data. **Data Governance Requirements**: Article 10 of the EU AI Act requires that data sets used in AI systems are managed in a way that respects the principles of data protection, including the minimization of identifiability and re-identification risks. This is directly relevant to the GDPR's focus on protecting personal data from unauthorized identification or re-identification.	**Conduct a Data Protection Impact Assessment (DPIA)**: Enterprises should perform a DPIA to evaluate the risks associated with the processing of personal data by AI systems. This assessment should focus on identifying potential risks of re-identification and implementing measures to mitigate these risks, such as data anonymization or pseudonymization techniques.
4(2)	Profiling	Articles **3** (Definitions), **5** (Prohibited AI Practices) and **Annex III** (High-risk AI systems)	**Consistency with GDPR**: The definition of profiling in the EU AI Act is consistent with the GDPR, ensuring that the same standards apply when AI systems process personal data for profiling purposes. This is crucial for maintaining data protection and privacy standards. **Prohibition and Risk Classification**: The EU AI Act explicitly prohibits certain profiling practices that could harm	**Implement Robust Compliance Measures**: Establish comprehensive compliance frameworks that ensure adherence to both the GDPR and the EU AI Act. This includes regular audits, transparency in profiling processes, and the implementation of technical and

			individuals or lead to discrimination. Additionally, profiling is classified as high-risk, requiring stringent compliance measures to protect individuals' rights and freedoms.	organizational measures to protect personal data.
4(11)	Consent	Articles **60** (Testing of high-risk AI systems) and **61** (Informed consent)	**Alignment with GDPR**: The concept of informed consent in the EU AI Act is consistent with GDPR Article 4(11), which defines consent as a freely given, specific, informed, and unambiguous indication of the data subject's wishes. The EU AI Act ensures that individuals are fully informed about the testing of AI systems and their rights, thereby aligning with GDPR's consent requirements. **Protection of Rights**: In requiring informed consent, the EU AI Act protects individuals' rights and ensures transparency in the testing of AI systems. This is crucial for maintaining trust and compliance with data protection standards.	**Document and Review Consent Procedures**: Ensure that consent is documented and regularly reviewed to maintain compliance with both the GDPR and the EU AI Act. This includes providing individuals with a copy of their consent and keeping records of consent for auditing purposes.
5(1)(a)	Farness, transparency	Articles **13** (Transparency and provision of information) and **50** (Transparency obligations)	**Fairness and Transparency**: Article 13 ensures that AI systems are transparent, allowing users to understand and trust the system's outputs, which aligns with GDPR's fairness and transparency principles. This is crucial for maintaining trust and ensuring that AI systems do not operate in a manner that is opaque or misleading.	**Implement Comprehensive Transparency Measures**: Enterprises should establish robust transparency frameworks that ensure users are informed about the AI systems they interact with. This includes providing clear information about how AI systems

			Disclosure of AI-Generated Content: Article 50 requires that AI-generated or manipulated content be disclosed, which supports transparency by informing users about the nature of the content they are interacting with. This aligns with the GDPR's emphasis on transparency, ensuring that individuals are aware of when they are engaging with AI systems.	process data and make decisions.
5(1)(b)	Purpose limitation	Article **10** (Data and data governance)	**Purpose Limitation**: Article 10 of the EU AI Act requires that data used in AI systems is relevant and necessary for the intended purpose. This aligns with GDPR's purpose limitation principle, which mandates that personal data be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. By ensuring that data governance practices are in place, the EU AI Act supports the adherence to purpose limitation by restricting data use to what is necessary for the AI system's intended function.	**Develop and Implement Data Governance Policies**: Enterprises should establish robust data governance frameworks that ensure compliance with both the GDPR and the EU AI Act. This includes defining clear purposes for data collection and processing, ensuring that data use is limited to these purposes, and regularly reviewing data processing activities to ensure they remain aligned with the stated purposes.
5(1)(c)	Data minimisation	Article **10** (Data and data governance)	**Data Minimization**: Article 10 of the EU AI Act requires that data used in AI systems is relevant and necessary for the intended purpose. This aligns with GDPR's data minimization principle, which mandates that	**Conduct Regular Audits**: Regularly audit data processing activities to ensure that they comply with the data minimization principle. This

			personal data be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed. By ensuring that data governance practices are in place, the EU AI Act supports the adherence to data minimization by restricting data use to what is necessary for the AI system's intended function.	involves verifying that data is only used for its intended purpose and that any further processing is compatible with the original purpose.
5(1)(d)	Accuracy	Articles **10** (Data and data governance) and **15** (Accuracy, robustness, and cybersecurity)	**Accuracy**: Article 15 of the EU AI Act requires high-risk AI systems to maintain an appropriate level of accuracy, which directly aligns with GDPR's accuracy principle. This ensures that AI systems produce reliable and precise outputs, minimizing errors that could affect individuals' rights. **Data Quality**: Article 10 supports the accuracy principle by requiring that data used in AI systems be of high quality, relevant, and accurate. This is crucial for training AI systems to perform accurately and avoid biases or errors that could lead to incorrect or misleading outputs.	**Implement Data Quality Assurance Processes**: Enterprises should establish robust data quality assurance processes to ensure that the data used in AI systems is accurate and reliable. This includes regular data audits, validation checks, and updates to maintain data integrity.
5(1)(e)	Storage limitation	Article **10** (Data and data governance)	**Storage Limitation**: The GDPR's storage limitation principle requires that personal data be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Although the	**Implement Data Retention Policies**: Enterprises should establish clear data retention policies that define how long data will be stored and the criteria for data deletion. This includes regular

			EU AI Act does not explicitly address storage limitation, Article 10's focus on data governance and management practices implies that data should not be retained longer than necessary, aligning with the GDPR's principle. This ensures that data is only kept for as long as it is needed for the AI system's intended purpose, thereby minimizing unnecessary data retention.	reviews of data retention practices to ensure compliance with both the GDPR and the EU AI Act.
6(1)(a)	Consent	Article **61** (Informed consent)	**Consent Alignment**: Article 61 of the EU AI Act aligns with GDPR Article 6(1)(a) by requiring that consent be freely given, specific, informed, and unambiguous. This ensures that individuals are fully aware of the nature and objectives of the AI system testing and their rights, thereby aligning with GDPR's consent requirements. The emphasis on informed consent in the AI Act is crucial for maintaining transparency and protecting individuals' rights when their data is used in AI system testing.	**Document and Review Consent Procedures**: Ensure that consent is documented and regularly reviewed to maintain compliance with both the GDPR and the EU AI Act. This includes providing individuals with a copy of their consent and keeping records of consent for auditing purposes.
6(1)(b-e)	Necessity	Articles **10** (Data and data governance) and **59** (AI Regulatory sandboxes)	**Necessity in Data Processing**: Article 10 of the EU AI Act requires that data used in AI systems is relevant and necessary for the intended purpose. This aligns with GDPR's necessity principle, which mandates that personal data processing should be limited to what is necessary for the	**Conduct Necessity Assessments**: Enterprises should conduct assessments to determine the necessity of data processing activities. This involves evaluating whether the data being processed is essential for

			purposes for which it is processed. By ensuring that data governance practices are in place, the EU AI Act supports the adherence to necessity by restricting data use to what is essential for the AI system's intended function. **AI Regulatory Sandboxes**: Article 59 allows for the processing of personal data in AI regulatory sandboxes when it is necessary for developing AI systems that serve substantial public interests. This provision ensures that data processing is justified by the necessity to achieve specific public interest objectives, aligning with the necessity principle.	achieving the intended purpose of the AI system and ensuring that no more data than necessary is collected or processed.
6(1)(f)	Legitimate interest	Article **59** (AI Regulatory sandboxes)	**Legitimate Interest in Data Processing**: Article 59 of the EU AI Act aligns with the concept of legitimate interest by allowing the processing of personal data in AI regulatory sandboxes for purposes that serve substantial public interests, such as public safety, health, and environmental protection. This provision ensures that data processing is justified by a legitimate interest that outweighs the potential risks to individuals' rights and freedoms. The conditions set forth in Article 59, such as ensuring data protection and monitoring mechanisms, support the balancing test	**Conduct a Legitimate Interest Assessment (LIA)**: Enterprises should perform an LIA to evaluate whether the processing of personal data in AI systems is necessary and proportionate to achieve the intended legitimate interest. This assessment should consider the potential impact on individuals' rights and freedoms and include measures to mitigate any identified risks.

			required under GDPR Article 6(1)(f).	
6(4)	Repurposing	Article **59** (AI Regulatory sandboxes)	**Repurposing of Data**: Article 59 of the EU AI Act aligns with the concept of repurposing under GDPR Article 6(4) by allowing personal data collected for one purpose to be processed for another purpose within the AI regulatory sandbox. This is permissible when the processing is necessary for developing AI systems that serve substantial public interests, such as public safety or health. The conditions outlined in Article 59 ensure that such repurposing is conducted with appropriate safeguards, aligning with GDPR's requirements for repurposing data.	**Implement Data Protection Measures**: Establish robust data protection measures to ensure compliance with both the GDPR and the EU AI Act. This includes implementing technical and organizational safeguards, such as data anonymization or pseudonymization, to protect personal data during repurposing.
9	Special categories of data	Articles **10** (Data and data governance) and **59** (AI Regulatory sandboxes)	**Processing Special Categories of Data**: Article 10 of the EU AI Act permits the processing of special categories of personal data when it is necessary for ensuring the accuracy and fairness of high-risk AI systems. This aligns with GDPR Article 9, which restricts processing such data unless specific conditions are met. The EU AI Act requires that such processing be accompanied by technical and organizational safeguards, including pseudonymization and data protection measures, to protect individuals' rights and freedoms.	**Implement Robust Data Protection Measures**: Establish comprehensive data protection frameworks that ensure compliance with both the GDPR and the EU AI Act. This includes implementing technical and organizational measures to protect personal data, such as encryption, access controls, and regular audits.

			AI Regulatory Sandboxes: Article 59 allows for the processing of special categories of data within AI regulatory sandboxes, provided it serves a substantial public interest and complies with data protection laws. This provision ensures that the processing is justified and necessary for the development of AI systems that benefit society, aligning with GDPR's requirements for processing special categories of data.	
13 – 14	Information duties	Article **13** (Transparency and provision of information to deployers')	GDPR Article 13 outlines the information that must be provided to data subjects when personal data is collected. Similarly, the EU AI Act's Article 13 ensures that deployers of high-risk AI systems receive sufficient information to understand and manage the AI system effectively. This includes details about the system's intended purpose, performance characteristics, and any known risks, which parallels the GDPR's emphasis on transparency and informed consent..	**Implement Comprehensive Documentation**: Enterprises should develop and maintain detailed documentation for their AI systems, ensuring that all relevant information is accessible to deployers. This documentation should include the system's intended purpose, performance metrics, and any potential risks or limitations.
15	The right to access	Article **86** (A Right to Explanation of Individual Decision-Making)	GDPR Article 15 grants data subjects the right to access their personal data and obtain information about how it is being processed. Similarly, Article 86 of the EU AI Act ensures transparency by requiring deployers of high-risk AI systems to provide explanations of decisions that impact	**Establish Clear Communication Channels**: Enterprises should implement processes to provide individuals with access to explanations of AI-driven decisions. This includes setting up

			individuals. This aligns with the GDPR's emphasis on transparency and the individual's right to understand how their data is used in decision-making processes.	dedicated communication channels where individuals can request and receive detailed explanations about how AI systems have influenced decisions affecting them. By doing so, enterprises can ensure compliance with both the EU AI Act and GDPR, enhancing transparency and trust.
17	The right to erasure	Article 59 (Further Processing of Personal Data for Developing Certain AI Systems in the Public Interest in the AI Regulatory Sandbox)	GDPR Article 17 grants individuals the right to have their personal data erased under certain conditions, such as when the data is no longer necessary for the purposes for which it was collected. Similarly, Article 59 of the EU AI Act ensures that personal data processed within AI regulatory sandboxes is deleted once it is no longer needed, aligning with the GDPR's emphasis on data minimization and the right to erasure.	**Implement Data Deletion Protocols**: Enterprises should establish robust data deletion protocols to ensure compliance with both GDPR and the EU AI Act. This includes setting clear guidelines for the timely deletion of personal data once it is no longer necessary for the intended purpose, particularly in contexts like AI regulatory sandboxes. By doing so, enterprises can uphold individuals' rights to erasure and maintain trust in their data handling practices.
19	The right to portability	Article 60 (Testing of High-Risk AI Systems in Real World	GDPR Article 19 grants individuals the right to receive their personal	**Develop Data Portability Protocols**:

		Conditions Outside AI Regulatory Sandboxes)	data in a structured, commonly used, and machine-readable format, and to transmit that data to another controller. While the EU AI Act does not directly address data portability, Article 60 ensures that personal data used in testing high-risk AI systems is handled in compliance with data protection laws, which include the principles of data portability. This alignment ensures that personal data is managed in a way that respects individuals' rights under the GDPR.	Enterprises should establish protocols to facilitate data portability, ensuring that personal data processed by AI systems can be easily transferred in a structured and machine-readable format. This includes implementing systems that support data export and transfer functionalities, thereby aligning with both GDPR requirements and the EU AI Act's emphasis on data protection compliance.
21(1)	The right to object	Article 60 (Testing of High-Risk AI Systems in Real World Conditions Outside AI Regulatory Sandboxes)	GDPR Article 21(1) grants individuals the right to object to the processing of their personal data under certain conditions. While the EU AI Act does not directly address the right to object, Article 60 ensures that personal data used in testing high-risk AI systems is handled in compliance with data protection laws, which include the principles of data subject rights such as the right to object. This alignment ensures that personal data is managed in a way that respects individuals' rights under the GDPR.	**Establish Objection Handling Protocols**: Enterprises should implement protocols to handle objections from individuals regarding the processing of their personal data by AI systems. This includes setting up clear procedures for individuals to submit objections and ensuring that these objections are addressed promptly and effectively. By doing so, enterprises can ensure compliance

				with both GDPR requirements and the EU AI Act's emphasis on data protection compliance.
21(2)	Objecting to processing for research and statistical purposes	Article **59** (Further Processing of Personal Data for Developing Certain AI Systems in the Public Interest in the AI Regulatory Sandbox)	GDPR Article 21(2) allows individuals to object to the processing of their personal data for research and statistical purposes unless the processing is necessary for the performance of a task carried out for reasons of public interest. Similarly, Article 59 of the EU AI Act ensures that personal data processed within AI regulatory sandboxes is done so under strict conditions that protect data subjects' rights. This includes ensuring that the processing does not affect the application of their rights under Union law on data protection, aligning with the GDPR's emphasis on the right to object.	**Implement Objection Handling Mechanisms**: Enterprises should establish mechanisms to handle objections from individuals regarding the processing of their personal data for research and statistical purposes. This includes setting up clear procedures for individuals to submit objections and ensuring that these objections are addressed promptly and effectively. By doing so, enterprises can ensure compliance with both GDPR requirements and the EU AI Act's emphasis on data protection compliance.
22(1)	The prohibition of automated decisions	Articles **13** (Transparency and provision of information to deployers) and **86** (A Right to Explanation of Individual Decision-Making)	GDPR Article 22(1) prohibits decisions based solely on automated processing, including profiling, that significantly affect individuals. The EU AI Act's Article 13 ensures transparency in high-risk AI systems, which is crucial for understanding and potentially contesting automated decisions.	**Implement Transparency and Explanation Protocols**: Enterprises should establish protocols to ensure transparency in their AI systems, particularly those classified as high-risk. This includes

			Article 86 further aligns with GDPR by providing individuals the right to explanations of AI-driven decisions, ensuring that they are not left in the dark about how decisions affecting them are made.	providing clear documentation and explanations of how AI systems make decisions. By doing so, enterprises can ensure compliance with both GDPR and the EU AI Act, empowering individuals to understand and, if necessary, contest automated decisions that affect them.
22(2)	Exceptions to the prohibition of 22(1)	Articles **13** (Transparency and provision of information to deployers) and **86** (A Right to Explanation of Individual Decision-Making)	GDPR Article 22(2) allows for exceptions to the prohibition of automated decision-making if certain conditions are met, such as when the decision is necessary for entering into or performing a contract, is authorized by Union or Member State law, or is based on explicit consent. The EU AI Act's Article 13 ensures transparency in high-risk AI systems, which is crucial for understanding and potentially contesting automated decisions. Article 86 further aligns with GDPR by providing individuals the right to explanations of AI-driven decisions, ensuring that they are informed and can exercise their rights effectively.	**Implement Consent and Transparency Protocols**: Enterprises should establish protocols to ensure that any automated decision-making processes comply with the exceptions outlined in GDPR Article 22(2). This includes obtaining explicit consent from individuals where necessary and providing clear documentation and explanations of how AI systems make decisions. By doing so, enterprises can ensure compliance with both GDPR and the EU AI Act, empowering individuals to understand and, if necessary, contest automated

				decisions that affect them.
22(3)	Safeguard measures	Articles **13** (Transparency and provision of information to deployers) and **14** (Human oversight)	GDPR Article 22(3) requires that appropriate safeguards be in place for individuals subject to automated decision-making, including the right to obtain human intervention, express their point of view, and contest the decision. The EU AI Act's Article 13 ensures transparency, which is essential for understanding and contesting automated decisions. Article 14 provides for human oversight, allowing for intervention and ensuring that decisions are not made solely by automated means without human review.	**Implement Human Oversight and Transparency Protocols**: Enterprises should establish protocols to ensure that high-risk AI systems are transparent and subject to human oversight. This includes providing clear documentation and instructions for use, as well as mechanisms for human intervention in decision-making processes. By doing so, enterprises can ensure compliance with both GDPR and the EU AI Act, safeguarding individuals' rights in the context of automated decision-making.
22(4)	Automated decision-making and sensitive data	Articles **10** (Data and data governance) and **13** (Transparency and provision of information to deployers)	GDPR Article 22(4) addresses the conditions under which automated decision-making involving sensitive data can occur. The EU AI Act's Article 10 provides guidelines for handling sensitive data, ensuring that such data is processed with appropriate safeguards to protect fundamental rights. Article 13 ensures transparency, which is essential for understanding and managing the implications	**Implement Robust Data Governance and Transparency Measures**: Enterprises should establish comprehensive data governance protocols to ensure that sensitive data is processed in compliance with both GDPR and the EU AI Act. This includes implementing

			of automated decisions involving sensitive data. These provisions align with GDPR's emphasis on protecting sensitive data in automated decision-making processes.	transparency measures to provide clear information about how sensitive data is used in automated decision-making processes. By doing so, enterprises can safeguard individuals' rights and maintain trust in their data handling practices.
24	Responsibility of the controller	Articles **24** (Obligations of Distributors) and **26** (Obligations of Deployers of High-Risk AI Systems)	GDPR Article 24 requires controllers to implement appropriate technical and organizational measures to ensure and demonstrate that processing is performed in accordance with the regulation. Similarly, Article 24 of the EU AI Act requires distributors to ensure that high-risk AI systems comply with regulatory requirements, while Article 26 requires deployers to monitor and manage the use of these systems. Both articles emphasize the responsibility of entities involved in the AI lifecycle to ensure compliance and accountability, aligning with the GDPR's focus on the controller's responsibility for data protection.	**Establish Compliance and Monitoring Protocols**: Enterprises should implement robust compliance and monitoring protocols to ensure that high-risk AI systems are used in accordance with regulatory requirements. This includes verifying conformity before deployment, continuously monitoring system performance, and taking corrective actions when necessary. By doing so, enterprises can ensure compliance with both GDPR and the EU AI Act, maintaining accountability and protecting individuals' rights.

25	Data protection by design and by default	Articles **10** (Data and data governance) and **13** (Transparency and provision of information to deployers)	GDPR Article 25 requires data controllers to implement appropriate technical and organizational measures to ensure data protection principles are integrated into processing activities. The EU AI Act's Article 13 ensures transparency and proper documentation, which are essential for embedding data protection into the design of AI systems. Article 10 emphasizes data governance, ensuring that data protection principles are considered throughout the lifecycle of high-risk AI systems. These provisions align with GDPR's focus on integrating data protection measures from the outset.	**Implement Data Protection Measures in AI Design**: Enterprises should establish protocols to ensure that data protection principles are integrated into the design and development of AI systems. This includes implementing transparency measures, comprehensive documentation, and robust data governance practices. By doing so, enterprises can ensure compliance with both GDPR and the EU AI Act, safeguarding individuals' data protection rights from the outset.
35 – 36	Data protection impact assessment	Articles **26** (Obligations of Deployers of High-Risk AI Systems) and **27** (Fundamental Rights Impact Assessment for High-Risk AI Systems)	GDPR Article 36 mandates that data controllers conduct a DPIA when processing operations are likely to result in a high risk to the rights and freedoms of individuals. The EU AI Act's Article 27 requires a fundamental rights impact assessment for high-risk AI systems, which aligns with the objectives of a DPIA by ensuring that potential risks to individuals' rights are assessed and mitigated. Article 26 further supports this by requiring deployers to use relevant information to	**Conduct Comprehensive Impact Assessments**: Enterprises should establish protocols to conduct both data protection and fundamental rights impact assessments for high-risk AI systems. This includes using the information provided by AI system providers to assess potential risks and implementing measures to

			conduct a DPIA, ensuring compliance with GDPR.	mitigate those risks. By doing so, enterprises can ensure compliance with both GDPR and the EU AI Act, safeguarding individuals' rights and maintaining trust in their AI systems.
37	Data protection officers	Article **70** (Designation of National Competent Authorities and Single Point of Contact)	GDPR Article 37 requires certain organizations to appoint a data protection officer to oversee data protection strategies and ensure compliance with GDPR requirements. Similarly, Article 70 of the EU AI Act emphasizes the need for national competent authorities to have personnel with expertise in personal data protection. This alignment ensures that both the GDPR and the EU AI Act prioritize the presence of knowledgeable individuals or bodies to oversee data protection and compliance efforts.	**Appoint a Data Protection Officer**: Enterprises should appoint a data protection officer if required under GDPR Article 37. This officer should have the necessary expertise in data protection laws and practices to ensure compliance with both GDPR and the EU AI Act. The DPO should work closely with relevant authorities and ensure that the enterprise's AI systems are compliant with data protection regulations.
40 – 43	Codes of conduct and certification	Article **95** (Codes of Conduct for Voluntary Applica on of Specific Requirements)	GDPR Article 40 encourages the development of codes of conduct to help ensure compliance with data protection laws. Similarly, Article 95 of the EU AI Act promotes the creation of codes of conduct for AI systems, aiming to foster voluntary compliance with certain requirements. Both articles emphasize the	**Participate in Developing Codes of Conduct**: Enterprises should actively participate in the development and adoption of codes of conduct for AI systems. This involves collaborating with industry peers, stakeholders, and

			role of codes of conduct in enhancing compliance and governance, involving stakeholders in their development to ensure they are comprehensive and effective.	regulatory bodies to create guidelines that ensure compliance with both GDPR and the EU AI Act. By doing so, enterprises can contribute to the establishment of best practices and enhance their compliance frameworks.
5(1)(b)	Repurposing for research and statistical processing	Article 59 (Further Processing of Personal Data for Developing Certain AI Systems in the Public Interest in the AI Regulatory Sandbox)	GDPR Article 5(1)(b) emphasizes that personal data should be collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes. However, further processing for research and statistical purposes is generally considered compatible. Similarly, Article 59 of the EU AI Act allows for the repurposing of personal data within AI regulatory sandboxes, provided it serves substantial public interest and complies with data protection laws. This alignment ensures that data repurposing for research and statistical purposes is conducted with appropriate safeguards.	**Implement Data Governance Protocols**: Enterprises should establish robust data governance protocols to ensure that any repurposing of personal data for research and statistical purposes complies with both GDPR and the EU AI Act. This includes ensuring that data processing is necessary, serves a substantial public interest, and is accompanied by appropriate safeguards to protect data subjects' rights. By doing so, enterprises can maintain compliance and foster trust in their data handling practices.
89 (1, 2)	Safeguards for research of	Article 59 (Further Processing of Personal Data for	GDPR Article 89(1, 2) requires that appropriate safeguards are in place	**Implement Robust Safeguards and Governance**

	statistical processing	Developing Certain AI Systems in the Public Interest in the AI Regulatory Sandbox)	when processing personal data for research and statistical purposes, ensuring that data subjects' rights and freedoms are protected. Similarly, Article 59 of the EU AI Act allows for the repurposing of personal data within AI regulatory sandboxes, provided it serves substantial public interest and complies with data protection laws. This alignment ensures that data repurposing for research and statistical purposes is conducted with appropriate safeguards, protecting individuals' rights.	**Protocols**: Enterprises should establish comprehensive data governance protocols to ensure that any repurposing of personal data for research and statistical purposes complies with both GDPR and the EU AI Act. This includes implementing appropriate technical and organizational measures to protect data subjects' rights and freedoms. By doing so, enterprises can maintain compliance and foster trust in their data handling practices.

Calls to action

1. Build Privacy-First AI Systems

Ensure compliance with AI regulations by embedding data protection principles into your AI design. Strengthen privacy by design to balance innovation with legal and ethical obligations.

2. Navigate the AI and Data Protection Landscape

AI regulation is reshaping data protection standards. Stay ahead by understanding how laws like the GDPR and AI Act impact AI-driven data processing and statistical research.

3. Turn Compliance into Competitive Advantage

Adapt to evolving AI and data protection regulations by implementing best practices for data minimization, pseudonymization, and lawful repurposing. Protect user privacy while driving AI innovation.

4. Future-Proof Your AI and Data Strategy

Don’t let regulatory uncertainty slow you down. Develop a compliant, responsible AI strategy that aligns with global data protection laws and fosters trust in AI-driven decision-making.

Conclusion

The rise of AI regulation marks a pivotal shift in ensuring structured, ethical, and accountable data governance. As organizations seek to harness AI's potential while safeguarding sensitive information, evolving legal frameworks—such as the EU AI Act and stricter GDPR enforcement—provide essential guidance for mitigating AI-related privacy risks. By emphasizing transparency, accountability, and data protection, these regulations are reshaping industry best practices and reinforcing global efforts toward responsible AI deployment.

However, the effectiveness of AI regulations will depend on how well organizations implement compliance measures. Businesses face varying levels of preparedness, with challenges including aligning AI systems with data protection laws, ensuring adequate oversight, and balancing regulatory requirements with operational agility. Small and medium enterprises (SMEs), in particular, may require additional support to integrate privacy-preserving AI governance while remaining competitive in an evolving regulatory landscape.

Despite these challenges, early adopters are already demonstrating the benefits of proactive compliance. Technology firms, financial institutions, and healthcare providers are enhancing AI transparency, reducing privacy risks, and strengthening public trust by embedding robust data protection measures into their AI ecosystems. By implementing risk assessments, ethical safeguards, and continuous monitoring, these organizations illustrate how a structured approach can improve both regulatory alignment and operational efficiency.

For businesses and policymakers alike, AI regulation presents a unique opportunity to establish leadership in responsible AI governance. Developing clear policies, investing in privacy-first AI strategies, and fostering cross-sector collaboration will be critical in driving widespread compliance. As AI-driven decision-making continues to expand, these regulations provide a foundation for ensuring AI remains secure, reliable, and aligned with societal expectations.

Looking ahead, the long-term impact of AI regulations will depend on industry-wide engagement, the refinement of best practices, and the integration of AI governance with broader data protection laws. Organizations that proactively adapt to regulatory shifts will position themselves at the forefront of ethical and sustainable AI development, setting a global benchmark for privacy-conscious AI adoption.

About AI & Partners

AI & Partners

Amsterdam - London - Singapore

AI & Partners – 'AI That You Can Trust'

At AI & Partners, we're here to help you navigate the complexities of the EU AI Act, so you can focus on what matters—using AI to grow your business. We specialize in guiding companies through compliance with tailored solutions that fit your needs. Why us? Because we combine deep AI expertise with practical, actionable strategies to ensure you stay compliant and responsible, without losing sight of your goals. With our support, you get AI you can trust—safe, accountable, and aligned with the law.

To find out how we can help you, email contact@ai-and-partners.com or visit https://www.ai-and-partners.com.

Contacts

Sean Donald John Musch, CEO/Founder, s.musch@ai-and-partners.com

Michael Charles Borrelli, Director, m.borrelli@ai-and-partners.com

Authors

Sean Donald John Musch, CEO/Founder

Michael Charles Borrelli, Director

References

European Parliament and The Council of the European Union, (2016), 'Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)', accessible at: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng (last accessed 29th March 2025)

European Parliament and The Council of the European Union, (2024), 2024/1689 Regulation (EU) 2024/1689 of the European Parliament and of The Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), accessible at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401689 (last accessed 29th March 2025)

Important notice

This document has been prepared by AI & Partners B.V. for the sole purpose of enabling the parties to whom it is addressed to evaluate the capabilities of AI & Partners B.V. to supply the proposed services.

Other than as stated below, this document and its contents are confidential and prepared solely for your information, and may not be reproduced, redistributed or passed on to any other person in whole or in part. If this document contains details of an arrangement that could result in a tax or National Insurance saving, no such conditions of confidentiality apply to the details of that arrangement (for example, for the purpose of discussion with tax authorities). No other party is entitled to rely on this document for any purpose whatsoever and we accept no liability to any other party who is shown or obtains access to this document.

This document is not an offer and is not intended to be contractually binding. Should this proposal be acceptable to you, and following the conclusion of our internal acceptance procedures, we would be pleased to discuss terms and conditions with you prior to our appointment. Images used throughout the document have either been produced in-house or sourced from publicly available sources (see **References** for details).

AI & Partners B.V. is the Dutch headquarters of AI & Partners, a global professional services firm. Please see https://www.ai-and-partners.com/ to learn more about us.

Designed and produced by AI & Partners B.V