



AI & Partners

Amsterdam - London - Singapore

EU AI Act

Data Governance Act versus EU AI Act

A Mapping Exercise

July 2025

AI & Partners

Sean Musch, AI & Partners

Michael Borrelli, AI & Partners

Charles Kerrigan, CMS UK

Diogo Pereira Coelho, DPC Legal

Dr. Elise Victor, TruSTAR Learning LLC

Bruno Schneider, intangible Asset Finance Strategies

Danny Van Rijen, EU Policy Expert

Articles

EU AI Act

DGA



↔
VS



01010100
01010100
01010100
01010100
01010100
01010100
01010100
01010100



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.

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.

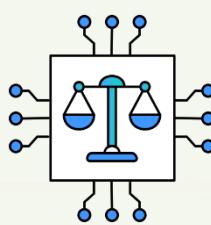
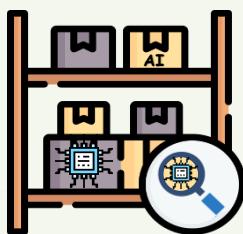
How Do We Do It?

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.

80%

of AI systems
are unknown



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.



Contents

Who Are We	2
Introduction	4
Key questions being asked about DGA	5
1. What is the main objective of the Data Governance Act (DGA)?	6
2. Why was the DGA introduced?	6
3. What are data intermediation services under the DGA?	6
4. How does data altruism work under the DGA?	6
5. What role does the European Data Innovation Board (EDIB) play?	7
6. How does the DGA support international data flows?	7
7. What safeguards exist for reusing sensitive public sector data?	7
8. How are data intermediation services regulated and monitored?	7
9. Who can become a recognised data altruism organisation?	8
10. What support structures are in place for implementing the DGA?	8
Understanding DGA.....	Error! Bookmark not defined.
Reuse of certain categories of data held by public sector bodies	10
Data intermediation services.....	11
Data altruism	12
European Data Innovation Board	13
International data flows	14
Mapping DGA to EU AI Act	Error! Bookmark not defined.
Calls to action	Error! Bookmark not defined.
Conclusion.....	33
References.....	34





Introduction

As the European Union deepens its commitment to building a fair and innovation-driven data economy, the intersection of the Data Governance Act (DGA) and the EU Artificial Intelligence Act (AI Act) is becoming increasingly significant. While the AI Act lays out obligations for the development and deployment of trustworthy AI systems—especially those classified as high-risk—the DGA provides the governance infrastructure to facilitate the secure, ethical, and transparent flow of data that AI systems rely on.

This report presents a practical mapping between the DGA and the AI Act to help stakeholders understand how data governance mechanisms underpin AI compliance. It highlights key areas of alignment, including the reuse of protected public sector data, the role of data intermediation services, and frameworks for data altruism and international transfers. Together, these regulatory pillars support a responsible and harmonized approach to AI innovation across Europe.

In clarifying these touchpoints, the report offers actionable insights for aligning data governance and AI lifecycle obligations—empowering organizations to enhance data accessibility and trust while upholding fundamental rights. Whether you are an AI developer, data governance lead, policymaker, or legal advisor, this guide supports efforts to build compliant, inclusive, and ethically grounded AI systems within the evolving EU regulatory landscape.



Best regards,

Sean Musch

Founder/CEO

AI & Partners

A handwritten signature in black ink, appearing to read "Sean Musch".



Key questions being
asked about DGA



1. What is the main objective of the Data Governance Act (DGA)?

The Data Governance Act aims to facilitate secure, ethical, and efficient data sharing across the European Union. It creates a legal framework to enable voluntary data sharing while protecting rights, fostering innovation, and supporting the development of Common European Data Spaces (CEDS). The DGA promotes trust by introducing new rules for data intermediaries, supporting data altruism, and regulating reuse of protected public sector data. By ensuring transparency, neutrality, and high standards for data handling, the DGA constitutes the foundational legislative pillar of the EU data strategy, supports the EU's digital economy, strengthens strategic autonomy, and encourages both public and private entities to participate in the data economy. It complements other instruments such as the Data Act, the Digital Markets Act, the Digital Services Act and the Artificial Intelligence Act (AI Act). Together, these instruments address the infrastructure layer (data access, sharing, and reuse), the platform governance layer (fairness, transparency, and user protection), and the algorithmic layer (trustworthy, human-centric AI). This multilayered legal architecture forms the backbone of the EU's digital transformation agenda, promoting technological innovation, digital sovereignty, and the protection of fundamental rights.

2. Why was the DGA introduced?

The DGA was introduced to address the lack of trust, interoperability, and legal clarity that hindered data sharing within and beyond the EU. While enormous amounts of data are generated across Europe, legal and technical barriers, privacy concerns, and dominance by Big Tech have limited its broader use. The DGA tackles these challenges by creating rules that ensure data is shared securely and fairly, especially by encouraging voluntary contributions and neutral intermediaries. It helps unleash the socioeconomic potential of data, fosters innovation, and strengthens EU competitiveness while safeguarding fundamental rights and data protection principles.

3. What are data intermediation services under the DGA?

Data intermediation services are neutral, regulated platforms that connect data holders (individuals or companies) with data users. These intermediaries facilitate data sharing without exploiting the data themselves. They must be legally and structurally separated from other business operations and cannot use the data for profit beyond the intermediation service. To operate, they must notify a competent authority and adhere to strict transparency, neutrality, and security standards. This framework aims to build trust, especially among SMEs and citizens, and serves as an ethical alternative to Big Tech-controlled data ecosystems, encouraging participation in the EU's data economy. These services may operate in B2B contexts (between companies), B2C contexts (enabling individuals to share their personal data with businesses), or as Personal Information Management Systems (PIMS), which empower individuals to control and manage access to their own data. Regardless of the model, they must meet the same neutrality and structural separation requirements.

4. How does data altruism work under the DGA?

Data altruism allows individuals and companies to voluntarily share their data—without compensation—for purposes of general interest, such as healthcare, environment, or public policy. Organisations facilitating this can register as “recognised data altruism organisations” if they meet requirements such as being not-for-profit, transparent, and committed to privacy. The DGA introduces a European consent form for data altruism to streamline permissions and withdrawals across the EU. These mechanisms ensure data is shared responsibly and ethically, building trust while unlocking





valuable datasets for research, innovation, and public benefit across Member States and sectors. As data altruism may involve the voluntary sharing of personal data, all such activities must fully comply with the General Data Protection Regulation (GDPR) and, where applicable, the Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), ensuring data subject rights, consent, purpose limitation, and data minimisation principles are respected.

5. What role does the European Data Innovation Board (EDIB) play?

The European Data Innovation Board (EDIB) provides expert guidance to harmonize data-sharing practices across the EU. Composed of national authorities, EU institutions, cybersecurity bodies, and SMEs, it supports implementation of the DGA by promoting best practices in data intermediation, altruism, and reuse of protected public sector data. It also helps prioritise cross-sector interoperability standards and proposes guidelines for Common European Data Spaces. The EDIB ensures coordination and consistency in applying the DGA, addressing legal and technical challenges while upholding EU values, privacy standards, and digital sovereignty in the evolving data economy.

6. How does the DGA support international data flows?

The DGA ensures that non-personal data shared with third countries is subject to safeguards equivalent to those in EU law. It prevents misuse of EU-held data by requiring third-country recipients to maintain EU-level protections and accept EU jurisdiction. This applies to data shared via public sector bodies, data intermediation services, and data altruism. The Commission may issue adequacy decisions and model contract clauses to facilitate compliant transfers. These provisions promote global data exchange while protecting economic interests, legal certainty, and public trust—especially important in maintaining the EU's strategic autonomy and competitive advantage globally.



7. What safeguards exist for reusing sensitive public sector data?

The DGA allows reuse of protected data held by public sector bodies—such as personal, confidential, or IP-protected data—under strict safeguards. Before reuse, such data must be anonymised or accessed within a secure processing environment. Reuse must be non-discriminatory, transparent, and proportionate, without creating exclusive rights. Public bodies may deny reuse but are encouraged to provide access for research and innovation. The regulation ensures that third-party rights, privacy, and system integrity are respected. Conditions for reuse focus on protecting fundamental rights while enabling the use of valuable datasets for public interest projects and cross-border collaboration. The DGA promotes the use of secure processing environments, certification schemes, and EU-wide standardisation initiatives to ensure trusted, auditable, and technically interoperable reuse of sensitive data across Member States.

8. How are data intermediation services regulated and monitored?

Data intermediation service providers must notify their national competent authority before operating. They must meet neutrality, transparency, and structural separation requirements—ensuring data is not used for unrelated commercial purposes. Once notified, they are listed in an EU-wide register and can use a special logo indicating their trusted status. Competent authorities monitor compliance and can take enforcement actions. These rules prevent misuse of data and ensure fair competition by creating a trustworthy ecosystem for data sharing. The framework also provides legal certainty and promotes innovation by encouraging more actors, including SMEs, to participate confidently.



9. Who can become a recognised data altruism organisation?

Any not-for-profit organisation operating in the EU that meets the DGA's transparency, governance, and data protection requirements can apply to become a recognised data altruism organisation. They must comply with a rulebook set by the Commission and offer technical and ethical safeguards for data contributors. These entities may include academic institutions, foundations, or civil society groups focused on advancing general interest objectives like research, health, or sustainability. Once recognised, they can use a dedicated logo and appear in the EU register. This status helps build trust, ensuring that donated data is used responsibly and transparently.

10. What support structures are in place for implementing the DGA?

To implement the DGA effectively, Member States must establish support structures including a single information point to guide re-users and competent bodies to assist public sector bodies with secure data sharing. These bodies may help with structuring data, ensuring interoperability, managing consent, and providing secure environments for processing. They act under public sector authority instructions but do not supervise. Data protection authorities may help out in this regard, but this depends on a case-by-case basis. For instance, the DGA also relates to non-personal data or sometimes there is specific law regarding public sector data which comes with its own levels of governance. These support mechanisms ensure technical and legal feasibility of data reuse, facilitate harmonised practices across the EU, and enable stakeholders to confidently engage in data sharing for innovation and research. By ensuring legal certainty and providing structured access to high-value datasets, these support mechanisms are expected to boost AI development, enhance public-sector innovation, and facilitate the emergence of EU-wide data-driven services in fields such as healthcare, energy, and mobility, contributing directly to the EU's digital sovereignty and global competitiveness.



Understanding DGA





Reuse of certain categories of data held by public sector bodies



What are the key goals?

The key goals are to enable safe reuse of protected data held by public sector bodies for purposes like scientific research, innovation, and policymaking. It aims to ensure data sharing under clear, secure, and fair conditions while safeguarding privacy and confidentiality. The framework encourages transparency, prevents exclusivity, and promotes broader access, especially for SMEs and researchers, without obligating public bodies to release data unless they choose to do so under regulated terms.



Why is it needed?

This framework is needed to unlock the value of protected public sector data that cannot be openly shared due to legal or ethical restrictions. By enabling controlled reuse, it supports innovation, research, and evidence-based policymaking while maintaining trust and compliance with privacy and IP laws. It also addresses barriers like lack of legal clarity and technical safeguards, and encourages fairer access to valuable data resources, particularly for smaller entities and researchers.

How does it work?

Public sector bodies may allow reuse of protected data in secure environments or with consent when anonymization isn't possible. Member States must create single information points and designate competent bodies to oversee compliance and support access. Data reuse must follow transparent, proportionate, and non-discriminatory rules, with safeguards for confidentiality and rights. Exclusive agreements are discouraged unless justified. This setup minimizes administrative burden and enables access especially for SMEs and researchers under clear, secure conditions. Importantly, public sector bodies must ensure that any reuse of personal data remains also in full compliance with the GDPR. Where anonymisation is not feasible, secure processing environments (mandated by the DGA) must be used to prevent unauthorized access and ensure compliance with privacy, IP, and trade secret protections. These environments act as technical safeguards that complement legal and ethical constraints, ensuring responsible secondary data use.



Data intermediation services



What are the key goals?

The primary goal of the Data Governance Act (DGA) regarding data intermediation services is to create a trusted environment for data sharing within the EU. By establishing a neutral and transparent framework, it aims to empower individuals and businesses to maintain control over their data while encouraging secure and voluntary data exchange. It addresses concerns around competitive disadvantage and misuse by defining strict obligations for intermediaries. Ultimately, it seeks to balance innovation and trust, enabling fair competition and fostering the development of Common European Data Spaces.

Why is it needed?

The DGA's provisions for data intermediation services are necessary because many companies are hesitant to share data due to concerns over losing competitive advantage and data misuse. Big Tech platforms dominate the data economy by controlling vast datasets, limiting opportunities for smaller actors. The regulation offers a trustworthy alternative that levels the playing field and encourages broader data access. By creating a neutral, secure mechanism for sharing, the DGA aims to remove barriers to data collaboration, protect users' rights, and stimulate innovation while ensuring compliance with EU data protection and competition principles. The DGA distinguishes among different types of data intermediation services, including those operating in B2B, B2C, and personal data management contexts (PIMS). Regardless of the configuration, all intermediaries must ensure full neutrality, maintain structural separation, and offer mechanisms for auditable consent and access control. These features are particularly relevant when intermediation supports AI development, ensuring that data used for model training has been accessed lawfully and with verifiable provenance.

How does it work?

In practice, data intermediaries act as neutral facilitators connecting data holders (e.g., individuals or companies) with data users. They can charge for their services but must not use the data for their own benefit. Intermediaries must maintain legal and structural separation between their data-sharing activities and any other business operations to avoid conflicts of interest. They are required to notify a competent authority before providing services, after which they can operate using an official EU-recognized label. These providers must ensure neutrality, follow transparency standards, and are subject to ongoing monitoring to safeguard compliance and maintain trust.





Data altruism



What are the key goals?

The key goal of data altruism under the Data Governance Act is to encourage individuals and companies to voluntarily share data for the public good, without expecting compensation. By enabling data contributions for objectives like improving healthcare, environmental protection, and mobility, the regulation promotes societal advancement. It seeks to build trust through transparency, clear safeguards, and strong ethical standards, ensuring that shared data is used responsibly. Ultimately, it aims to facilitate the creation of large, cross-border data pools that support research, innovation, and machine learning.



Why is it needed?

Although many are willing to share data for public interest purposes, existing data-sharing mechanisms are limited or lack sufficient trust. Without proper tools and clear protections, individuals and companies hesitate to participate. The Data Governance Act addresses this by creating a legal and technical framework that supports ethical and secure data altruism. It provides structure, transparency, and legal certainty to encourage responsible data sharing, especially for sectors like health and science. By standardizing consent and enabling trustworthy data reuse, the regulation empowers contributors and strengthens the data ecosystem for societal benefit across the EU.

How does it work?

In practice, organisations that facilitate data altruism can register as “data altruism organisations recognised in the Union”. To qualify, they must be not-for-profit, transparent, and uphold data protection standards. They must comply with an EU-developed rulebook outlining technical, security, and communication obligations. Recognised organisations can use a common logo and appear in a public EU register. A standardised, modular European consent form allows individuals and companies to give or withdraw permission to share data easily, supporting cross-border use. Moreover, organisations engaging in data altruism must implement robust governance mechanisms, including transparent internal decision-making processes and mechanisms for responding to data subject requests. The modular European consent form introduced by the DGA provides not only legal clarity but also a technological standard that can be embedded into digital identity and self-sovereign data systems. This aligns directly with the AI Act’s emphasis on traceability, documentation, and voluntary participation in the development of trustworthy AI systems.





European Data Innovation Board



What are the key goals?

The European Data Innovation Board (EDIB) aims to promote harmonized and efficient data sharing across the EU. Its key goals include supporting best practices in data intermediation and altruism, guiding the secure use of sensitive public sector data, and prioritizing cross-sector interoperability standards. EDIB seeks to ensure that the governance of data flows aligns with EU values like trust, transparency, and privacy. By offering strategic guidance and expertise, it strengthens the foundation for Common European Data Spaces and ensures consistency in how data is accessed, shared, and protected across the EU.



Why is it needed?

The EDIB is essential to unify and coordinate efforts across the EU in managing and sharing data responsibly and effectively. Given the diversity of national practices and legal frameworks, there's a need for a central advisory body to ensure consistency and foster collaboration. It addresses challenges like cross-border interoperability, secure data sharing, and protection of sensitive or non-open public data. By providing expert advice and harmonized guidelines, the EDIB helps ensure that new data-sharing models—especially under the Data Governance Act—are implemented uniformly, with safeguards and standards that uphold the EU's digital sovereignty and fundamental rights.

How does it work?

The EDIB operates as an expert advisory body composed of representatives from national authorities, EU institutions, cybersecurity bodies, and SMEs. It meets regularly to exchange knowledge and shape recommendations related to data sharing, especially in areas like data altruism, intermediation, and non-open public data. The Commission facilitates its work, and additional experts may be appointed through calls. EDIB can propose guidelines for implementing Common European Data Spaces and ensuring proper safeguards for international data transfers. Its inclusive structure ensures diverse stakeholder input and helps shape coherent, practical EU-wide policies and standards.



International data flows



What are the key goals?

The key goals of the DGA regarding international data flows are to support an open yet secure global exchange of data while safeguarding EU values. It aims to enhance the Union's strategic autonomy, boost economic growth, and strengthen its competitiveness in the global data economy. By setting clear rules for non-personal data transfers, it fosters trust among stakeholders and ensures that international data-sharing aligns with the Union's legal framework. This balances openness with protection, enabling the EU to participate actively in global data ecosystems without compromising on data security or sovereignty.



Why is it needed?

In practice, the DGA requires that non-personal data transferred internationally is protected to the same standards as in EU law. Any third-country reuser must accept EU-level safeguards and legal jurisdiction. These rules apply across all DGA domains: public sector data, data intermediation, and data altruism. The Commission may issue adequacy decisions—mirroring those under GDPR—if a third country ensures equivalent protection. Additionally, model contractual clauses may be provided to help public bodies and reusers structure compliant international agreements. These mechanisms ensure secure, lawful, and transparent data transfers beyond EU borders, upholding EU interests and trust. For AI systems trained on globally sourced datasets, the DGA's restrictions on non-personal data transfers act as a legal backstop to mitigate jurisdictional risk. These measures are particularly relevant where high-risk AI systems depend on structured or real-time input from third countries. The DGA thus supports the AI Act's Article 9 (risk management system) and Recitals concerning third-country interference, enhancing the Union's capacity to defend its digital sovereignty and fundamental rights in the face of extraterritorial data demands.

How does it work?

In practice, the DGA requires that non-personal data transferred internationally is protected to the same standards as in EU law. Any third-country reuser must accept EU-level safeguards and legal jurisdiction. These rules apply across all DGA domains: public sector data, data intermediation, and data altruism. The Commission may issue adequacy decisions—mirroring those under GDPR—if a third country ensures equivalent protection. Additionally, model contractual clauses may be provided to help public bodies and reusers structure compliant international agreements. These mechanisms ensure secure, lawful, and transparent data transfers beyond EU borders, upholding EU interests and trust.



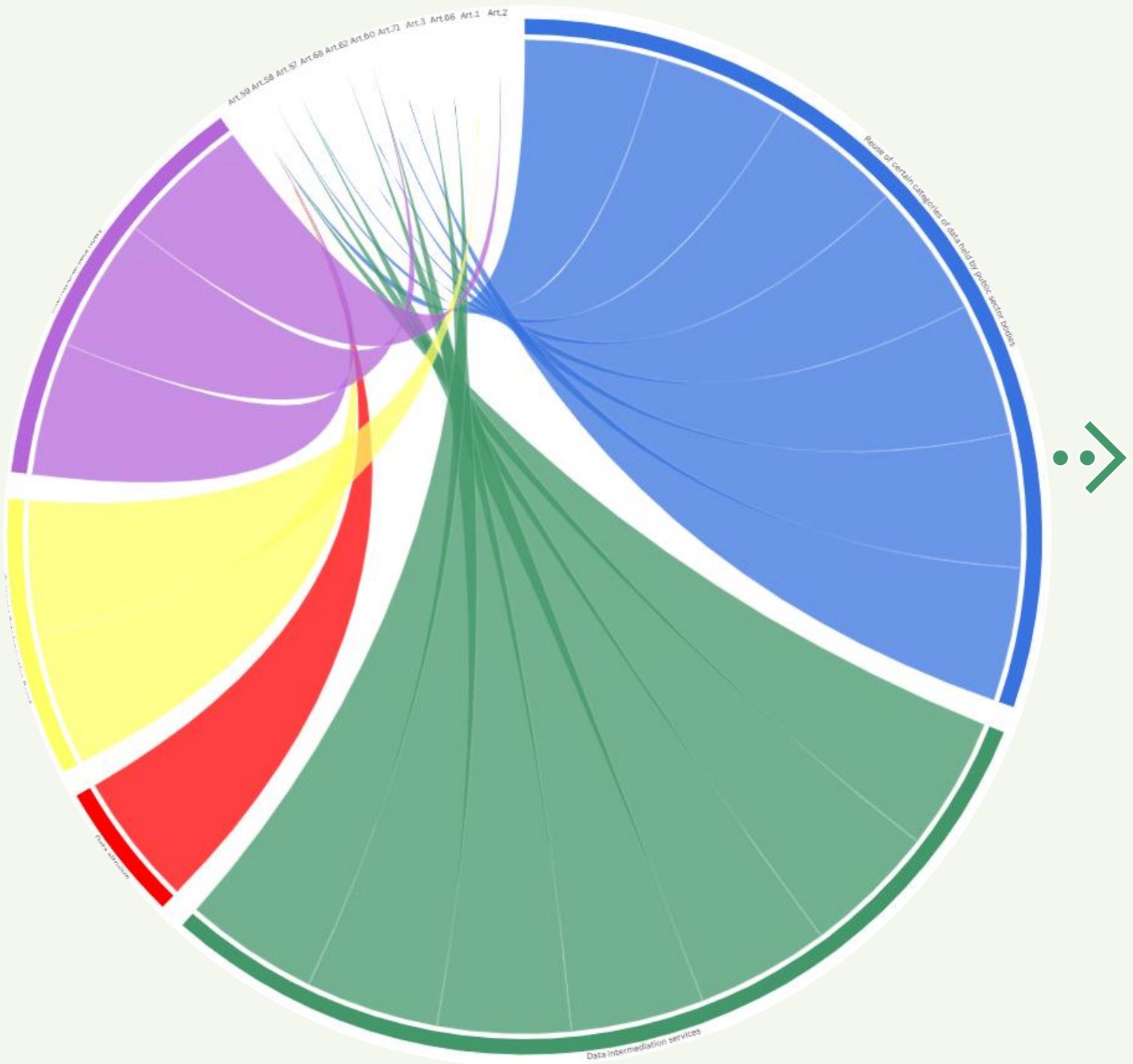
Mapping DGA to EU AI Act





DGA

EU AI Act





DGA		EU AI Act		
Section	Description	Article(s)	Explanation	Action
Reuse of certain categories of data held by public sector bodies	<p>Purpose: To enable the safe and controlled reuse of protected data (e.g., personal, confidential, or commercially sensitive data) held by public sector bodies, particularly for scientific research, innovation, and policymaking.</p> <p>Key Focus:</p> <p>Establishes a framework for reusing data that cannot be made openly available due to legal restrictions (e.g., privacy, trade secrets, IP rights).</p> <p>Encourages reuse by providing clear rules, technical safeguards, and secure processing environments to protect rights and data integrity.</p> <p>Public sector bodies are not obligated to make data reusable but are encouraged to do so under non-discriminatory, proportionate, and transparent conditions.</p> <p>Allows reuse only within secure environments or based on consent when anonymization is not possible.</p>	59, 58, 57, 68, 62, 60, 71	<p>AI Regulatory Sandboxes</p> <ul style="list-style-type: none">AI regulatory sandboxes are established to provide a controlled environment for the development, testing, and validation of innovative AI systems. These sandboxes facilitate the safe and controlled reuse of data, including personal data, under secure conditions.Details the functioning of AI regulatory sandboxes, emphasizing simple and clear procedures to encourage participation, especially by SMEs and start-ups. This aligns with the goal of minimizing administrative burdens and promoting access.The AI Act (Article 59) mandates that sandboxes support the development of compliant, rights-preserving AI systems, especially high-risk applications. Participation is voluntary, and sandbox projects must include risk mitigation plans,	<p>Deploy Secure Data Environments for AI Training Establish secure processing environments (as defined under Article 5 DGA) for accessing and reusing protected public sector data, particularly where anonymisation is not feasible. These environments must guarantee technical and organizational safeguards in line with the AI Act (Articles 10 and 17), GDPR (Article 32), and relevant IP/trade secret regimes. Member States should ensure non-discriminatory access, prioritizing SMEs and research entities to support ethical, high-quality AI training and reduce systemic data access asymmetries.</p> <p>Leverage AI Regulatory Sandboxes for High-Risk Prototypes Engage with AI regulatory sandboxes (AI Act Article 59) to test and refine high-risk AI systems in real-world conditions under the supervision of competent authorities. Ensure sandbox participation</p>





	<p>Prevents exclusive agreements unless justified, ensuring broad and fair access to valuable datasets.</p> <p>Promotes access especially for SMEs, start-ups, and scientific research under conditions that minimize administrative burden.</p> <p>Member States must establish single information points and competent bodies to support public sector entities and facilitate access.</p>		<p>document safeguards, and submit to supervisory authority oversight. Importantly, the sandboxes function not only as legal test beds but also as regulatory learning mechanisms, providing feedback loops for future standard-setting and enforcement practices at the EU level.</p> <p>Data Processing and Protection</p> <ul style="list-style-type: none">Allows for the further processing of personal data within AI regulatory sandboxes for developing AI systems in the public interest. It ensures that data processing is secure and that personal data is deleted after the sandbox participation ends.Governs the testing of high-risk AI systems in real-world conditions, ensuring that data is processed securely and that personal data is deleted post-testing. Any further processing of personal data within the sandbox must comply with	<p>integrates risk management, human oversight, and data protection-by-design from early development stages. Sandboxes help bridge innovation and compliance, especially for SMEs and researchers navigating complex legal requirements.</p> <p>Ensure Data Governance Compliance Across the AI Lifecycle</p> <p>Embed data governance obligations (AI Act Article 10) into all phases of the AI lifecycle (from data collection and preprocessing to training, validation, and retraining). Ensure datasets are representative, accurate, and free of bias, and that data lineage is fully documented. Harmonize these practices with GDPR, DGA, and sector-specific regulations, forming a robust compliance architecture across jurisdictions.</p>
--	--	--	--	--





			<p>Article 6(4) of the GDPR and relevant guidance from the EDPB. The sandbox must also integrate privacy-by-design and data minimisation principles (GDPR Article 25) and align with AI Act Article 10 on data governance, especially around traceability, quality, and representativeness of data used in high-risk AI training and testing. This supports the safe reuse of data under controlled conditions.</p> <p>Support for SMEs and Innovation</p> <ul style="list-style-type: none">• Encourages Member States to provide SMEs, including start-ups, with priority access to AI regulatory sandboxes. This supports the reuse of data for innovation and research while minimizing administrative burdens.• The AI Act obliges Member States to ensure that regulatory sandboxes are accessible to SMEs, start-ups, and not-for-profit research organisations, and that participation is free of charge or	
--	--	--	---	--





			<p>subject to minimal administrative fees (Recital 143). This ensures that AI innovation ecosystems are inclusive, balanced, and not skewed in favour of large economic operators.</p> <p>Transparency and Access</p> <ul style="list-style-type: none">• Establishes an EU database for high-risk AI systems, ensuring transparency and access to information about AI systems, which can facilitate the reuse of data for research and innovation.• The EU database for high-risk AI systems (AI Act Article 71) must include details on the system's intended purpose, risk category, compliance evidence, and post-market monitoring plans. This database is pivotal for ensuring public oversight, supporting civil society scrutiny, and facilitating academic reuse of AI system information for auditing or accountability research. <p>Governance and Oversight</p> <ul style="list-style-type: none">• Involves a scientific panel of	
--	--	--	--	--





			<p>independent experts to support the implementation and enforcement of the regulation, ensuring that data reuse aligns with legal and ethical standards.</p> <ul style="list-style-type: none">• The AI Act (Article 65) provides for the establishment of the AI Office, a central EU-level authority under the Commission, which will coordinate enforcement, standard-setting, and oversight. The scientific panel of independent experts will advise both the Commission and Member States on best practices for risk mitigation, technical documentation, and data governance. This multi-level governance model ensures both legal consistency and responsiveness to evolving risks.	
Data intermediation services	<p>Purpose: To establish a trustworthy, neutral environment for data sharing between individuals/companies and data users.</p> <p>Key Focus: Encourages data</p>	57, 3, 58, 59, 60, 62, 66	<p>AI Regulatory Sandboxes</p> <ul style="list-style-type: none">• AI regulatory sandboxes are established to provide a controlled environment for the development, testing, and validation of innovative AI	<p>Register as a Neutral AI Data Intermediary If engaging in data brokerage for AI development, register as a data intermediation service provider under Article 10 DGA. Maintain strict legal, structural, and</p>





	<p>sharing by removing fear of misuse or loss of competitive advantage.</p> <p>Requires data intermediaries to remain neutral, legally separated from other business operations.</p> <p>Intermediaries cannot use the data for their own benefit.</p> <p>Providers must notify authorities and are monitored to ensure compliance.</p>		<p>systems. These sandboxes facilitate the safe and controlled reuse of data, including personal data, under secure conditions.</p> <ul style="list-style-type: none">This article details the functioning of AI regulatory sandboxes, emphasizing simple and clear procedures to encourage participation, especially by SMEs and start-ups. This aligns with the goal of minimizing administrative burdens and promoting access. <p>Data Processing and Protection</p> <ul style="list-style-type: none">Allows for the further processing of personal data within AI regulatory sandboxes for developing AI systems in the public interest. It ensures that data processing is secure and that personal data is deleted after the sandbox participation ends.Governs the testing of high-risk AI systems in real-world conditions, ensuring that data is processed securely and that personal data is deleted post-	<p>operational separation from any AI development or deployment activities to prevent conflicts of interest. Ensure neutrality, avoid self-preferencing, and comply with notification, transparency, and auditability requirements. This supports a level playing field, especially for SMEs, and mitigates risks of data monopolisation and market foreclosure.</p>
--	--	--	---	--





			<p>testing. This supports the safe reuse of data under controlled conditions.</p> <p>Support for SMEs and Innovation</p> <ul style="list-style-type: none">• Encourages Member States to provide SMEs, including start-ups, with priority access to AI regulatory sandboxes. This supports the reuse of data for innovation and research while minimizing administrative burdens. <p>Transparency and Access</p> <ul style="list-style-type: none">• Establishes an EU database for high-risk AI systems, ensuring transparency and access to information about AI systems, which can facilitate the reuse of data for research and innovation. <p>Governance and Oversight</p> <ul style="list-style-type: none">• Involves a scientific panel of independent experts to support the implementation and enforcement of the regulation, ensuring that data reuse aligns with legal and ethical standards.	
Data altruism	Purpose: To enable voluntary sharing of data by individuals and	59	<p>Purpose and Key Focus</p> <ul style="list-style-type: none">• Voluntary Data Sharing: The concept of data	Support Ethical AI Through Data Altruism Facilitate voluntary



	<p>companies for the public good, without expecting compensation.</p> <p>Key Focus:</p> <p>Supports research and innovation in areas like health, environment, and mobility.</p> <p>Organisations can register as "recognised data altruism organisations" if they meet strict not-for-profit, transparency, and security criteria.</p> <p>A common EU consent form facilitates consistent, cross-border data contributions.</p> <p>The Commission oversees and supports this framework with a dedicated rulebook and public registry.</p>		<p>altruism aligns with the EU AI Act's emphasis on supporting innovation and research, particularly in areas like health, environment, and mobility. The Act encourages the use of data for public interest purposes, which is a core aspect of data altruism.</p> <p>Recognised Data Altruism Organisations</p> <ul style="list-style-type: none">• Not-for-Profit and Transparency Criteria: While the EU AI Act does not explicitly mention "recognised data altruism organisations," it emphasizes transparency and accountability in the use of AI systems. This aligns with the criteria for organisations to be recognized as data altruism entities, ensuring they operate under strict not-for-profit and transparency guidelines. <p>Common EU Consent Form</p> <ul style="list-style-type: none">• Cross-Border Data Contributions: The EU AI Act supports the harmonization of data practices across Member States, which is essential for facilitating consistent, cross-	<p>data sharing for trustworthy, public-interest AI applications by adopting the data altruism framework under Articles 16–22 DGA. Utilize the standardized European data altruism consent form, ensure data subjects can easily withdraw consent, and comply fully with GDPR Articles 6 and 7. Prioritize use cases in health, climate, urban mobility, and education. Where appropriate, pursue formal recognition as a Data Altruism Organisation, signalling commitment to ethical data governance and strengthening trust in AI ecosystems.</p>
--	---	--	---	--





			<p>border data contributions. The Act's provisions on data governance and protection ensure that data sharing is conducted securely and transparently.</p> <p>Oversight and Support by the Commission</p> <ul style="list-style-type: none">• Dedicated Rulebook and Public Registry: The EU AI Act establishes frameworks for oversight and support by the Commission, similar to the proposed rulebook and registry for data altruism. This ensures that data sharing initiatives are monitored and supported at the EU level, promoting trust and compliance.	
European Data Innovation Board	<p>Purpose: To establish a trustworthy, neutral environment for data sharing between individuals/companies and data users.</p> <p>Key Focus: Encourages data sharing by removing fear of misuse or loss of competitive advantage.</p> <p>Requires data intermediaries to remain neutral, legally separated from other</p>	59, 1	<p>Purpose and Key Focus</p> <ul style="list-style-type: none">• Trustworthy Environment for Data Sharing: The EU AI Act emphasizes the importance of creating a trustworthy environment for data sharing, which aligns with the purpose of the European Data Innovation Board. This is reflected in the Act's focus on transparency, accountability, and the protection of	<p>Support Ethical AI Through Data Altruism</p> <p>Facilitate voluntary data sharing for trustworthy, public-interest AI applications by adopting the data altruism framework under Articles 16–22 DGA. Utilize the standardized European data altruism consent form, ensure data subjects can easily withdraw consent, and comply fully with GDPR Articles 6 and</p>





	<p>business operations.</p> <p>Intermediaries cannot use the data for their own benefit.</p> <p>Providers must notify authorities and are monitored to ensure compliance."</p> <p>"Purpose:</p> <p>To enable voluntary sharing of data by individuals and companies for the public good, without expecting compensation.</p> <p>Key Focus:</p> <p>Supports research and innovation in areas like health, environment, and mobility.</p> <p>Organisations can register as "recognised data altruism organisations" if they meet strict not-for-profit, transparency, and security criteria.</p> <p>A common EU consent form facilitates consistent, cross-border data contributions.</p> <p>The Commission oversees and supports this framework with a dedicated rulebook and public registry.</p>		<p>fundamental rights.</p> <ul style="list-style-type: none">• Neutrality of Data Intermediaries: While the EU AI Act does not explicitly mention data intermediaries, it emphasizes the need for transparency and neutrality in the handling of data, ensuring that intermediaries do not misuse data for their own benefit. <p>Compliance and Monitoring</p> <ul style="list-style-type: none">• Notification and Monitoring: The Act requires providers to comply with specific obligations and be subject to monitoring to ensure adherence to the regulations. This aligns with the requirement for data providers to notify authorities and be monitored for compliance.• Beyond notification and monitoring obligations, AI providers participating in regulatory sandboxes must maintain comprehensive documentation and audit trails under AI Act Articles 11–13, covering system design, data lifecycle,	<p>7. Prioritize use cases in health, climate, urban mobility, and education. Where appropriate, pursue formal recognition as a Data Altruism Organisation, signalling commitment to ethical data governance and strengthening trust in AI ecosystems.</p>
--	---	--	--	--



			<p>performance testing, and risk controls. This ensures that even in experimental phases, high-risk AI development remains transparent, traceable, and subject to post-hoc accountability.</p> <p>Data Altruism</p> <p>Purpose and Key Focus</p> <ul style="list-style-type: none">• Voluntary Data Sharing for Public Good: The EU AI Act supports the voluntary sharing of data for public interest purposes, particularly in areas like health, environment, and mobility. This aligns with the purpose of data altruism.• Recognised Data Altruism Organisations: Although the Act does not specifically mention "recognised data altruism organisations," it emphasizes transparency and accountability, which are key criteria for such organisations. <p>Cross-Border Data Contributions</p> <ul style="list-style-type: none">• Common EU Consent Form: The Act supports harmonization across Member States, facilitating	
--	--	--	--	--



			<p>consistent, cross-border data contributions. This is essential for the effective implementation of data altruism.</p> <p>Oversight and Support</p> <ul style="list-style-type: none">Commission's Role: The EU AI Act outlines the role of the Commission in overseeing and supporting frameworks that promote innovation and data sharing, similar to the proposed rulebook and public registry for data altruism.	
International data flows	<p>Purpose: To ensure safe, transparent, and legally consistent transfer of non-personal data to third countries.</p> <p>Key Focus: Extends GDPR-like safeguards to non-personal data in the context of international transfers. Requires third-country data users to uphold EU-level protections and accept EU jurisdiction. Allows the Commission to issue adequacy decisions or model contractual clauses.</p>	59, 2, 60	<p>Purpose and Key Focus Safe and Transparent Data Transfer</p> <ul style="list-style-type: none">GDPR-like Safeguards: While the EU AI Act primarily focuses on AI systems, it emphasizes the protection of fundamental rights and data governance, which aligns with the extension of GDPR-like safeguards to non-personal data in international transfers. <p>EU-Level Protections and Jurisdiction</p> <ul style="list-style-type: none">Article 2 Scope: The EU AI Act applies to providers and deployers of AI systems within the Union, as well as those outside the	<p>Control International AI Data Transfers Before transferring AI-related datasets (especially for training or deploying high-risk AI systems) ensure third-country recipients provide equivalent protections under AI Act Article 2(1)(c) and DGA Chapter V. Adopt model contractual clauses or use adequacy decisions and ensure adherence to ethical design principles (AI Act Articles 8–9). Clarify jurisdictional accountability and risk-sharing mechanisms contractually. These measures reinforce strategic autonomy, safeguard EU values, and reduce</p>



	<p>Ensures that data sharing abroad supports EU strategic autonomy, trust, and competitiveness.</p>		<p>Union whose outputs are used within it. This ensures that third-country data users must uphold EU-level protections and accept EU jurisdiction.</p> <p>Mechanisms for International Data Transfers</p> <p>Adequacy Decisions and Model Contractual Clauses</p> <ul style="list-style-type: none">• Article 59 Further Processing: Although focused on personal data within AI regulatory sandboxes, the principles of secure data processing and compliance with Union law can be extended to non-personal data transfers, supporting the use of adequacy decisions or model contractual clauses.• The AI Act encourages alignment with the DGA's international data transfer safeguards (Chapter V) when non-personal data is involved. This includes ensuring functional equivalence with EU law, using model contractual clauses, and submitting to EU jurisdiction (Article 2(1)(c) of the AI	<p>regulatory fragmentation in cross-border AI supply chains.</p>
--	---	--	--	---





			<p>Act). In mixed datasets, the GDPR continues to apply, with no derogation via the sandbox framework.</p> <p>Strategic Autonomy, Trust, and Competitiveness Supporting EU Strategic Goals</p> <ul style="list-style-type: none">• Article 60 Testing in Real World Conditions: This article emphasizes the need for compliance with Union law during testing, which can be interpreted as supporting strategic autonomy and trust in data sharing practices.• Considering Articles 1 and 5 of the AI Act, the sandbox and data reuse mechanisms also operationalize the EU's digital strategic autonomy doctrine. They reduce dependency on extra-EU data sources and AI training pipelines, enhance competitiveness of the internal market, and embed democratic oversight and fundamental rights into the Union's AI innovation fabric.	
--	--	--	--	--



Calls to Action





Leverage DGA-Compliant Data Reuse for AI Training Integrity

The DGA establishes secure frameworks for reusing protected public sector data. Applying these reuse conditions when sourcing training data for AI systems ensures compliance with the AI Act's requirements on data quality, traceability, and legal sourcing—particularly for high-risk systems.



Register as a Trusted Data Intermediary to Support Fair AI Access

The DGA requires data intermediation services to operate with neutrality and transparency. Registering as a compliant intermediary strengthens your role in ethical data sharing and supports equitable data access for AI system development, in line with the AI Act's fairness and accountability goals.



Embed Data Altruism Mechanisms into AI Development Pipelines

In aligning with the DGA's framework for data altruism—including use of the standardized EU consent form—AI developers can legally and ethically source data for public-interest AI applications, reinforcing the AI Act's emphasis on transparency, social benefit, and voluntary participation.



Use DGA Safeguards to Enable Lawful International AI Data Transfers

The DGA mandates EU-level protections for international non-personal data transfers. Implementing these safeguards ensures that data used in AI systems—especially for cross-border training or deployment—meets the AI Act's requirements for lawful, transparent, and jurisdictionally sound data governance.





Conclusion

The convergence of the Data Governance Act (DGA) and the EU Artificial Intelligence Act represents a foundational shift in how data and AI systems are governed across the European Union. Together, these frameworks support a more coherent, rights-preserving, and innovation-friendly regulatory model—one that emphasizes transparency, trust, and accountability at every stage of AI development and deployment.

This mapping document has shown how the DGA and the AI Act complement one another: the DGA provides the mechanisms for ethical and secure data access—through reuse of public sector data, data intermediation services, and data altruism—while the AI Act establishes clear rules for risk-based oversight, human-centric design, and the safe use of AI technologies. For AI developers, compliance professionals, and data governance leads, understanding these synergies is essential to navigating complex obligations while unlocking the full potential of European data and AI ecosystems.

However, realizing the benefits of this alignment will demand strong operational follow-through. Organizations must embed data stewardship practices into their AI workflows, adopt secure data-sharing mechanisms, and ensure governance frameworks are in place for compliance across both acts. For SMEs and public bodies alike, early implementation, standardization, and collaboration will be key to overcoming resource and technical barriers.

Ultimately, forward-thinking organizations are already demonstrating how integrating DGA principles into AI design can accelerate trustworthy innovation, foster public confidence, and reinforce Europe's leadership in ethical technology. Together, the DGA and the AI Act form the backbone of a digital future that is not only intelligent—but also inclusive, transparent, and fundamentally human-centric.





References

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) (Text with EEA relevance), accessible at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R0868> (last accessed 10th May 2025)

European Parliament and The Council of the European Union, (2023), Commission Implementing Regulation (EU) 2023/1622 of 9 August 2023 on the design of common logos to identify data intermediation services providers and data altruism organisations recognised in the Union, accessible at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32023R1622> (last accessed 14th July 2025)

European Parliament and The Council of the European Union, (2024), 2024/1689 Regulation (EU) 2024/1689 of the European Parliament and of The Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), accessible at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401689 (last accessed 10th May 2025)





Important notice

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

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

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

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