ri

AI & Partners

Amsterdam - London - Singapore

EU AI Act

Data Act versus EU AI Act

A Mapping Exercise

July 2025

AI & Partners

Sean Musch, AI & Partners

Michael Borrelli, AI & Partners

Charles Kerrigan, CMS UK

Richard Self, University of Derby

Lord Chris Holmes, House of Lords

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

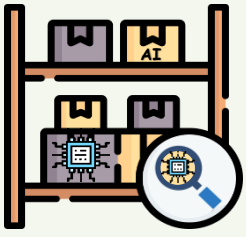
What Do We Do?

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?

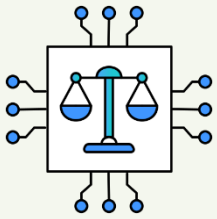
Do you know what AI systems you have? Identify all known and unknown AI systems (algorithms, LLMs, prompts, and models) from all internal and external AI vendors, automated by generating your inventory. Overall, 80% of AI inventory is unknown to our clients.

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.

Contents

Introduction

As the European Union continues to construct a digital single market rooted in openness, fairness, and innovation, the alignment between the Data Act (DA) and the EU Artificial Intelligence Act (AI Act) becomes a cornerstone of this vision. The AI Act sets out comprehensive obligations for the safe and ethical deployment of AI systems—particularly those deemed high-risk—while the Data Act ensures that the data fuelling these systems is accessible, portable, and governed under principles of fairness and interoperability.

This report offers a strategic mapping between the Data Act and the AI Act, designed to help stakeholders navigate their combined obligations. It explores how business-to-business data sharing, real-time user access to IoT-generated data, and robust safeguards for international data flows all reinforce AI transparency, traceability, and accountability. From dispute resolution mechanisms to protections against unfair contractual terms, the synergies between the two acts create a foundation for lawful and trustworthy AI innovation.

By connecting the data-sharing rights and obligations under the Data Act with the lifecycle requirements of high-risk AI systems under the AI Act, this report equips developers, compliance officers, policymakers, and legal practitioners with actionable guidance. It supports organizations in embedding legal interoperability, enhancing data governance, and ensuring that AI development across the EU remains competitive, rights-respecting, and future-ready.

Best regards,

Sean Musch

Founder/CEO

AI & Partners

Key questions being asked about Data Act

1. What is the main objective of the EU Data Act?

The Data Act aims to establish fair rules for accessing and using data within the EU. It promotes a more competitive data economy by ensuring that users of connected products and related services can access and share the data they generate. By defining clear rights and obligations, the Act empowers consumers and businesses to benefit from data they help create while preventing data hoarding by manufacturers or large platforms. It complements existing laws like the GDPR and supports innovation, competition, and digital transformation across sectors.

2. How does the Data Act interact with the GDPR?

The Data Act fully respects the GDPR. Where personal data is involved, the GDPR takes precedence. However, the Data Act complements the GDPR by introducing real-time portability rights for users, including access to non-personal data. Data protection authorities remain responsible for enforcing GDPR obligations. In cases where both the GDPR and the Data Act apply, users won't need to approach different authorities, simplifying redress. The Data Act's provisions encourage a harmonized and fair data-sharing environment while ensuring that personal data remains protected under existing EU privacy laws.

3. Who qualifies as a "user" under the Data Act?

A "user" is a natural or legal person that either owns a connected product, has contractual rights to use it (like through renting or leasing), or receives a related digital service. Only users established in the EU are covered. Users have the right to access and share data generated through their use of such products or services. They may also instruct the data holder to share the data with a third party. This ensures users—not just manufacturers or service providers—can benefit from the data they co-generate.

4. What types of data fall within the scope of the Data Act?

The Data Act applies to raw and pre-processed data generated by connected products or related services, provided it's readily available to the data holder without disproportionate effort. This includes sensor data like temperature or speed, along with metadata that explains how it was collected. Highly enriched or inferred data, such as those resulting from complex algorithms or proprietary models, are excluded. Also excluded is creative content (e.g., photos or videos) meant for human consumption. The focus is on opening access to operational and functional data, not IP-protected materials.

5. Does the Data Act apply to second-hand connected products?

Yes, the Data Act applies equally to second-hand connected products. New owners or renters of such products gain user rights under the Act. The seller must inform the new user about how to access the data and who the data holders are. This ensures continuity of data rights even as the product changes hands. The transparency obligation helps maintain clarity and access, allowing new users to benefit from data generated both during and prior to their ownership, provided such access respects other users' rights and applicable legal protections.

6. Can users monetize their non-personal data under the Data Act?

Yes, users can monetize their non-personal data. They may share or license access to this data with third parties or data holders, even for commercial purposes, as long as contractual agreements are in place. The Act allows for compensation in return for data access and use, and users can even waive certain rights if properly compensated. This flexibility supports a data economy where users—not just corporations—can extract value from the data they generate through connected products and services, provided personal data rights and confidentiality protections are respected.

7. What rights do data holders have under the Data Act?

Data holders are required to share certain data but retain important protections. They can refuse or suspend access if it threatens trade secrets, safety, or security, using mechanisms known as “handbrakes.” Trade secrets are protected through confidentiality agreements and technical safeguards. Data holders may also request compensation when sharing data with third parties. Furthermore, the Act restricts data recipients from using shared data to develop competing products. These safeguards ensure data sharing obligations do not undermine legitimate commercial interests or investments in data-generating technologies.

8. Are manufacturers obligated to redesign products for direct data access?

No, manufacturers are not required to redesign products solely to enable direct data access. However, the Data Act encourages providing data access in a way that is relevant and technically feasible. Manufacturers can choose between enabling direct access (user extracts data themselves) or indirect access (user requests data from the data holder). The method must be clearly explained to the user. Where direct access is provided, manufacturers can still impose conditions, such as confidentiality obligations, especially when trade secrets are involved. Flexibility helps balance usability with commercial protections.

9. Can public sector bodies request data under the Data Act?

Yes, under certain conditions. Public bodies may request data in cases of public emergencies or for tasks explicitly provided by law (e.g., disaster recovery or public health). Such requests must be justified, proportionate, and time-limited. Data shared this way does not become public information and cannot be freely reused. The Act ensures sensitive data like personal information or trade secrets are protected. Cross-border requests are allowed, but must be notified to competent national authorities. These provisions balance societal needs with safeguards for business and individual rights.

10. What mechanisms exist for resolving disputes under the Data Act?

The Data Act provides for voluntary dispute resolution through designated settlement bodies in each Member State. These bodies can help resolve disagreements about data access, sharing terms, safety/security concerns, or trade secret protection. Parties must agree in advance if the decision will be binding. If resolution fails or is contested, courts remain available. These mechanisms aim to provide accessible and efficient alternatives to litigation, especially in cross-border or complex data-sharing cases. They support enforcement while maintaining flexibility and fairness in business-to-business and business-to-government data interactions.

Understanding Data Act

Business-to-business and business-to-consumer data sharing in the context of IoT

What are the key goals?

The key goals are to ensure fairness, innovation, and value-sharing in the digital economy. The Data Act empowers users—both businesses and consumers—to access, use, and share the data they co-generate through connected IoT products. It promotes competition by preventing data monopolies, particularly by manufacturers, and enhances transparency in data use. It also supports user autonomy, enabling them to choose service providers, including third parties, and to port their data in real-time.

Why is it needed?

The Data Act is needed to address imbalances in the current data economy, where manufacturers or service providers often hold exclusive control over valuable data generated through IoT devices. Users who help generate this data typically lack access, limiting their ability to derive value or seek competing services. This creates inefficiencies, hinders innovation, and reinforces market dominance. The regulation ensures equitable access and encourages new business models and services.

How does it work?

In practice, the Data Act obliges manufacturers and service providers (data holders) to make relevant IoT data available to users, including businesses and consumers, either directly (via built-in access interfaces) or indirectly (upon request). Users can also instruct the data holder to share this data with a third party of their choice. Data covered includes raw and pre-processed operational data, not inferred or highly processed data. Safeguards exist for trade secrets, personal data, and product safety. Contracts and technical means must transparently inform users how to access, use, or transfer their data effectively.

Business-to-business data sharing

What are the key goals?

The key goals are to create a fair, transparent, and balanced framework for business-to-business (B2B) data sharing, especially where data sharing is legally required. The Data Act ensures that when a business is obliged to share data with another, this occurs under fair, reasonable, and non-discriminatory (FRAND) conditions. It seeks to prevent power imbalances—particularly where dominant players impose unfair terms on smaller entities. In setting clear rules on access, compensation, and dispute resolution, the regulation promotes trust.

Why is it needed?

This regulation is needed to address the lack of clarity and imbalance in current B2B data-sharing practices. Often, larger companies unilaterally impose contractual terms or restrict access to valuable data, limiting competition and innovation. Small and medium-sized enterprises (SMEs) are especially vulnerable. The Data Act ensures that where data sharing is mandatory—whether by sectoral legislation or under the Act itself—it takes place on terms that are equitable and legally sound.

How does it work?

When a business is legally required to share data with another, the Data Act requires that this be done under FRAND terms. The data holder must provide the data in a transparent and accessible manner, with compensation based on objective criteria (e.g., cost of sharing), particularly benefiting SMEs. Dispute resolution bodies can intervene if parties disagree on terms. The Act prohibits discriminatory practices and unfair contract clauses, and limits the use of shared data to agreed purposes.

Unfair contractual terms

What are the key goals?

The primary goal is to protect businesses—especially SMEs—from being subjected to unfair contractual terms in data-sharing agreements, particularly when terms are imposed unilaterally by stronger parties. The Data Act ensures that contracts reflect good faith, balance, and transparency in the digital economy. It prevents exploitative practices by prohibiting clauses that deviate grossly from commercial norms.

Why is it needed?

Many SMEs lack bargaining power and legal resources to challenge unfair terms in data-sharing contracts imposed by larger companies. These imbalances can prevent smaller firms from accessing or using data they need to innovate or compete. Without safeguards, dominant players may insert clauses that excessively limit liability, restrict use rights, or unilaterally change terms. The Data Act addresses this by defining and prohibiting unfair terms, creating legal certainty and redress options.

How does it work?

Under the Data Act, any contractual term that is unilaterally imposed and grossly deviates from good commercial practice may be deemed unfair and unenforceable. Examples include clauses that exclude liability for breach, permit unilateral contract changes, or excessively limit data use. A list of such terms—either automatically unfair or presumed unfair—is provided in the Act. If a business finds such a clause in a contract, it can seek redress through courts or designated authorities. The rest of the contract remains valid if the unfair term can be separated, ensuring legal protection for businesses.

Business-to-government data sharing

What are the key goals?

The key goal of B2G data sharing under the Data Act is to empower public sector bodies to make timely, evidence-based decisions in situations of exceptional need. By enabling targeted access to data held by private companies—particularly during public emergencies or for specific public interest tasks—the Act enhances governmental responsiveness and policy effectiveness. It ensures such access is justified, proportionate, and transparent, while protecting trade secrets and personal data.

Why is it needed?

Public authorities often lack access to critical real-time data during emergencies or for essential public services, even when such data exists within the private sector. This gap can delay responses to crises like natural disasters or pandemics. The Data Act addresses this by creating a legal pathway for public bodies to request data in defined exceptional situations. It ensures that such access is not misused and comes with proper safeguards. Ultimately, it bridges the information divide between public need and private data resources.

How does it work?

When an exceptional need arises—such as a public emergency or a legally defined public interest task—public sector bodies may request access to specific non-personal data from private companies. The request must be proportionate, justified, and clearly outline the data needed, purpose, duration, and involved entities. Data holders can verify the request and may refuse it if legal criteria are not met. Shared data remains restricted to the original purpose and is not made public. Trade secrets and personal data are protected, and any onward sharing is tightly controlled.

Switching between data processing services

What are the key goals?

The primary goal is to make switching between cloud and edge computing services easier, faster, and less costly. The Data Act sets rules to prevent vendor lock-in, ensure service portability, and foster competition in the digital infrastructure market. It empowers customers to move their data, applications, and digital assets between providers seamlessly. As a result of requiring providers to support interoperability and reduce switching barriers, the Act promotes innovation, enhances user choice, and strengthens digital sovereignty.

Why is it needed?

Currently, many cloud and edge service providers use proprietary technologies and restrictive practices that hinder interoperability and make switching difficult, time-consuming, or expensive. This creates vendor lock-in and limits user choice, innovation, and market competition. The Data Act addresses this by mandating technical and contractual measures to facilitate switching and prevent dependency on a single provider. It is especially important for SMEs and public bodies, who often lack the leverage to negotiate better terms.

How does it work?

Under the Data Act, cloud and edge providers must ensure that customers can switch to another provider—or to on-premises systems—within defined notice and transition periods. Providers must offer exportable data in a structured, machine-readable format and support the transfer of digital assets like configurations and access rights. Switching fees are gradually eliminated: from 2024, they must reflect actual costs, and from 2027, they are prohibited entirely. Providers must also ensure interoperability through open interfaces.

Unlawful third country government access to data

What are the key goals?

The key goal is to ensure that non-personal data stored in the EU is protected from unlawful or disproportionate access by third-country authorities. This provision upholds EU sovereignty, legal certainty for businesses, and trust in the European data economy. In requiring that foreign access requests comply with international agreements or EU/national law, the Data Act seeks to prevent extraterritorial overreach and reinforces the EU's commitment to safeguarding data from unauthorized or politically motivated surveillance.

Why is it needed?

This protection is needed to address growing concerns over foreign surveillance and extraterritorial laws that may force EU-based data holders or processors to unlawfully disclose data. Without these safeguards, businesses risk violating EU laws, undermining customer trust, and facing conflicting legal obligations. In sectors like cloud computing and industrial IoT, where vast volumes of sensitive non-personal data are stored and processed, the risk of foreign overreach is high. The provision helps reinforce legal clarity and assures that only legitimate, proportionate, and legally justified access to data is permitted under EU rules.

How does it work?

In practice, a data holder or processor in the EU must verify the legal basis of any third-country government request for access to non-personal data. Access is only allowed if based on an international agreement (e.g. mutual legal assistance treaties) or if the request is deemed lawful, necessary, proportionate, and subject to oversight under EU or Member State law. If the request does not meet these criteria, the data holder must reject it and inform the requesting authority accordingly. Competent national authorities may also be consulted, and legal remedies are available to challenge unlawful disclosures.

Interoperability

What are the key goals?

The primary goal is to ensure seamless interoperability between data spaces and data processing services across the EU. This allows data to flow efficiently and securely between different systems, platforms, and sectors. By harmonizing technical standards, the Data Act supports innovation, competition, and cross-border data use. It also aims to avoid vendor lock-in, simplify switching between cloud providers, and foster a more open, interconnected European data economy.

Why is it needed?

Interoperability is essential for realizing the EU's vision of a functioning single market for data. Without it, data remains siloed, fragmented, or tied to specific providers, limiting its value and usability. Businesses, public bodies, and researchers need a trusted environment where data can be shared, combined, and reused regardless of the underlying system or service provider. Ensuring interoperability reduces technical and contractual barriers, supports digital sovereignty, and enables fair competition — especially in cloud computing and emerging data spaces like health, mobility, and energy.

How does it work?

The Data Act mandates that data processing service providers — including cloud platforms — implement open interfaces, use standardized formats, and enable smooth data portability and switching. The European Commission will establish a common EU repository listing harmonized standards and technical specifications to guide these requirements. Participants in data spaces must comply with these interoperability rules to ensure compatibility across systems. This includes obligations to make exportable data and digital assets accessible in a structured, machine-readable way, enabling users to switch providers or integrate services without disruption.

Enforcement

What are the key goals?

The goal is to ensure consistent, effective enforcement of the Data Act across all Member States. By requiring the designation of competent authorities and a national data coordinator, the Act aims to provide clear accountability, streamline oversight, and facilitate cooperation within the EU. These structures help resolve disputes, monitor compliance, and protect users' and data holders' rights. The enforcement mechanism ensures the Data Act's provisions are applied uniformly, giving businesses and users confidence that their obligations and rights are upheld regardless of where they operate within the EU.

Why is it needed?

Effective enforcement is essential to ensure the Data Act functions in practice. Without clear national authorities responsible for oversight, there's a risk of fragmented implementation, regulatory confusion, and uneven protection across the EU. Appointing a single point of contact — the data coordinator — simplifies communication for citizens, businesses, and EU institutions. It also ensures better coordination between different national regulators, especially in cases involving cross-border data use, trade secret protection, or unlawful data access.

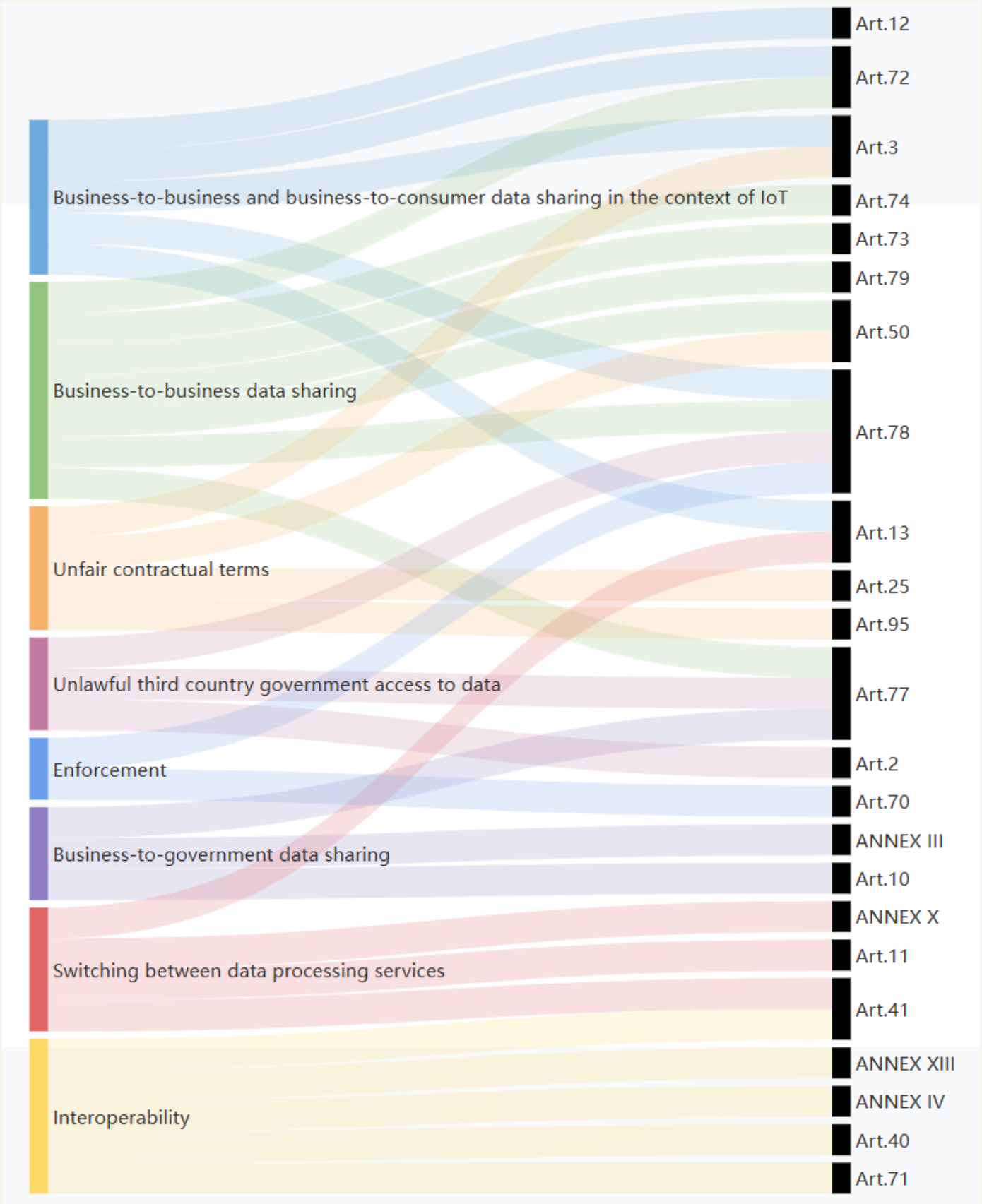
How does it work?

Each Member State must designate one or more authorities to enforce the Data Act's provisions. If multiple bodies are involved (e.g. sectoral regulators, consumer agencies, data protection authorities), a central data coordinator must be appointed to act as the single national contact point. This coordinator ensures efficient cooperation between enforcement bodies and facilitates EU-level coordination via the European Data Innovation Board. Users and businesses can contact the coordinator with questions, complaints, or compliance issues. Enforcement includes handling trade secret disputes, unfair contract terms, and cross-border data access concerns.

Mapping Data Act to EU AI Act

Data Act

EU AI Act



Data Act		EU AI Act		
Section	Description	Article(s)	Explanation	Action
Business-to-business and business-to-consumer data sharing in the context of IoT	Users of IoT objects can access, use and port data that they co-generate through their use of a connected product.	3, 78, 72, 13, 12	**Definitions and Scope:** • The Act defines an "AI system" as a machine-based system designed to operate with varying levels of autonomy and generate outputs such as predictions or decisions that can influence environments. This broad definition can encompass AI systems used in IoT devices. **High-Risk AI Systems:** • The Act outlines obligations for providers and deployers of high-risk AI systems, which may include IoT devices if they are classified as high-risk. These obligations include ensuring transparency, providing instructions for use, and maintaining records. **Transparency and Information Provision:** • High-risk AI systems must be designed to ensure transparency, enabling users to interpret and use the system's output appropriately. This includes providing clear instructions and information about the system's capabilities and limitations. **Data Access and Portability:**	**Enable User Data Access and Portability for IoT-based AI Systems** Ensure users of AI-enabled IoT products can access, use, and port the data they co-generate. Implement user dashboards, APIs, or direct access mechanisms to meet transparency and data rights obligations, especially when training or fine-tuning AI systems using IoT data inputs.

			• While the Act does not explicitly address data portability in the context of IoT, it emphasizes the importance of transparency and the provision of information, which can facilitate data access and understanding for users. **Post-Market Monitoring:** • Providers are required to establish a post-market monitoring system to collect and analyze data on the performance of high-risk AI systems, which could include IoT devices. This system helps ensure ongoing compliance and safety. **Confidentiality and Data Protection:** • The Act includes provisions to protect the confidentiality of information and data obtained during compliance activities, which is relevant for data sharing and protection in IoT contexts.	
Business-to-business data sharing	This clarifies the data-sharing conditions wherever a business is obliged by law, including through the Data Act, to share data with another business.	77, 78, 74, 50, 73, 72, 79	**Confidentiality and Data Protection:** • The EU AI Act emphasizes the importance of confidentiality in data handling. It outlines that any information or data obtained during compliance activities must be	**Review and Structure B2B Data Sharing Agreements** When legally required to share data with another business, define access conditions, purpose limitations, and technical

			treated with confidentiality, protecting intellectual property rights and trade secrets. This is crucial in business-to-business data sharing to ensure sensitive information is safeguarded. **Transparency Obligations:** • The Act mandates transparency obligations for providers and deployers of certain AI systems, ensuring that users are informed about the AI system's operations. This transparency can facilitate understanding and compliance in data-sharing scenarios. **Post-Market Monitoring and Information Sharing:** • The Act discusses post-market monitoring and the sharing of information on serious incidents. These provisions require providers to establish systems for monitoring AI systems and sharing relevant data with authorities, which can overlap with data-sharing obligations between businesses. **Market Surveillance and Control:** • The Act details the role of market surveillance authorities in monitoring AI	safeguards—especially if AI systems rely on or process the shared data. This avoids regulatory risk and supports lawful AI model development and service delivery.

			systems, ensuring compliance with regulations. This includes the ability to access necessary documentation and data, which is relevant for businesses required to share data under legal obligations. **Enforcement and Compliance:** • The Act provides enforcement mechanisms for ensuring compliance with the AI Act, including the ability of authorities to request documentation and organize testing of AI systems. This enforcement framework supports the legal obligations of businesses to share data.	
Unfair contractual terms	These provisions protect all businesses, in particular SMEs, against unfair contractual terms imposed on them.	3, 25, 50, 95	**Responsibilities Along the AI Value Chain:** • The Act outlines the responsibilities of providers and third parties involved in high-risk AI systems. It emphasizes the need for written agreements specifying necessary information, capabilities, and technical access to ensure compliance with the regulation. This provision indirectly supports fair contractual terms by requiring clarity and mutual understanding in agreements. **Transparency Obligations:**	**Audit Contracts for Fairness in AI Training and Data Use** Review AI-related data sharing and licensing agreements—especially with SMEs—to ensure terms are not unilaterally imposed or grossly imbalanced. Use the Commission's model clauses to avoid unfair practices and support fair AI innovation ecosystems.

			• The Act mandates transparency obligations for providers and deployers of certain AI systems, ensuring that users are informed about the AI system's operations. This transparency can help prevent unfair contractual terms by ensuring that all parties have a clear understanding of the AI system's capabilities and limitations. **Market Surveillance and Control:** • The Act details the role of market surveillance authorities in monitoring AI systems, ensuring compliance with regulations. This oversight can help identify and address unfair contractual terms that may arise in the deployment of AI systems. **Enforcement and Compliance:** • The Act provides enforcement mechanisms for ensuring compliance with the AI Act, including the ability of authorities to request documentation and organize testing of AI systems. These mechanisms can be used to address unfair contractual terms by ensuring that all parties	

			adhere to the agreed terms and conditions. **Codes of Conduct:** • The Act encourages the development of codes of conduct to foster the voluntary application of specific requirements to AI systems. These codes can include provisions to protect businesses from unfair contractual terms by promoting best practices and ethical guidelines.	
Business-to-government data sharing	Public sector bodies will be able to make more evidence-based decisions in certain situations of exceptional need through measures to access certain data held by the private sector.	ANNEX III, 10, 77	**Data Access and Sharing:** • The EU AI Act does not explicitly detail provisions for business-to-government data sharing. However, it emphasizes the importance of data governance and management practices, particularly for high-risk AI systems, which could indirectly support data sharing by ensuring data quality and compliance. **High-Risk AI Systems and Public Sector Use:** • High-risk AI systems, as defined in the Act, include those used by public authorities for essential services and benefits, which may require data from private entities to function effectively. This implies a framework	**Prepare for Public Sector AI Data Requests** Put in place internal procedures to respond to public sector data requests for AI-related insights, particularly during emergencies or for official statistics. Ensure legal review, documentation, and clarity on data scope and use, especially when data is used to train or validate public sector AI models.

			where data sharing could be necessary for public sector decision-making. **Market Surveillance and Compliance:** • The Act grants national public authorities the power to request and access documentation necessary for fulfilling their mandates, which could include data from private entities if it pertains to high-risk AI systems. This provision supports the idea of accessing private sector data for public interest. **Post-Market Monitoring and Information Sharing:** • The Act requires providers of high-risk AI systems to establish post-market monitoring systems, which involve collecting and analyzing data on system performance. This data could be shared with public authorities to aid in decision-making. **Confidentiality and Data Protection:** • The Act ensures that any information or data obtained during compliance activities is treated with confidentiality, protecting sensitive business information while allowing necessary	

			data access for public sector needs.	
Switching between data processing services	Providers of cloud and edge computing services must meet minimum requirements to facilitate interoperability and enable switching.	ANNEX X, 11, 13, 41	**Interoperability Framework:** • The EU AI Act emphasizes the importance of interoperability, particularly in the context of large-scale IT systems in the area of freedom, security, and justice. While this primarily pertains to public sector systems, the principles of interoperability can be extended to cloud and edge computing services to ensure seamless data exchange and service switching. **Technical Documentation and Compliance:** • The Act requires that high-risk AI systems have comprehensive technical documentation to demonstrate compliance with the Act's requirements. This documentation must be clear and comprehensive, facilitating interoperability by providing necessary information to assess compliance. This principle can be applied to cloud and edge computing services to ensure they meet interoperability standards. **Standards and Conformity Assessment:** • The Act discusses the establishment	**Ensure Cloud Portability for AI Training and Inference Workloads** Implement open standards and data export tools to allow customers to switch AI workloads between cloud and edge environments. This includes migrating AI models, metadata, training datasets, and APIs to avoid vendor lock-in and comply with the Data Act's switching obligations.

			of common specifications and standards to ensure compliance with the Act's requirements. These standards can include interoperability requirements for cloud and edge computing services, ensuring they can switch between different service providers without significant barriers. **Transparency and Information Provision:** • The Act mandates transparency in high-risk AI systems, requiring clear instructions and information for deployers. This transparency can support interoperability by ensuring that users have the necessary information to switch between different data processing services.	
Unlawful third country government access to data	Non-personal data stored in the EU is protected against unlawful foreign government access requests.	2, 77, 78	**Confidentiality and Data Protection:** • The Act emphasizes the confidentiality of information and data obtained during the application of the regulation. It specifically protects intellectual property rights, confidential business information, and trade secrets, which can include non-personal data. This provision indirectly supports the protection against	**Implement Legal Review for Foreign Government Data Requests** Develop internal protocols to assess the legality of foreign access requests for non-personal data used in AI systems. Reject any unlawful or extraterritorial demands unless aligned with EU or international law, and document all such interactions

			unlawful access by foreign governments by ensuring that data is handled with strict confidentiality. **Scope and Applicability:** • The Act outlines the scope of the regulation, which applies to providers and deployers of AI systems within the EU, as well as those outside the EU whose systems are used within the Union. This broad scope ensures that data protection measures apply to all relevant entities, potentially limiting unlawful access by third-country governments. **Market Surveillance and Compliance:** • The Act grants national public authorities the power to request and access documentation necessary for fulfilling their mandates, ensuring compliance with the regulation. This oversight can help prevent unlawful access to data by ensuring that all entities comply with EU data protection standards. **International Cooperation and Agreements:** • The regulation acknowledges the possibility of exchanging confidential information with	to ensure compliance.

			regulatory authorities of third countries, provided there are adequate confidentiality arrangements in place. This ensures that any data sharing with foreign governments is conducted under strict conditions that protect against unlawful access.	
Interoperability	Participants in data spaces must fulfil criteria to allow data to flow within and between data spaces. An EU repository will lay down relevant standards and specifications for cloud interoperability.	ANNEX XIII, ANNEX IV, 40, 71, 41	**Interoperability Framework:** • The EU AI Act emphasizes the importance of interoperability, particularly in the context of large-scale IT systems. While the Act itself does not explicitly detail interoperability for data spaces, the principles of interoperability are crucial for ensuring seamless data exchange and service switching. **Standards and Conformity Assessment:** • The Act discusses harmonized standards and standardization deliverables, which are essential for ensuring interoperability. These standards help ensure that AI systems, including those used in cloud services, meet the necessary requirements for interoperability. **Common Specifications:** • The Act allows the Commission to	**Implement Legal Review for Foreign Government Data Requests** Develop internal protocols to assess the legality of foreign access requests for non-personal data used in AI systems. Reject any unlawful or extraterritorial demands unless aligned with EU or international law, and document all such interactions to ensure compliance.

			adopt implementing acts establishing common specifications for requirements, which can include interoperability standards for cloud services. These specifications ensure that systems can work together seamlessly across different platforms and services. **Technical Documentation:** • The Act requires detailed technical documentation for AI systems, which includes information on how the system interacts with other hardware or software. This documentation supports interoperability by providing necessary details for integration and compatibility. **EU Database for High-Risk AI Systems:** • The Act establishes an EU database for high-risk AI systems, which can include information on standards and specifications relevant to interoperability. This database serves as a repository for ensuring that systems comply with interoperability requirements.	
Enforcement	Member States must designate one or more competent	70, 78	**Designation of National Competent Authorities:**	**Appoint an Internal EU Data Coordinator Role**

	authority(ies) to monitor and enforce the Data Act. Where more than one authority is designated, a 'data coordinator' must be appointed to act as the single point of contact at the national level.		• The Act requires each Member State to establish or designate at least one national competent authority, including a notifying authority and a market surveillance authority, to ensure the application and implementation of the regulation. These authorities must operate independently and impartially. **Single Point of Contact:** • The same article mandates that Member States designate a market surveillance authority to act as the single point of contact for the regulation. This authority's identity must be communicated to the Commission, which will make a list of these single points of contact publicly available. **Coordination and Resources:** • Member States are required to ensure that their national competent authorities are provided with adequate resources, including technical, financial, and human resources, to effectively fulfill their tasks. This includes having personnel with expertise in AI technologies, data	Designate a compliance lead to liaise with national authorities on Data Act matters, especially where AI systems are developed or deployed across jurisdictions. This supports coherent enforcement, streamlines regulatory engagement, and aligns with EU AI governance expectations under the AI Act.

			protection, and cybersecurity. **Confidentiality and Cooperation:** • The Act emphasizes the confidentiality of information obtained during compliance activities, ensuring that sensitive data is protected while allowing necessary cooperation between authorities.	

Calls to action

Establish Internal Data Reuse Protocols for Public Sector Sources

Develop and formalize procedures for identifying, requesting, and reusing public sector datasets in accordance with the DGA's access and reuse conditions. Ensure alignment with the AI Act by integrating checks for dataset provenance, relevance to intended AI use cases, and compatibility with high-risk AI transparency requirements.

Incorporate Legal and Ethical Vetting into Dataset Onboarding

Before incorporating public sector data into AI training pipelines, conduct a structured vetting process to verify legal permissibility, data quality, and documentation completeness. Cross-reference this process with the AI Act's Article 10 obligations on data governance, traceability, and minimization of bias.

Use the European Single Access Point (ESAP) and National Portals

Leverage trusted data sources such as the ESAP or Member State open data platforms to access reusable public sector data under DGA terms. Prioritize datasets that come with metadata, usage conditions, and licensing clarity to simplify downstream compliance with AI Act auditability and documentation requirements.

Train AI Teams on Reuse-Ready Data Stewardship

Provide cross-functional training for data scientists, compliance officers, and developers on how to responsibly source and integrate protected public sector data. Embed DGA reuse criteria and AI Act data management standards into your organization's model development lifecycle and documentation frameworks.

Conclusion

The convergence of the Data Act and the EU Artificial Intelligence Act represents a transformative evolution in Europe's approach to governing data and AI. Together, these regulatory frameworks establish a unified, innovation-enabling model—anchored in fairness, legal clarity, and fundamental rights. They promote an ecosystem where AI development is underpinned by equitable data access, robust safeguards, and accountability across the digital value chain.

This mapping document illustrates how the Data Act and the AI Act operate in tandem: while the Data Act empowers users and businesses to access and share IoT-generated and industrial data under fair and transparent conditions, the AI Act sets out risk-based obligations for the development and deployment of trustworthy AI systems. From data portability and interoperability to contractual fairness and public sector access, the synergies between the two acts are foundational to responsible AI lifecycle management.

Yet, unlocking the full potential of this alignment requires more than legal awareness—it demands proactive implementation. Organizations must operationalize their data-sharing rights and responsibilities, embed compliance across AI development pipelines, and build internal processes to support transparency, switching, and lawful data use. For startups, SMEs, and public institutions alike, success will depend on early engagement with technical standards, regulatory guidance, and sector-specific best practices.

Leading actors across Europe are already showing how integration of Data Act principles into AI workflows can reduce friction, support compliance, and enhance public trust. In doing so, they are laying the groundwork for a data economy—and an AI ecosystem—that is resilient, competitive, and fundamentally aligned with Europe's democratic values. Together, the Data Act and the AI Act form the regulatory architecture for a digital future that is open, interoperable, and people-centered.

About AI & Partners

AI & Partners

Amsterdam - London - Singapore

AI & Partners – 'AI That You Can Trust'

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

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

Contacts

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

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

Authors

Sean Donald John Musch, CEO/Founder

Michael Charles Borrelli, Director

References

European Parliament and The Council of the European Union, (2023), Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act) (Text with EEA relevance), accessible at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023R2854&qid=1747514874846 (last accessed 17th May 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 17th 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.

Designed and produced by AI & Partners B.V