AI & Partners

Amsterdam - London - Singapore

EU AI Act

Advancing Data Governance

How Article 10 (Data and data governance) of the EU AI Act supports the Data Governance Act's objective of increasing trust in data sharing, strengthening mechanisms to increase data availability, and overcoming technical obstacles to the reuse of data with respect to AI systems.

September 2025

AI & Partners

Sean Musch, AI & Partners

Michael Borrelli, AI & Partners

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.

AI & Partners

Amsterdam - London - Singapore

Who Are We

AI That You Can Trust

Why Us?

Stay on the right side of history. At AI & Partners, we believe AI should unlock potential—not cause harm. We've seen the fear and fallout when teams lose control of AI, but also the trust and innovation that follow when it's handled responsibly. That's why we exist: to help you build AI you can trust and stand behind—for the long run.

80%

of AI systems are unknown

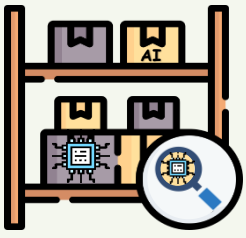
What Do We Do?

We enable safe AI usage—for your organization and your clients. Unknown AI adoption leads to confusion, risk, and reputational damage. We help you take control with tools to identify, monitor, and govern all AI systems—so you're not reacting to AI, you're leading it.

How Do We Do It?

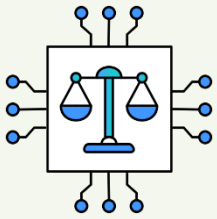
Do you know what AI systems you have? Identify all known and unknown AI systems (algorithms, LLMs, prompts, and models) from all internal and external AI vendors, automated by generating your inventory. Overall, 80% of AI inventory is unknown to our clients.

How do you guarantee ongoing safe AI use? Continuously monitor deployed AI systems for performance drift, anomalies or failures, real-world impacts, and emerging risks (e.g. data poisoning). Any malfunction of an AI system has severe implications for organisations (e.g. inability to assess online misinformation that leads to widespread public mistrust), so monitoring becomes a matter of urgency.



AI Discovery & AI Inventory

Automatically detect all AI systems, including models, algorithms, and prompts, and maintain a live, always-updated register for full visibility and compliance.



Responsible AI

Embed fairness, transparency, and control into every stage of AI use—aligning with the EU AI Act and building 'Trustworthy-by-Design'.

Model Monitoring

Continuously track your AI models after deployment to detect drift, bias, or failure—so you stay in control and prevent harm before it happens.

Our data finds that Article 10 of the EU AI Act aligns with the Data Governance Act by fostering trust in data sharing for AI systems through transparency and accountability. It mandates robust data governance practices, including ensuring data quality, representativeness, and integrity during AI training. This supports the objective of increasing data availability by requiring that datasets used in AI systems are properly documented and accessible. Furthermore, Article 10 addresses technical obstacles to data reuse by promoting interoperability and traceability, enabling secure and efficient sharing. These measures enhance the reliability of AI systems and contribute to a trustworthy framework for innovation in the European data economy.

About this report

This report is based on market research, publicly available data, and interviews with AI specialists in AI & Partners, financial services organisations, and relevant third-parties. Moreover, quotations provided on specific topics reflect those of AI specialists at AI & Partners to be as representative as possible of real-world conditions. All references to EU AI Act reflect the version of text valid as at 13 June 2024. Accessible here.

Contents

Executive Summary

The increasing integration of artificial intelligence (AI) systems into critical aspects of society underscores the need for robust data governance.

AI systems rely heavily on data to function effectively, making the quality, accessibility, and security of that data essential for their success. Recognizing this, the European Union has established a dual regulatory framework: the **Data Governance Act (DGA)** and the **AI Act**, each designed to address specific challenges in the data-driven economy. Central to this alignment is **Article 10 of the AI Act**, which emphasizes data governance and supports the broader objectives of the DGA.

This introduction explores how Article 10 advances the goals of the DGA by building trust in data sharing, increasing data availability, and addressing barriers to data reuse. Together, these frameworks foster a secure and innovative data ecosystem while safeguarding European values of privacy, transparency, and fairness.

Data Governance: A Pillar of the EU's Digital Strategy

The DGA, effective since September 2023, represents a cornerstone of the European data strategy. It provides a structured framework for unlocking the potential of data across Member States and sectors while maintaining high standards of security and ethical compliance. The DGA's objectives include:

- **Building Trust in Data Sharing:** Ensuring that data is exchanged securely and transparently to foster confidence among stakeholders.
- **Increasing Data Availability:** Facilitating access to datasets held by public and private entities to fuel innovation and research.
- **Overcoming Technical Barriers:** Promoting interoperability and standardized approaches to enable seamless data reuse.

At its core, the DGA aims to create **Common European Data Spaces**—secure environments where data can be shared and pooled for strategic purposes. These spaces serve critical domains such as healthcare, mobility, environment, and agriculture, driving collaboration and innovation across sectors.

AI Regulation: Ensuring Safe and Ethical Systems

The EU AI Act complements the DGA by focusing on the responsible development and deployment of AI systems. Article 10, in particular, sets out data governance requirements for high-risk AI systems, mandating the use of high-quality, representative, and secure datasets. This ensures that AI systems operate fairly and effectively, aligning with EU principles of trust and accountability.

Article 10's key provisions include:

- Ensuring datasets are relevant, representative, and free from significant errors.
- Requiring safeguards to detect and mitigate biases that may result in discrimination or harm.
- Establishing secure mechanisms for processing sensitive data, such as pseudonymization and encryption.

These measures align with the DGA's emphasis on trust and data quality, creating a cohesive regulatory environment for AI innovation.

The Importance of Synergy Between the DGA and AI Act

As a result of integrating data governance with AI regulation, the EU addresses critical challenges in the digital economy. The DGA and Article 10 work in tandem to:

- Provide citizens with greater control over their data, fostering public confidence in data-sharing ecosystems.
- Enable businesses, particularly SMEs, to access high-quality data, reducing costs and driving innovation.
- Support societal goals through data-driven advancements in healthcare, environmental protection, and public administration.

This collaborative approach positions Europe as a global leader in ethical data governance and AI innovation, setting a benchmark for other regions to follow.

Introduction

The rapid integration of artificial intelligence (AI) systems into daily life underscores the importance of robust data governance. Data is a cornerstone of AI, serving as the foundation for training, validation, and optimization.

For example, the European Commission's research (2024)[1] shows that, since 2021, the number of key data companies using artificial intelligence increased annually by 10% (from 39 companies in 2021 to 52 in 2024). Recognizing this, the European Union has implemented a dual framework: the **Data Governance Act (DGA)**, aimed at creating a secure, interoperable, and trusted data-sharing ecosystem, and the **AI Act**, which sets regulatory parameters for safe and ethical AI deployment. Central to this synergy is Article 10 of the AI Act, which directly supports the objectives of the DGA by increasing trust in data sharing, enhancing data availability, and addressing technical obstacles to data reuse.

This introduction provides a comprehensive overview of how Article 10 complements the DGA's mission and lays the groundwork for fostering a resilient data economy in line with EU values and principles. By examining its regulatory goals, mechanisms, and implications, this paper establishes the foundational context for understanding the integration of data governance and AI regulation in the European Union.

Data Governance Act: A Pillar of the European Data Strategy

The Data Governance Act, effective since September 2023, is a pivotal component of the EU's data strategy. Designed to unlock the economic and societal potential of data, the DGA establishes a framework for secure, transparent, and equitable data sharing across sectors and Member States. Its objectives include:

1. **Building Trust in Data Sharing:** Introducing measures to ensure data security and privacy, thereby fostering confidence among individuals and organizations in sharing their data.
2. **Expanding Data Availability:** Creating mechanisms to facilitate access to vast datasets held by public and private entities.
3. **Overcoming Technical Barriers:** Addressing interoperability challenges and promoting standardized approaches to enable seamless data reuse.

The DGA facilitates the development of Common European Data Spaces across strategic domains—such as healthcare, agriculture, mobility, and public administration—to foster collaboration and innovation. These data spaces provide a unified infrastructure that aligns with EU principles of transparency, privacy, and data sovereignty.

AI Act and Data Governance: A Symbiotic Relationship

The AI Act introduces a harmonized regulatory framework to ensure that AI systems deployed in the EU are safe, transparent, and respectful of fundamental rights. Article 10 of the AI Act is particularly significant as it emphasizes the governance and management of data used in high-risk AI systems. It mandates that datasets are of high quality, representative, and free of errors, with specific safeguards to address biases and protect privacy.

[1] **European Commission**, (2024), 'The European Data Market study 2024-2026', accessible at: https://digital-strategy.ec.europa.eu/en/library/european-data-market-study-2024-2026 (last accessed 9th December 2024)

This provision aligns seamlessly with the DGA's objectives:

1. **Increasing Trust:** By establishing stringent requirements for data processing in AI, Article 10 enhances public confidence in how data is used, particularly in high-risk applications such as healthcare or finance.
2. **Strengthening Availability:** It ensures that relevant and high-quality datasets are accessible, enabling better AI training and innovation.
3. **Overcoming Obstacles:** Through technical and procedural safeguards, Article 10 addresses barriers to data reuse, fostering an interoperable and collaborative data-sharing ecosystem.

Importance of Data in High-Risk AI Systems

Data is the lifeblood of AI systems, influencing their accuracy, reliability, and fairness. High-risk AI systems, such as those used in critical sectors like healthcare or legal decision-making, require datasets that adhere to stringent governance standards. Article 10 specifies key requirements for such datasets, including:

- **Relevance and Representation:** Ensuring that datasets reflect the demographic or contextual settings of their intended application.
- **Bias Detection and Correction:** Implementing safeguards to identify and mitigate biases that could lead to discrimination or unfair outcomes.
- **Secure Handling of Sensitive Data:** Processing personal or sensitive data under strict conditions, with advanced technical measures like pseudonymization and encryption.

These principles ensure that high-risk AI systems not only comply with legal standards but also operate ethically and effectively, fostering greater trust in AI-driven solutions.

Article 10: Supporting the Objectives of the Data Governance Act

Figure 1: Data Governance Act Objectives

1. Increasing Trust in Data Sharing

Trust is central to the success of any data-sharing framework. Article 10 contributes to this by ensuring that data used in AI systems is managed transparently and securely. Providers are required to document the origin, processing, and preparation of datasets, offering full traceability. This builds confidence among stakeholders, from individual data contributors to businesses and regulatory bodies.

Additionally, the provision mandates measures to prevent misuse of sensitive data, such as restricting access to authorized personnel and implementing technical safeguards. By aligning with the DGA's emphasis on secure data-sharing mechanisms, Article 10 reinforces trust across the data ecosystem.

2. Strengthening Data Availability

High-quality data is a critical resource for AI innovation. Article 10 encourages the reuse of existing datasets by addressing gaps and shortcomings that may hinder compliance. Providers are urged to supplement incomplete datasets with additional sources or synthetic data, ensuring robust training environments for AI systems.

This proactive approach mirrors the DGA's goal of expanding data availability. By facilitating access to diverse datasets—whether through public sector repositories or data intermediaries—both regulations create a fertile ground for data-driven innovation.

3. Overcoming Technical Obstacles to Data Reuse

Interoperability and standardization are recurring challenges in data governance. Article 10 specifies that datasets must meet certain statistical and technical standards, promoting consistency across AI applications. Moreover, it advocates for collaboration with trusted data intermediaries, as envisioned by the DGA, to pool and share data in a neutral and secure manner.

As a result of harmonizing technical practices, these measures reduce fragmentation in the data ecosystem, enabling seamless reuse and cross-sector applications of data.

Impact on Stakeholders

Figure 2: Impact on stakeholders

Citizens

Businesses

Society

1. Citizens

For citizens, the integration of the DGA and AI Act ensures that their data is handled with care and purpose. Mechanisms like data altruism allow individuals to voluntarily share their data for societal benefits, such as advancing medical research or combating climate change. Enhanced transparency under Article 10 reassures citizens that their contributions are used ethically and securely.

2. Businesses

Businesses, particularly SMEs, benefit from lower costs and reduced barriers to data access. The availability of high-quality datasets accelerates product development and fosters innovation, allowing firms to create AI-driven solutions tailored to market needs. For instance, mobility data can enable real-time navigation tools, saving time and resources for users and service providers alike.

3. Society

Society as a whole reaps the rewards of data-driven advancements in public services and policies. Evidence-based decisions informed by high-quality data enhance governance, emergency responses, and environmental sustainability. The integration of data governance principles ensures that these benefits are distributed equitably and transparently.

Challenges and Future Directions

While the DGA and AI Act offer a comprehensive framework, their implementation presents challenges. Ensuring cross-sector interoperability, addressing biases in AI systems, and maintaining compliance with privacy regulations require ongoing effort and collaboration.

Future developments may focus on:

- **Refining Technical Standards:** To address emerging technologies and complex data-sharing scenarios.
- **Enhancing Public Awareness:** Educating citizens about data altruism and their rights under the DGA and AI Act.
- **Promoting International Collaboration:** Aligning EU standards with global data governance practices to foster a cohesive digital ecosystem.

Conclusion

The European Data Governance Act and the AI Act, particularly Article 10, represent a transformative approach to data management and AI regulation. By fostering trust, enhancing data availability, and addressing technical barriers, these frameworks lay the foundation for a thriving data economy rooted in EU values.

Together, they empower citizens, businesses, and society to harness the full potential of data, driving innovation while safeguarding privacy and ethical principles. As implementation progresses, these regulations will not only bolster Europe's digital sovereignty but also set a global benchmark for responsible and inclusive data governance.

The European Data Governance Act: An Overview

The European Data Governance Act ("DGA"), a cornerstone of the European data strategy, reflects the EU's commitment to fostering a robust data economy while upholding its core values of trust, privacy, and fairness.

Entering into force on June 23, 2022, and applicable as of September 2023 after a 15-month transitional period, the DGA aims to enhance data sharing and reuse across sectors and borders. This legislation creates a structured framework to maximize the economic and societal potential of data while ensuring secure and transparent governance practices.

As it aims to establish mechanisms for trusted data sharing and enabling the creation of Common European Data Spaces, the DGA helps address critical barriers to data utilization and foster innovation in key strategic domains such as health, mobility, environment, agriculture, and public administration. This document provides an in-depth analysis of the DGA's objectives, mechanisms, and anticipated impacts on European citizens, businesses, and society at large.

Objectives of the Data Governance Act

The DGA addresses three primary objectives:

1. **Increasing Trust in Data Sharing:**

   The DGA emphasizes the importance of trust by implementing robust mechanisms to ensure data security, privacy, and neutrality in data transactions. By offering citizens and organizations greater control over their data, the Act builds confidence in sharing information for commercial and societal purposes.

2. **Enhancing Data Availability:**

   The Act seeks to unlock the vast reservoirs of data held by public and private entities. By creating a cohesive framework for data sharing across borders and sectors, it ensures that data is accessible for innovation while respecting intellectual property rights and data protection laws.

3. **Overcoming Technical Obstacles to Data Reuse:**

   The DGA introduces measures to tackle technical barriers to data reuse, including interoperability standards and secure infrastructures. This ensures that data can be effectively utilized across diverse sectors, facilitating the development of innovative products and services.

The Role of Common European Data Spaces

The DGA supports the establishment of Common European Data Spaces in strategic domains, enabling public and private stakeholders to share and pool data within secure and transparent ecosystems. These data spaces are designed to harness the transformative power of data in sectors critical to Europe's economic and societal growth.

Key domains include:

- **Health:** Enhancing personalized treatments and addressing chronic diseases.
- **Mobility:** Streamlining navigation and reducing labor costs through real-time data.
- **Environment:** Tackling climate change and responding to emergencies like floods and wildfires.

- **Agriculture:** Promoting precision farming and rural innovation.
- **Public Administration:** Improving statistical reliability and supporting evidence-based policymaking.

Key Mechanisms of the Data Governance Act

The DGA introduces four broad measures to achieve its objectives:

1. **Reuse of Public Sector Data:**

   The DGA facilitates the reuse of sensitive public sector data, such as health records, that cannot be made openly available. This allows researchers and innovators to leverage this data under secure conditions, advancing areas like rare disease treatments and pandemic responses.

2. **Data Intermediaries:**

   To enhance trust, the Act establishes a framework for data intermediaries—trusted entities that organize and facilitate data sharing. These intermediaries ensure data neutrality by operating independently and adhering to stringent transparency and security requirements.

3. **Data Altruism:**

   The DGA promotes data altruism, where individuals and organizations voluntarily share data for societal benefits. For example, mobility data can be shared to improve urban transport systems, or health data can be used to enhance medical research. A standardized European consent form ensures that data sharing is conducted uniformly across Member States.

4. **Cross-Sector and Cross-Border Data Sharing:**

   To enable seamless data sharing, the Act emphasizes interoperability and standardization. It supports the creation of infrastructures that allow data to flow securely across sectors and borders, ensuring that the right data can be found and used for the right purposes.

Anticipated Benefits of the Data Governance Act

The DGA is expected to drive significant benefits for various stakeholders:

1. **Citizens**

   Citizens gain greater control over their personal data through secure data-sharing mechanisms. This enhances transparency and empowers individuals to contribute their data for societal benefits, such as improving healthcare outcomes. For example, people with chronic diseases can securely share their data to advance research and treatments.

2. **Businesses**

   The Act lowers barriers to entry for businesses by reducing costs associated with acquiring, integrating, and processing data. SMEs, in particular, will benefit from shorter time-to-market for data-driven products and services. Additionally, the framework fosters innovation by providing businesses with access to high-quality data.

3. **Society**

   Society as a whole stands to benefit from evidence-based policymaking and solutions to societal challenges. Enhanced data sharing can support climate action, disaster response, and public health initiatives. For instance, mobility data can optimize public transport, reducing time and costs for commuters.

Practical Implementation of the DGA

1. **Public Sector Data Reuse:**

   Public sector entities are encouraged to make sensitive data available for reuse under secure and privacy-compliant conditions. This requires robust technical and legal frameworks to ensure that data confidentiality is preserved.

2. **Data Intermediaries' Role:**

   Trusted data intermediaries are pivotal to implementing the DGA. They act as neutral facilitators of data sharing, adhering to transparency standards and separating their data-sharing activities from other commercial interests.

3. **Standardized Consent and Documentation:**

   The DGA introduces a European consent form to simplify data altruism. This standardized approach facilitates cross-border data sharing, ensuring that individuals and organizations retain control over their contributions.

4. **Capacity Building:**

   The EU is investing in infrastructure, tools, and mechanisms to support the implementation of the DGA. This includes funding through the Digital Europe programme and the Connecting Europe Facility, with €2 billion allocated to developing advanced data processing capabilities.

Impact Across the EU

The DGA positions Europe as a leader in the global data economy, ensuring the EU remains at the forefront of the second wave of data-driven innovation. By fostering a culture of trusted data sharing, the regulation is expected to generate new jobs, enhance competitiveness, and strengthen Europe's digital sovereignty.

Additionally, the Act supports sustainable development goals by promoting data use in areas such as environmental protection, disaster management, and healthcare improvement. For businesses, the DGA reduces costs, encourages market entry, and accelerates product development cycles, benefiting firms of all sizes.

Table 1: Article 10 of EU AI Act versus Data Governance Act's Objectives

Specific Objectives	Operational Objectives	EU AI Act Application
Reinforcing trust in data sharing	Trust in data sharing increases as clear rules are available for data exchanged or pooled by data holders to be secure and processed in compliance with applicable legislation as well as with the conditions they set on use of such data.	Article 10 of the EU AI Act mandates high-quality data governance, bias detection, and transparency, ensuring data used in AI systems is reliable and secure. This builds stakeholder confidence in data sharing by promoting accountability and compliance with data protection regulations.
Making more data available for reuse within the common European data spaces	More data are made available for reuse on voluntary grounds based on the existing legislation and where data holders agree to this.	By enforcing stringent data quality and governance standards, Article 10 ensures data is relevant, representative, and error-free, facilitating its reuse across various applications and contexts, thus supporting the creation of a single market for data.
Ensuring interoperability across sectors and countries	Interoperability and generic standards contribute to reduction of transaction costs and allow data to be reused across sectors and Member States.	Article 10's emphasis on standardized data governance practices and quality criteria promotes consistency in data handling, enabling seamless data integration and interoperability across different sectors and EU member states, fostering a unified data ecosystem.

Conclusion

The European Data Governance Act is a transformative regulatory framework that seeks to unlock the full potential of data for the benefit of citizens, businesses, and society. By fostering trust, enhancing data availability, and addressing technical barriers, the DGA lays the foundation for a resilient and innovative data economy. Through the creation of Common European Data Spaces and the establishment of trusted intermediaries, the Act aligns with EU values of transparency, security, and fairness. It paves the way for data-driven advancements across sectors, enabling Europe to tackle societal challenges, support economic growth, and secure its place as a global leader in the digital age.

Implementing Article 10

This article outlines that high-risk AI systems must be developed using high-quality data sets for training, validation, and testing. These data sets should be managed properly, accounting for factors such as data collection processes, data preparation, potential biases, and data gaps. The data sets should be relevant, representative, error-free, and complete as much as possible. They should also consider the specific context in which the AI system will be used. For certain cases, providers may process special categories of personal data to detect and correct biases, but they adhere to strict conditions to protect individuals' rights and freedoms.

Paragraph 1.

Text

1. High-risk AI systems which make use of techniques involving the training of AI models with data shall be developed on the basis of training, validation and testing data sets that meet the quality criteria referred to in paragraphs 2 to 5 whenever such data sets are used.

Analysis

To comply with Article 10 of the EU AI Act, providers must establish rigorous data governance frameworks to manage training, validation, and testing datasets for high-risk AI systems. These datasets must meet stringent quality criteria, ensuring that data is relevant, representative, and free from significant errors. Providers must adopt robust data curation practices, including thorough data preparation steps such as annotation, cleaning, and bias mitigation.

Key implementation measures include systematic data assessments to evaluate availability, suitability, and quantity. Providers should use statistical techniques to ensure datasets reflect the diversity required for equitable AI outcomes, addressing biases that may compromise safety, health, or fundamental rights. Automated tools and manual reviews can help identify and rectify gaps or inconsistencies, fostering data quality and regulatory compliance.

Providers should document all data management activities, including data origin, collection methods, and processing decisions. Cross-referencing datasets with relevant legal and ethical standards enhances transparency and trust. Collaborative mechanisms, such as data-sharing agreements, aligned with the Data Governance Act, can overcome technical barriers to data reuse.

Paragraph 2.

Text

2. Training, validation and testing data sets shall be subject to data governance and management practices appropriate for the intended purpose of the high-risk AI system. Those practices shall concern in particular:

(a) the relevant design choices;

(b) data collection processes and the origin of data, and in the case of personal data, the original purpose Ox`f the data collection;

(c) relevant data-preparation processing operations, such as annotation, labelling, cleaning, updating, enrichment and aggregation;

(d) the formulation of assumptions, in particular with respect to the information that the data are supposed to measure and represent;

(e) an assessment of the availability, quantity and suitability of the data sets that are needed;

(f) examination in view of possible biases that are likely to affect the health and safety of persons, have a negative impact on fundamental rights or lead to discrimination prohibited under Union law, especially where data outputs influence inputs for future operations;

(g) appropriate measures to detect, prevent and mitigate possible biases identified according to point (f);

(h) the identification of relevant data gaps or shortcomings that prevent compliance with this Regulation, and how those gaps and shortcomings can be addressed.

Analysis

High-risk AI systems, as regulated under the EU AI Act, rely on robust data governance practices to ensure compliance and maintain public trust. Article 10 emphasizes data quality and governance throughout the lifecycle of training, validation, and testing datasets. This section outlines actionable steps for implementing the provisions of Article 10, fostering alignment with the Data Governance Act to enhance data sharing, availability, and reuse.

'Significance lies in fostering trust in data sharing', Lisa Ventura MBE

Article 10 of the EU AI Act establishes comprehensive data governance requirements for high-risk AI systems, mandating that training datasets be relevant, representative, and error-free. These provisions align with the Data Governance Act's objectives by fostering trust in data sharing, enhancing availability, and addressing technical barriers to reuse.

'Enabling trust in data sharing through transparency'

"Trust is the cornerstone of data governance and is essential for enabling individuals and organizations to share their data confidently through transparency, accountability, and security."

Lisa Ventura MBE, *Chief Executive & Founder*, Cyber Security Unity

Key Components of Data Governance Practices

Effective implementation of Article 10 requires a structured approach to data governance, addressing the following areas:

Design Choices and Data Collection Processes

AI system providers must document and justify design decisions, focusing on how these decisions shape data collection and use. This includes specifying the origin of data, ensuring relevance to the intended purpose, and clarifying, in the case of personal data, its original collection purpose. Establishing ethical data collection frameworks aligned with EU regulations is critical.

Data Preparation and Processing Operations

High-quality datasets require thorough preparation. Article 10 mandates operations such as annotation, labelling, cleaning, updating, and aggregation. Automating these processes with AI-enabled tools ensures consistency and minimizes human error. Moreover, detailed documentation of data processing steps increases transparency and facilitates audits.

Addressing Assumptions and Data Evaluation

Formulating and Documenting Assumptions

AI datasets are built upon assumptions about the data's representativeness and what it measures. Providers must systematically record these assumptions, aligning them with the system's intended purpose. For example, assumptions about demographic representativeness should reflect the user base of the AI system.

Assessing Data Availability, Quantity, and Suitability

Providers must evaluate datasets to ensure sufficient volume and suitability for training. This involves statistical analyses to verify data adequacy and address gaps. For instance, if a dataset lacks sufficient coverage of underrepresented groups, supplementary data collection efforts may be required.

'Heavy focus on input space', Dr. Don Liyanage

The EU AI Act's Article 10 mandates robust data governance for high-risk AI systems, focusing on the input space. It requires procedures to ensure training, validation, and testing datasets are high-quality, representative, and bias-free, enhancing transparency and accountability as a foundation for AI explainability.

> 'Championing a future where innovation thrives on trust'
>
> *"By aligning the AI Act with the Data Governance Act, the EU champions a future where innovation thrives on trust, transparency, and high-quality data, ensuring AI serves humanity responsibly."*
>
> **Dr. Don Liyanage**, Co-*Founder*, Tikos

Mitigating Bias and Ensuring Compliance

Bias Detection and Prevention

Bias in datasets can negatively impact individuals' health, safety, and fundamental rights. Providers must examine potential biases—such as gender or ethnic disparities—and implement proactive measures to mitigate them. Techniques like differential privacy, stratified sampling, and fairness-aware algorithms are effective tools.

Detecting and Addressing Gaps

Systematic reviews should identify gaps or shortcomings that hinder compliance with the EU AI Act. Providers can address these gaps by integrating diverse datasets, employing synthetic data to fill voids, or refining data collection methodologies.

Implementing Continuous Data Governance

Ongoing Monitoring and Updates

Data governance is not a one-time effort. Providers should establish mechanisms for ongoing monitoring and updating datasets. This includes routine evaluations to ensure data quality and relevance as societal and technological contexts evolve.

Collaboration and Data Sharing

To overcome technical barriers to data reuse, providers can engage in collaborative agreements supported by the Data Governance Act. Shared data pools, standardization, and interoperable formats enhance data availability and accessibility across sectors.

'Integration of dataset checks key', Dave Bohnert

Through the **Fairify app**, I've operationalized Article 10 by integrating dataset checks and bias diagnostics using Giskard and AIF360. My focus is on making AI Act compliance feasible for small, high-risk models with limited compute and documentation capacity. We need tooling that matches real-world constraints without compromising regulatory integrity.

'Implementation journey starts at the dataset level'

"Practical compliance starts at the dataset level. Article 10 should empower developers of small models with concrete, testable standards for data quality and fairness — not just policy principles."

Dave Bohnert, *Founder & Lead Architect*, DataDave LegalBot

Paragraph 3.

3. Training, validation and testing data sets shall be relevant, sufficiently representative, and to the best extent possible, free of errors and complete in view of the intended purpose. They shall have the appropriate statistical properties, including, where applicable, as regards the persons or groups of persons in relation to whom the high-risk AI system is intended to be used. Those characteristics of the data sets may be met at the level of individual data sets or at the level of a combination thereof.

Analysis

To align with Article 10 of the EU AI Act, organizations must ensure that training, validation, and testing datasets meet stringent quality requirements to support high-risk AI systems. These datasets must be relevant, sufficiently representative, and, to the greatest extent possible, free of errors and complete, reflecting the intended purpose of the AI system.

Key implementation measures include conducting comprehensive assessments to confirm datasets' statistical properties. This is particularly important when AI systems impact specific groups of people. For instance, datasets must account for demographic diversity to prevent biases that may compromise fairness or safety. Combining datasets with complementary attributes can address gaps in individual datasets, enhancing overall quality and representativeness.

Providers should employ advanced data management practices, such as automated error detection and correction, to minimize inconsistencies. Documentation of data preparation, including cleaning and annotation, enhances transparency and compliance with regulatory standards.

Collaboration with stakeholders, including policymakers and data contributors, can help ensure datasets reflect real-world complexities and meet ethical considerations. Adhering to these principles permits organizations strengthen trust in AI systems and align with the broader objectives of the Data Governance Act, fostering secure, interoperable data-sharing practices that drive innovation and public confidence.

Paragraph 4.

4. Data sets shall take into account, to the extent required by the intended purpose, the characteristics or elements that are particular to the specific geographical, contextual, behavioural or functional setting within which the high-risk AI system is intended to be used.

Analysis

To comply with Article 10 of the EU AI Act, providers must ensure that datasets used in high-risk AI systems reflect the unique geographical, contextual, behavioural, and functional settings in which the systems operate. Tailoring datasets to these characteristics enhances the AI system's relevance and performance, while reducing risks of unintended bias or errors.

Effective implementation begins with identifying the specific use cases and environments for the AI system. For instance, an AI system designed for urban traffic management requires datasets that account for traffic patterns, infrastructure, and demographics specific to the targeted city. Similarly, behavioural datasets for healthcare applications must reflect variations in patient behaviour across regions and cultures.

Providers should conduct gap analyses to determine whether existing datasets sufficiently represent the intended contexts. When deficiencies are identified, they can supplement data through additional collection or use synthetic data generation. Collaborative efforts with local stakeholders or domain experts can help capture nuanced contextual information.

Documentation of these efforts ensures transparency and facilitates audits. Embedding contextual considerations into data governance practices enables providers to align with the broader objectives of the Data Governance Act, building trust, enhancing data availability, and promoting interoperable and equitable data reuse across sectors.

Paragraph 5.

5. To the extent that it is strictly necessary for the purpose of ensuring bias detection and correction in relation to the high-risk AI systems in accordance with paragraph (2), points (f) and (g) of this Article, the providers of such systems may exceptionally process special categories of personal data, subject to appropriate safeguards for the fundamental rights and freedoms of natural persons. In addition to the provisions set out in Regulations (EU) 2016/679 and (EU) 2018/1725 and Directive (EU) 2016/680, all the following conditions must be met in order for such processing to occur:

(a) the bias detection and correction cannot be effectively fulfilled by processing other data, including synthetic or anonymised data;

(b) the special categories of personal data are subject to technical limitations on the re-use of the personal data, and state-of-the-art security and privacy-preserving measures, including pseudonymisation;

(c) the special categories of personal data are subject to measures to ensure that the personal data processed are secured, protected, subject to suitable safeguards, including strict controls and documentation of the access, to avoid misuse and ensure that only authorised persons have access to those personal data with appropriate confidentiality obligations;

(d) the special categories of personal data are not to be transmitted, transferred or otherwise accessed by other parties;

(e) the special categories of personal data are deleted once the bias has been corrected or the personal data has reached the end of its retention period, whichever comes first;

(f) the records of processing activities pursuant to Regulations (EU) 2016/679 and (EU) 2018/1725 and Directive (EU) 2016/680 include the reasons why the processing of special categories of personal data was strictly necessary to detect and correct biases, and why that objective could not be achieved by processing other data.

Analysis

High-risk AI systems, as governed by Article 10 of the EU AI Act, may necessitate processing special categories of personal data to effectively detect and correct biases. Such processing is permissible only under strict conditions, ensuring fundamental rights and freedoms are safeguarded. Providers must establish robust governance frameworks to manage these sensitive datasets while maintaining compliance with the EU AI Act, GDPR (Regulation (EU) 2016/679), and other relevant legislation.

‘Critics’ view Article 10 as vague and burdensome’

"Critics argue that Article 10 of the EU AI Act is vague and overly burdensome, requiring unrealistically onerous standards for data quality and documentation. They also argue that Article 10 imposes sometimes overlapping or contradictory obligations to existing laws (e.g., GDPR), while potentially exposing proprietary information during compliance efforts."

Jerry Silber. AI *2030 Evangelist*. AI 2030

Conditions for Processing Special Categories of Personal Data

Providers must ensure that processing special categories of personal data is strictly necessary and cannot be achieved using alternative methods, such as anonymized or synthetic data. For instance, detecting biases in a healthcare AI system might require using specific medical data to identify disparities in patient outcomes. Comprehensive documentation must justify why other data types are insufficient.

To mitigate risks, state-of-the-art technical safeguards such as pseudonymization must be applied. Pseudonymized data helps protect identities while retaining analytical value. Providers should also limit data reuse through strict access controls, ensuring sensitive data is processed only for the intended purpose.

Security and Privacy Safeguards

To comply with Article 10, providers must implement robust security measures, including encryption and access controls, to prevent unauthorized access. For example, healthcare AI systems should ensure that only authorized medical researchers can access sensitive patient data. Detailed documentation of access logs enhances transparency and accountability, preventing misuse.

Additionally, stringent retention policies are required. Special categories of personal data must be deleted once the bias is corrected or the retention period expires. Automated deletion tools can enforce this policy, ensuring compliance without manual intervention.

Ensuring Limited Transmission and Controlled Access

Under Article 10, special categories of personal data must not be transmitted or shared with third parties. This provision reduces the risk of data breaches or unauthorized reuse. Providers can employ secure environments, such as on-premise or private cloud solutions, for processing sensitive data.

Controlled access protocols, including multifactor authentication and role-based access, should restrict data handling to authorized personnel. For example, a financial AI system analyzing credit risks might limit access to anonymized consumer profiles, with sensitive attributes shielded from unnecessary personnel.

Transparency and Documentation

Providers must maintain comprehensive records of processing activities, as required by the GDPR and Directive (EU) 2016/680. These records should detail why processing sensitive data was necessary for bias detection and correction. Audit trails must include justifications for not using synthetic or anonymized data, ensuring accountability.

Moreover, clear communication with stakeholders, including regulators and affected individuals, enhances trust. Data protection impact assessments (DPIAs) provide an opportunity to proactively address potential risks, aligning with broader objectives under the Data Governance Act.

Alignment with Broader Governance Objectives

Adhering to these strict protocols permits providers to contribute to the Data Governance Act's goals of increasing trust in data sharing, enhancing data availability, and mitigating technical barriers to data reuse. Processing special categories of personal data responsibly ensures that AI systems are fair, transparent, and accountable.

Paragraph 6.

6. For the development of high-risk AI systems not using techniques involving the training of AI models, paragraphs 2 to 5 apply only to the testing data sets.

Analysis

For high-risk AI systems that do not rely on training models, Article 10 specifies that data governance requirements apply solely to testing datasets. While these systems may bypass traditional model training, the robustness, accuracy, and fairness of their outputs heavily depend on the integrity of the testing datasets. Implementation begins with ensuring that testing datasets adhere to the same high standards as outlined for training datasets in Article 10. These datasets must be relevant, representative, and error-free to the extent possible. Providers should focus on capturing the specific characteristics of the intended operational environment, including geographical, contextual, and functional settings. For example, testing data for a rule-based fraud detection system should reflect realistic transaction patterns from its intended application region.

Providers must adopt rigorous data validation techniques to identify gaps, biases, or inconsistencies that could undermine the system's performance or fairness. Documentation of testing procedures, data sources, and validation results is crucial for demonstrating compliance and fostering transparency. **'Leverage DeepTech to optimise data governance capabilities', Prof. Dr. Ingrid Vasiliu-Feltes**

Robust data governance for high-risk AI systems under the EU AI Act can be facilitated by leveraging deep tech—data mesh, data fabric, DLTs like blockchain, and quantum-proof encryption—to ensure accountability, transparency, and digital trust. These technologies can enable secure, compliant AI deployments, fostering scalable innovation and transformation while meeting stringent regulatory standards.

‘Data provenance forms bedrock of data governance’

“Data provenance, validity, integrity, and dynamic informed consent form the bedrock of data governance, ensuring accountability, transparency, and digital trust for transformative AI-portfolio innovation across industries.”

Prof. Dr. Ingrid Vasiliu-Feltes, *Founder & CEO*, Institute for Science, Entrepreneurship and

‘Moving beyond procedural accountability towards culturally aware data governance frameworks’, Dr. Amritha Subhayan Krishnan

As AI systems increasingly influence creative, civic, and public-facing domains, Article 10 of the EU AI Act must move beyond procedural accountability to embed context-sensitive, culturally aware data governance. Provenance, consent ethics, and community trust must guide reuse and interoperability, ensuring human-centred, resilient frameworks for next-generation digital infrastructures.

‘Data governance akin to a cultural contract’

"Data governance is not just a technical protocol but a cultural contract. Article 10 offers a generational opportunity to rebuild trust through provenance, contextual intelligence, participatory design, and decentralized, future-facing inclusion."

Dr. Amritha Subhayan Krishnan, *Founder and CEO*, Smart Story Labs

Addressing Data Life Cycle

The data life cycle encompasses the stages through which data is generated, processed, and utilized, ensuring its value is maximized while maintaining compliance and security. From collection and curation to analysis, sharing, and eventual disposal, effective governance at each stage is essential for fostering trust, accessibility, and innovation in data-driven ecosystems.

Table 1: EU AI Act and NGI Support for Five Key Pillars

Stage	Sub-Stage	EU AI Act	Data Governance Act
Input	Collection	**Design Choices and Data Origin**: The Act requires that data collection processes consider relevant design choices and the origin of data, especially when personal data is involved. This ensures that the data is collected with a clear understanding of its original purpose. **Data Suitability and Availability**: It mandates an assessment of the availability, quantity, and suitability of data sets necessary for the AI system's intended purpose, ensuring appropriateness and sufficiency.	**Public Sector Data**: The regulation emphasizes making public sector data available under FAIR principles (Findable, Accessible, Interoperable, and Reusable). See Recital (2) and Articles 5 and 8, which discuss enabling data collection and pooling across sectors to foster data-driven innovation.
	Curation	**Data Preparation Processes**: The Act specifies that data must undergo preparation processes such as annotation, labelling, cleaning, updating, enrichment, and aggregation to ensure quality and relevance. **Bias Detection and Mitigation**: It emphasizes examining data for biases that could affect health, safety, or fundamental rights, requiring measures to detect, prevent, and mitigate these biases.	**Techniques for Curation**: Provisions for secure processing environments, anonymization, and other techniques to curate sensitive data are outlined in Recitals (7) and (15). **Harmonization and Metadata Standards**: See Recital (16), which discusses creating streamlined administrative procedures, standardizing metadata, and facilitating data usability.
Process	Processing	**Data Governance and Management**: Training, validation, and testing data sets must adhere to data governance and management practices suitable for the AI system's purpose, including data collection, annotation, and cleaning. **Bias Detection and Mitigation**: The regulation requires examination for potential biases and mandates measures to detect, prevent, and mitigate them.	**Secure Environments**: Articles 5(4) and 9 establish secure processing environments for data processing and reuse while ensuring privacy. **Automated Means**: Recital (26) mentions the use of automated systems for transmitting and processing data queries and requests.
	Analysis	**Quality and Representativeness**: Data sets must be relevant, sufficiently representative, and as error-free as possible, with appropriate statistical properties to ensure high-quality analysis. **Assumptions and Data Suitability**: The regulation emphasizes formulating assumptions about what the data measures and represents, and assessing the data's availability, quantity, and suitability.	**Data Reuse for Research**: Recital (16) supports data analysis for public interest and scientific research, encouraging reuse through secure processing environments. **Ethical Oversight**: Recognized data altruism organizations, as detailed in Articles 18 and 20, must ensure ethical use of data for analysis.
Output	Visualisation	The EU AI Act does not explicitly detail the output stage, including visualization, sharing, application of insights, benefit sharing, reuse, retention, and disposal, within Article 10. However, the Act's emphasis on transparency and documentation, as highlighted in Recital 101, suggests a framework for ensuring that outputs are managed responsibly. This includes maintaining documentation and providing information on AI models to facilitate their integration and use by downstream providers.	**Transparency**: Recital (47) highlights the use of transparency mechanisms, such as QR codes and public registries, to ensure visibility of data sharing and reuse processes.
	Sharing		**Data Sharing Mechanisms**: The establishment of data intermediation services and single information points to facilitate data sharing is detailed in Recitals (27) and (26).
	Application of resulting insights		**Reuse Conditions**: Article 5(1) outlines non-discriminatory conditions for sharing and reusing data. **Public Benefit Applications**: Recital (45) promotes applying data-driven insights to public policies, including health, climate, and mobility.
	Benefit sharing		**Support for SMEs**: Recital (25) emphasizes incentivizing data use by SMEs and start-ups. **Data Altruism**: Recital (45) and Articles 18–22 focus on voluntary data sharing to advance public interests and include provisions for compensating contributors.
	Reuse Retention and afterlife Disposal		**Retention Standards**: Recital (15) specifies safeguards for retaining data only as long as necessary and under defined conditions. **Disposal**: Secure disposal mechanisms and prohibitions on reusing sensitive data improperly are described in Recital (15) and Article 5(6).

Upholding Data Governance requirements – Questions and Answers

Upholding data governance requirements is essential for ensuring trust, compliance, and effective data management. This section answers key questions about how to meet regulatory standards, addressing challenges related to data collection, processing, and sharing. It provides insights on maintaining transparency, safeguarding privacy, and fostering secure, responsible data practices in various settings.

What is data governance?

Data governance is the structured management of data's availability, usability, integrity, and security within an organization. It involves establishing policies, procedures, and standards to ensure data is handled consistently and responsibly. In the context of the EU AI Act, particularly for high-risk AI systems, data governance is crucial for ensuring that data sets used in AI systems are managed appropriately to meet regulatory requirements. This includes making informed design choices, understanding data origins, and implementing processes like data annotation, cleaning, and aggregation to maintain data quality and relevance.

'Impactful AI deployment relies on integrity of datasets', Anandady Misshra

As AI systems increasingly shape decision-making, Article 10 of the EU AI Act plays a pivotal role in setting rigorous data governance standards. By aligning with the Data Governance Act's objectives, it promotes trustworthy, high-quality datasets, transparency in data processing, and accountability mechanisms critical for lawful, ethical, and impactful AI deployment.

'Ethical data use bridges innovation'

"Robust data governance under the EU AI Act bridges innovation and compliance, fostering trust, ensuring transparency, and enabling responsible AI development aligned with the Data Governance Act's vision for ethical data use."

Anandaday Misshra, *Founder & Managing Partner*, AMLEGALS

Why do we need regulatory requirements for data governance?

Regulatory requirements for data governance are essential for several reasons. They ensure data quality and integrity by mandating that data used in AI systems is relevant, accurate, and representative of the intended application. This is crucial for the reliability and effectiveness of AI systems, as poor data quality can lead to incorrect or biased outcomes. Regulations also help mitigate bias and discrimination by requiring the examination of data for biases that could negatively impact health, safety, or fundamental rights. This is particularly important for high-risk AI systems, where biased data can lead to discriminatory outcomes. Additionally, regulatory requirements ensure compliance with existing data protection laws, such as the GDPR, thereby safeguarding personal data and maintaining public trust.

'Data links compliance with strategic resilience', Steven Paul

Article 10 ensures board attention because it links compliance with strategic resilience. Mandating documented data lineage, bias checks, and interoperability, it operationalises the Data Governance Act's aims ie., trust, availability, and reuse. For high-risk AI systems, this transforms data governance from an IT issue into a core board responsibility for risk, ethics, and innovation.

'Data has become a governance imperative'

"Boards must treat Article 10 as a governance imperative, not a technical detail. For e.g. its mandates on data quality, traceability, and interoperability are critical to safeguarding trust and enabling responsible AI at scale."

Steven PAUL, CDir, Fellow IoD, Freshriver AI

How will regulatory requirements on data governance benefit citizens and businesses?

Regulatory requirements on data governance benefit both citizens and businesses. For citizens, these regulations enhance the safety and fairness of AI systems by ensuring they are developed and operated transparently and ethically. This helps build public trust in AI technologies, which is essential for their widespread adoption and acceptance. For businesses, regulatory requirements provide a framework for ensuring compliance with legal standards, thereby reducing the risk of legal liabilities and enhancing the reliability and safety of their AI systems. This can lead to increased consumer confidence and market competitiveness. Furthermore, by fostering innovation and trust, regulatory frameworks support the development of an AI ecosystem that benefits both citizens and businesses.

'Data becomes an important adjustment screw', Ina Schöne

When we will live with AI in responsible way with excellence results by generating new informations based on training data sets, the data input is an important adjustment screw. ISO 8000 series is the guideline to handle the data management in combination with ISO/IEC42001:2023 Artificial Intelligence Management Systems and an essential to have quailty in all data sets.

'Responsible AI relies on good data quality '

"*Data is the 'food' for every AI-System - Data Quality is essential to provide responsible AI*."

Ina Schöne, *Lead Auditor IEC/ISO42001 and Founder*, Data Privacy and AI

Supporting European strategy for data

The EU AI Act is a cornerstone in the broader European strategy for data, which aims to harness the power of data to drive economic growth, innovation, and societal progress while upholding European values and rights. This strategy is pivotal in creating a single market for data, ensuring Europe's global competitiveness and data sovereignty. The EU AI Act supports this strategy through legislative measures, enhancing data availability, and fostering investment in data infrastructure.

Legislative Measures

The EU AI Act introduces harmonized rules for AI systems, particularly high-risk ones, to ensure they are developed and used safely and ethically. By setting stringent requirements for data governance, the Act mandates that data used in AI systems is managed with transparency and accountability. This includes ensuring data quality, relevance, and representativeness, which are essential for the reliability and fairness of AI systems. The Act also emphasizes the need for bias detection and mitigation, ensuring that AI systems do not perpetuate discrimination or harm fundamental rights. These measures align with the European strategy for data by promoting trust and security in data-driven technologies, which are crucial for their acceptance and integration into society.

Data Availability

The EU AI Act supports data availability by requiring that data sets used in AI systems are comprehensive and suitable for their intended purposes. This involves assessing the availability, quantity, and suitability of data sets, ensuring they are sufficient to support the AI system's functions. By mandating that data sets are relevant and representative, the Act ensures that AI systems can operate effectively across different contexts and applications, thereby enhancing data availability for AI development. This is crucial for creating a single market for data, as it ensures that more data becomes available for use in the economy and society, while keeping the companies and individuals who generate the data in control.

Investment in Data Infrastructure

The EU AI Act encourages investment in data infrastructure through measures that support innovation and the development of AI technologies. The establishment of AI regulatory sandboxes, as outlined in the Act, provides a controlled environment for testing and validating AI systems, facilitating innovation and the development of new data-driven technologies. These sandboxes also promote collaboration between public and private sectors, fostering an ecosystem that supports data infrastructure development and investment. This aligns with the European strategy for data, which includes investing €2 billion in a European High Impact Project to develop data processing infrastructures, data sharing tools, architectures, and governance mechanisms for thriving data sharing and to federate energy-efficient and trustworthy cloud infrastructures and related services.

Benefits to Citizens and Businesses

The EU AI Act, in conjunction with the European strategy for data, offers numerous benefits to both citizens and businesses. For citizens, the strategy aims to improve healthcare, create safer and cleaner transport systems, generate new products and services, reduce the costs of public services, and improve sustainability and energy efficiency. By ensuring that AI systems are developed and used responsibly, the EU AI Act helps to realize these benefits while protecting citizens' rights and promoting trust in digital technologies.

For businesses, the EU AI Act provides a clear regulatory framework that facilitates compliance and reduces the risk of legal liabilities. This is particularly important for small and medium-sized enterprises (SMEs), which can leverage the Act's provisions to compete with larger companies in the data economy. By ensuring fair access to data and preventing monopolistic practices, the Act promotes competition and innovation, driving economic growth and enhancing the EU's competitiveness in the global data market.

Role of the Data Governance Act and the Data Act

The DGA and the Data Act are pivotal components of the European strategy for data, designed to enhance data sharing, build trust, and stimulate the data economy across the EU. The DGA aims to create a robust framework for data sharing by establishing mechanisms that facilitate the reuse of public sector data, particularly data that is sensitive or subject to third-party rights. It introduces the concept of data intermediaries, which are neutral entities that help manage data sharing between parties, ensuring that data is exchanged in a secure and trustworthy manner. This act is crucial for building trust among data holders and users, as it provides clear guidelines and safeguards for data sharing, thereby encouraging more entities to participate in the data economy.

The Data Act complements the DGA by focusing on the rights and obligations related to data access and use. It seeks to ensure fair access to data for businesses and consumers, particularly in the context of the Internet of Things (IoT) and connected devices. The act aims to prevent data monopolies by ensuring that data generated by devices can be accessed and used by multiple parties, thus promoting competition and innovation. By establishing clear rules on data access and sharing, the Data Act aims to create a level playing field for businesses, enabling SMEs to compete with larger companies. This is expected to drive innovation and growth in the data economy, as more businesses can leverage data to develop new products and services.

Conclusion

In conclusion, the EU AI Act, along with the Data Governance Act and the Data Act, plays a crucial role in supporting the European strategy for data. By establishing a comprehensive framework for data governance, enhancing data availability, and fostering investment in data infrastructure, these legislative measures ensure that data is used responsibly and effectively in AI systems. This promotes a digital economy that is innovative, competitive, and aligned with EU values, ultimately benefiting both citizens and businesses. Through these efforts, the EU aims to maintain its leadership in the global data economy, ensuring that data-driven technologies contribute positively to society and the economy.

‘Opt-in necessary for sensitive use cases, such as healthcare ’

"The DGA allows for the use of personal healthcare data with an opt-out regime, which fails to protect individuals' sufficiently and risks eroding public trust in EU data governance, and the EU should mandate explicit opt-in consent for each use case of healthcare data."

Neil Oschlag-Michael, *Head of AI Risk and Security*, boost.ai

Conclusion

The interplay between the Data Governance Act (DGA) and Article 10 of the EU AI Act establishes a transformative framework for leveraging data across Europe. By fostering trust, enhancing data availability, and addressing technical barriers to reuse, these regulations set the stage for a resilient and ethical data ecosystem.

Building Trust in Data Sharing

Trust is the cornerstone of data governance and is essential for enabling individuals and organizations to share their data confidently. Article 10 of the EU AI Act contributes significantly to this objective by embedding transparency, accountability, and security into the development of high-risk AI systems. Specifically, the article's requirements for documenting data origins, ensuring representativeness, and mitigating biases directly align with the DGA's focus on creating a trusted environment for data sharing.

For citizens, these measures provide reassurance that their data will be handled ethically, securely, and in line with EU values. For businesses, the robust governance structures eliminate uncertainties about compliance, encouraging more active participation in data-sharing ecosystems. As trust deepens, data altruism—a central tenet of the DGA—can flourish, enabling individuals and organizations to contribute data for societal benefits, such as healthcare advancements or climate resilience.

Enhancing Data Availability

Data is a critical enabler of innovation, and its availability underpins the success of both the DGA and the AI Act. Article 10 ensures that data used in high-risk AI systems is relevant, representative, and free from significant errors. This commitment to quality amplifies the potential of available datasets, enabling better training, validation, and testing of AI models.

Moreover, the DGA's mechanisms for unlocking public sector data complement these efforts by expanding access to previously underutilized datasets. By aligning public and private data-sharing initiatives, the DGA supports the creation of Common European Data Spaces, which foster collaboration and innovation across strategic sectors such as health, mobility, and energy. This alignment ensures that AI systems developed in Europe are not only compliant but also highly effective and inclusive.

For businesses, especially SMEs, the enhanced availability of high-quality data reduces operational costs and accelerates product development cycles. This democratization of data access levels the playing field, allowing smaller players to compete in data-driven markets and contribute to Europe's broader innovation agenda.

Addressing Technical Barriers to Reuse

The reuse of data across sectors and borders presents technical challenges, such as interoperability, standardization, and privacy compliance. Both the DGA and Article 10 tackle these issues head-on by emphasizing harmonized frameworks and secure infrastructures.

Article 10 mandates the use of statistical and technical standards to ensure that datasets are interoperable and suitable for their intended purposes. This creates consistency in how data is processed and shared, reducing fragmentation in the data ecosystem. The DGA complements this by establishing trusted data intermediaries and shared infrastructures that facilitate seamless cross-sector and cross-border data exchanges. These efforts not only address immediate technical obstacles but also lay the foundation for long-term innovation. For example, the combination of standardized datasets and secure sharing mechanisms accelerates the deployment of AI systems in complex domains like precision agriculture or personalized medicine. By reducing redundancy and increasing efficiency, the DGA and AI Act together unlock new possibilities for data reuse and collaboration.

Empowering Stakeholders

Citizens

Citizens are at the heart of Europe's data governance strategy. By granting individuals greater control over their data and ensuring transparency in its use, the DGA and AI Act empower people to make informed decisions about sharing their information. Mechanisms like the European consent form for data altruism simplify this process, enabling citizens to contribute data for societal benefits without compromising their privacy. These frameworks also protect citizens from potential risks associated with high-risk AI systems. Article 10's provisions for bias detection, error mitigation, and secure data handling ensure that AI applications operate fairly and ethically, preserving fundamental rights and freedoms.

Businesses

For businesses, the combined impact of the DGA and AI Act is transformative. Enhanced access to high-quality data reduces costs, fosters innovation, and accelerates market entry. The regulations also create a level playing field by ensuring that all participants adhere to the same standards, reducing competitive imbalances caused by disparate data practices. SMEs, in particular, stand to benefit from these changes. With lower barriers to entry and reduced costs for data integration, smaller firms can leverage the same high-quality datasets as larger corporations. This democratization of data access fuels entrepreneurial innovation and contributes to Europe's economic growth.

Society

At a societal level, the integration of the DGA and AI Act drives evidence-based policymaking, improves public services, and addresses global challenges such as climate change and public health crises. For instance, access to mobility data can optimize urban transportation systems, reducing emissions and saving time for commuters. Similarly, the reuse of health data can expedite medical research and enhance healthcare delivery, benefiting communities across the EU.

Strengthening Europe's Digital Sovereignty

A central goal of the DGA and AI Act is to position Europe as a global leader in the data economy. By fostering a secure, interoperable, and inclusive data-sharing framework, these regulations strengthen Europe's digital sovereignty and competitiveness. The emphasis on EU values—such as privacy, transparency, and fairness—sets a global benchmark for responsible data governance.

Digital sovereignty is Europe's pathway toward a more open, participatory, and multi-stakeholder model of internet governance. This vision supports a digitally connected Europe that remains open for business while mitigating emerging risks such as internet fragmentation, censorship through digital tools, and deepening digital divides. As other regions look to Europe's example, the DGA and AI Act could inspire similar initiatives worldwide, further solidifying Europe's leadership in shaping a global digital order grounded in democratic values like openness, inclusivity, and security.

Challenges and Recommendations

While the DGA and AI Act provide a robust framework, their successful implementation requires addressing several challenges:

1. **Interoperability Across Sectors:** Harmonizing data-sharing practices across diverse domains is complex. Continued investment in standardization and cross-sector collaboration is essential.
2. **Public Awareness:** Educating citizens about their rights and the benefits of data altruism can enhance participation and trust in data-sharing ecosystems.

3. **Global Coordination:** Aligning EU data governance practices with international frameworks can foster a cohesive global data economy while safeguarding EU principles.

4. **Advancing AI Auditability**: Developing interpretability tools and audit standards to address the opacity of complex models such as large language models (LLMs), ensuring that transparency requirements under the AI Act are both meaningful and enforceable.

To overcome these challenges, policymakers should prioritize stakeholder engagement, capacity-building initiatives, and adaptive regulatory approaches that accommodate emerging technologies and use cases.

Future Outlook

The DGA and AI Act mark the beginning of a new era in data governance and AI regulation. As implementation progresses, these frameworks will evolve to address emerging challenges, such as the rise of generative AI or the increasing importance of real-time data analytics. Looking ahead, the EU's focus on Common European Data Spaces will likely expand to include new domains, reflecting the dynamic nature of the data economy. Initiatives like the European Health Data Space and Green Deal Data Space exemplify the potential for sector-specific frameworks to drive targeted innovation and societal benefits. Additionally, advancements in technologies like blockchain and federated learning may offer new opportunities for secure and decentralized data sharing, further enhancing the effectiveness of the DGA and AI Act.

'A value-added contribution to AI governance'

"A timely white paper summarising the key elements of the EU AI Act, the attendant corporate governance responsibilities, and how the EU AI Act works alongside EU Data Governance Act."

Thomas Naylor, *Founder & Editor*, hibo

Concluding Remarks

The synergy between the Data Governance Act and Article 10 of the EU AI Act establishes a comprehensive framework for building a trusted, interoperable, and innovative data ecosystem in Europe. By aligning data governance with AI regulation, these legislative efforts address the challenges of the digital age while unlocking the transformative potential of data for citizens, businesses, and society. Through enhanced trust, expanded data availability, and the removal of technical barriers, the DGA and AI Act lay the foundation for a resilient and inclusive data economy. As these frameworks continue to evolve, they will not only bolster Europe's digital sovereignty but also serve as a global model for ethical and sustainable data governance.

Annex I – Third-Party Opinions (Karushkov)

‘Regulators’ focus on data set integrity’

The relevant statutory provisions regarding data governance of high-risk AI systems aim at regulatory modelling the design, maintenance, release and operation of the high-risk AI systems. This regulatory goal will, probably, be reached. However, using many adjectives in the provisions of the AI Act seems to also produce a confusing effect in the real life and market environment. Here’s a sample of some of the said adjectives: … the relevant data sets utilised shall be: “ … relevant, sufficiently representative, and to the best extent possible, free of errors …” . Sounds more like a good wish rather than a regulatory requirement, though. It could become factual that the subjective factor (and not only the factual circumstances) will estimate, for example, what it means “to the best extent possible” about a dataset containing sensitive data. The public authorities, as well as relevant governmental experts, shall have the power to qualify the efforts of the AI proprietors as good, better, best.

Karushkov Legal Solutions URL: www.karushkov.com

‘Real-world scenarios determine effectiveness’

Regulating data sets may increase the trust in data utilization within high-risk AI systems at legislative level. However, the stakeholders, the regulators, as well as the real life situations shall prove this trust working or not.

Karushkov Legal Solutions LinkedIn: http://linkedin.com/in/mitko-karushkov-3533882

References

European Commission, (2020), 'Data Governance Act', accessible at: https://digital-strategy.ec.europa.eu/en/library/data-governance-act (last accessed 9th December 2024)

European Commission, (2020), 'Data Governance Act explained', accessible at: https://digital-strategy.ec.europa.eu/en/policies/data-governance-act-explained (last accessed 9th December 2024)

European Commission, (2020), 'Impact Assessment report and support study accompanying the Proposal for a Regulation on Data Governance', accessible at: https://digital-strategy.ec.europa.eu/en/library/impact-assessment-report-and-support-study-accompanying-proposal-regulation-data-governance (last accessed 9th December 2024)

European Commission, (2020), 'Regulation on data governance – Questions and Answers', accessible at: https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_2103 (last accessed 9th December 2024)

European Commission, (2024), 'A European strategy for data', accessible at: https://digital-strategy.ec.europa.eu/en/policies/strategy-data (last accessed 9th December 2024)

European Commission, (2024), 'European Data Governance Act', accessible at: https://digital-strategy.ec.europa.eu/en/policies/data-governance-act (last accessed 9th December 2024)

European Commission, (2024), 'New practical guidance to the Data Governance Act', accessible at: https://digital-strategy.ec.europa.eu/en/library/new-practical-guide-data-governance-act (last accessed 9th December 2024)

European Commission, (2024), 'The European Data Market study 2024-2026', accessible at: https://digital-strategy.ec.europa.eu/en/library/european-data-market-study-2024-2026 (last accessed 9th December 2024)

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 9th December 2024)

European Parliament and The Council of the European Union, (2022), Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on harmonised rules on fair access to and use of data (Data Act), accessible at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A68%3AFIN (last accessed 9th December 2024)

European Parliament and The Council of the European Union, (2022), REGULATION (EU) 2022/868 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act), accessible at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R0868 (last accessed 9th December 2024)

World Economic Forum, (2024), 'Advancing Data Equity: An Action-Oriented Framework', accessible at: https://www3.weforum.org/docs/WEF_Advancing_Data_Equity_2024.pdf (last accessed 9th December 2024)

Acknowledgements

Corporate Partners

We are grateful to our network of corporate partners for their invaluable contributions:

boost·ai
Trust every conversation

hifo.co
Revealing the best in tech

Freshriver
AI with emotional intelligence

Individual Partners

We are also grateful to our network of individual supporters for their invaluable contributions:

Ademulegun Blessing James, Ademulegun Blessing James is a dedicated AI ethicist and governance expert with a passion for responsible innovation. Leveraging my extensive knowledge in AI, corporate governance, and compliance to ensure ethical AI implementation across industries. **Ademulegun** is specialized in identifying and mitigating algorithmic biases, particularly those affecting underrepresented communities and regions with limited data infrastructure. **Ademulegun is** passionate about driving awareness and influencing policy on the need for a robust data infrastructure in the Global South countries, especially, Africa for a homegrown and context-aware AI-powered innovations.

Anandaday Misshra, Anandaday Misshra, As a legal professional with over 27 years of experience, Anandaday Misshra specializes in data privacy, artificial intelligence, Goods and Services Tax (GST), international arbitration, international laws, and strategic dispute resolution across diverse jurisdictions. My career is dedicated to assisting organizations in navigating the complexities of legal compliance within an ever-evolving regulatory landscape.

Dr. Amritha Subhayan Krishnan, Dr. Amritha Subhayan Krishnan is a cultural foresight researcher and creative industries policy advisor specialising in AI governance and the Next Generation Internet. She leads Smart Story Labs, shaping human-centred futures in the digital ecosystem.

Carolyn Harrison, Carolyn Harrison is a A senior marketing professional and business leader with 25+ years' experience working in varied roles in different sectors. Carolyn has gained all round business experience creating and running companies and has a proven aptitude to build successful brands. For many years, she has run a successful marketing and management consultancy, with assignments looking at the convergence of new technologies – in particular positive disruptive models, evaluating the commercial opportunities globally across both public and private sectors. Equally In all elements of business activities Carolyn understands the importance of being totally commercially aware and customer focused. Having spent the last few years exploring ways to fix the current broken model of trying to conduct business in the digital world, she is passionate about rolling out Assured Clarity's unique innovative solution. Helping clients at a board level to 'Manage their Risk and Protect their Reputation', creating organisational resilience. As an experienced education and training specialist, Carolyn is keen to help organisations develop, Education, Awareness and Training programmes to help deliver positive outcomes throughout the whole organisation. GDPR (The new data protection legislation) has provided the perfect opportunity for organisations to address the whole mismanagement of information culture, which has lead to the current problem of cyber breaches and huge data losses.

Charles Kerrigan, Charles is part of teams working on transactions and consulting/advisory for emtech in the UK, EMEA, and the US. He was invited to be a founding member of the UK Parliament's Advisory Group on AI in 2016, acting as legal advisor to the group, and has remained a member to the present. He has worked in AI in academic and legal contexts since 2010. At CMS he is part of the firm's specialist emerging technologies team. He works on business model and go-to-market strategies in AI; on investment and M&A in the deep tech sectors; on implementation projects to establish compliance with AI regulations and standards; on technical writing and policies; and on AI literacy projects and other institutional training. His clients include global technology firms and financial institutions; VC and other deep tech investment firms; and governments and regulators. He has recently written the worldwide AI training modules for a global bank. He is a Board Advisor of Holistic AI https://www.holisticai.com/ and Home | AI & Partners (ai-and-partners.com) He sits on the advisory boards of the Investment Association Engine The IA Engine - FinTech accelerator from The Investment Association and the All Party Parliamentary Group on Artificial Intelligence (APPG AI) APPG AI 2024.2025 Brochure (May 2024) (biginnovationcentre.com). He is the Chair of the Technology Working Group of the Association of Real Estate Funds Tech Working Group - January 2020 (aref.org.uk). He teaches on AI and entrepreneurship at UCL.

Dave Bohnert, Dave Bohnert is the creator of **DataDave LegalBot** and the **Fairify app**, a toolset designed to assess small-scale supervised machine learning models using **Giskard** and **AIF360**. His work bridges technical audit tools with sociotechnical risk assessment aligned with the **EU AI Act**, focusing on model-level fairness, robustness, and transparency for startups and SMEs. He advocates for accessible, open-source AI compliance aligned with Article 10's principles of high-quality data, documentation, and governance.

Dr. Benedikt Kohn, Dr. Benedikt Kohn is a specialist lawyer in information technology law in the technology, media and telecommunications practice group of Taylor Wessing. He has particular expertise in legal issues related to digitization and artificial intelligence. His areas of expertise include IT contract drafting, advising on complex data protection projects, and advising on the implementation of new regulatory requirements for the use of AI. Dr. Benedikt Kohn regularly publishes and speaks on the topics of digitization and AI regulation.

Dr. Don Liyanage, Dr, Don Liyanage is an Experienced AI Research Engineer and a Technical Architect with a demonstrated history of working in the computer software industry. Skilled in 2nd and 3rd generation AI, Data Science, Complex Solutions design, multiple DBMS technologies, Cloud Computing and Distributed Systems. Strong research professional carrying out a Doctor of Philosophy (PhD) focused in Artificial Neural Network Reasoning with Case Based Reasoning in University of Manchester/Gloucestershire.

Ina Schoene, Ina Schoene is a Lead Auditor ISO/IEC42001 and Founder of Data Privacy and AI. She follows the practice-oriented approach to understand the requirements of AI-Act and the measures to implement this requirements based of the ISO/IEC42001 & additional & guides the companies on the path to get the corresponding certifications.

Jerry Silber, Jerry Silber is an accomplished attorney with a distinguished career spanning private practice, corporate counsel, and legal education. He recently retired from Verizon, where he served as Vice President and Deputy General Counsel, playing a key role in shaping the company's legal strategy across areas including broadcast law, telecommunications, outsourcing, contract negotiation, data security, and mergers and acquisitions. Prior to his tenure at Verizon, he practiced corporate law at a major New York City firm, focusing on broadcast and telecommunications law. Mr. Silber now leads his own law firm, where he consults for Frontier Internet and serves as the Fractional General Counsel for Screengeni.us, a startup operating in the streaming ecosystem. He is also a Fellow at World Commerce & Contracting, reflecting his continued engagement with cutting-edge developments in global contract and commercial practice. In parallel with his legal work, Mr. Silber has maintained a longstanding commitment to legal education. He is currently an Adjunct Professor of Law at the Elisabeth Haub School of Law at Pace University, and has taught graduate seminars in media law and ethics for over three decades at The New School, Iona University, and Manhattanville University. Mr. Silber is actively engaged in the intersection of law and emerging technologies, particularly artificial intelligence. He serves as an Advisor and Evangelist for AI 2030, where he authors a monthly column analyzing major legal developments affecting AI. He is also collaborating with AI 2030 and Cornell University on a Global AI Regulation Index and has contributed to several white papers for AI & Partners."

Lisa Ventura MBE, Lisa Ventura MBE FCIIS is an award-winning cyber security specialist, published writer/author, journalist and keynote speaker. She is the Chief Executive and Founder of Cyber Security Unity, a global community organisation that is dedicated to bringing individuals and organisations together who actively work in cyber security to help combat the growing cyber threat. As a consultant Lisa also provides cyber security awareness and culture change training, along with neurodiversity in the workplace training, and works with cyber security leadership teams to help them collaborate more effectively. She has specialist knowledge in the intersection of AI and cyber security, the human factors of cyber security/social engineering, cyber psychology, neurodiversity and diversity, equity, belonging and inclusion (DEIB). More information about Lisa can be found on www.lisaventura.co.uk.

Mitko Karushkov, Mitko Karushkov has been providing legal, regulatory, compliance, transactional and business solutions to international companies for more than 20 years now. Focused on enterprise companies and their strategic (or daily) operations, Mitko has solved matters related to the digital, tech or electronic assets of such businesses. Active and involved also in bridging between traditional and technology markets, including to the application of the EU DSA, DMA, AI and other regulations. Media, Telecoms, IPRs, Corporate, M&As are also part of the service portfolio of Mitko. For further information: www.karushkov.com.

Neil Oschlag-Michael, Neil Oschlag-Michael is Head of AI Risk and Security Manager in boost.ai. Prior to this he has worked with AI and built AI GRC solutions in 2021.AI, managed data in Denmark's National Genome Center, consulted in Valcon and as a freelancer, worked with technology in IBM and Tieto, and contributed to developing AI standards as an expert associate member of ISO/CEN-CENELEC.

Prof. Ingrid Vasiliu-Feltes, MD EMBA, Prof. Dr. Ingrid Vasiliu-Feltes is a visionary leader operating at the intersection of academia, business, government and not-for-profit sectors, recognized globally for her deep tech diplomacy and digital ethics efforts. With over two decades of executive experience, she has held numerous high-impact leadership roles and has extensive complex system integration expertise, driving the development of responsible, inclusive, diverse, sustainable AI, blockchain and other deep tech innovation ecosystems at a regional, national or international level. Her unique background positions her as a thought leader on how emerging or frontier technologies are posing unique ethical challenges and are reshaping law, regulatory frameworks, corporate governance, risk management, compliance and enterprise digital strategy. She is an alumna of MIT, Harvard, Stanford, Columbia University, and University of Miami's Herbert Business School. She is a Lean Six Sigma Master Black Belt, holding executive certifications in AI, Blockchain, Finance, Mediation, Tech Diplomacy, Human Rights, and Ethics. She has served as an expert advisor to numerous Fortune 100 and 500 companies, US DOD, IEEE, NIST, and EU, UN or G20-affiliated organizations, guiding them on strategic decisions around digital transformation, digital risk governance, digital trust, and digital cyber-ethics orchestration

Steven PAUL CDir, FIoD. Steven Paul is a board strategist, transformation and AI governance leader with 20+ years' executive experience at HSBC, SVB, Lloyds, Accenture, and BMO. A Chartered Director and NED, he serves on multiple boards, builds and advises boards on AI oversight, private LLMs, and transformation strategy. At Freshriver, he leads on AI Governance and Trust, helping institutions embed intelligence, integrity, and foresight into their business operating models and board governance.

Thomas Naylor, Founder and editor of hifo.co: the platform that enables tech buyers to more easily discover the right vendor for their Thomas has 25 years delivering enterprise IT transformation programmes and deep expertise in the full technology change lifecycle, from vendor selection and contract negotiation, through planning, to successful implementation He provides IT Due Diligence reports for PE companies and is a regular speaker at conferences and seminars on cyber resilience. He is also a Cyber Security vendor judge for SC Awards Europe.

Tomer Jordi Chaffer. Tomer Jordi Chaffer is an interdisciplinary researcher interested in the evolving relationship between AI, Web3, and society.

Dave Bohnert,
Founder & Lead Architect,
DataDave LegalBot

Tomer Jordi Chaffer,
Interdisciplinary Researcher

Dr. Don Liyanage,
Co-Founder,
Tikos

Jerry Silber,
AI 2030 Evangelist,
AI 2030

Prof. Ingrid Vasiliu-Feltes,
Founder and CEO, Institute for Science, Entrepreneurship and Investments

Charles Kerrigan,
Partner,
CMS UK

Dr. Amritha Subhayan Krishnan,
Founder and CEO,
Smart Story Labs

Lisa Ventura,
Chief Executive and Founder,
Cyber Security Unity

Dr. Benedikt Kohn,
Tech Attorney | AI Regulation | IT & Data, Taylor Wessing

Ademulegun Blessing James,
AI Ethicist

Anandaday Misshra,
Foiunder & Managing Director,
AMLEGALS

Ina Schöne,
Lead Auditor ISO/IEC42001 and Founder,
Data Privacy & AI

Mitko Karushkov,
Founder,
Karushkov Legal Solutions

Neil Oschlag-Michael,
Head of AI Risk and Security,
boost.ai

Thomas Naylor,
Founder and Editor,
higo

Steven Paul,
AI Transformer|
Board Director

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.