



# GDA SUBMISSION ON THE EUROPEAN DATA UNION STRATEGY

## *Response to the European Commission's Call for Evidence and Public Consultation*

17 July 2025

The Global Data Alliance<sup>1</sup> (GDA) is a cross-industry coalition of companies that are committed to high standards of data responsibility and that rely on the ability to transfer data around the world to innovate and create jobs. The GDA supports policies that help instill trust in the digital economy while safeguarding the ability to transfer data across borders and refraining from imposing data localization requirements that restrict trade. The GDA's members are headquartered across the globe, including the European Union, and are active in advanced manufacturing, aerospace, automotive, consumer goods, electronics, energy, financial services, health, supply chain, and telecommunications sectors, among others.

The GDA welcomes this opportunity to provide [input for the future](#) European Data Union Strategy. We support the European Commission's objectives to promote secure, responsible, and innovation-friendly data sharing, enhance international data flows, and reduce administrative burdens.

In this submission, the GDA develops three recommendations to the European Commission, with a particular focus on international data transfers.

### **Boosting EU competitiveness through smarter data policies to scale-up data use and availability.**

***The GDA encourages the European Commission to promote policies that facilitate data sharing, improve access to high-value data, and support innovation and digital services. Forward-thinking digital policy must enable the free and responsible flow of data, which empowers job creation, economic competitiveness, and innovation across [all sectors](#). The EU recognizes that global services rely on seamless cross-border data flows, which positively impact the EU economy and contribute to digital trade between the EU and third countries.***

---

<sup>1</sup> For more information on the Global Data Alliance, please see: <https://www.globaldataalliance.org/>. Business Software Alliance administers the Global Data Alliance; *EU Register of Interest Representatives*: 75039383277-48

The cornerstone of EU data protection legislation, the **General Data Protection Regulation (GDPR)**, is designed to ensure a high level of protection while facilitating the free movement of personal data. As the EU strives to establish its standard for personal data as a global benchmark, it must also promote the best international practices that support a risk-based approach and the interoperability of privacy systems. To improve the use of personal data, the European Commission should:

- **Strengthen the international data transfer toolbox** to support global data flows by ensuring that businesses can rely on the full range of existing GDPR-compliant mechanisms, including adequacy decisions (such as the EU-US Data Privacy Framework), certifications, codes of conduct, Binding Corporate Rules, and Standard Contractual Clauses.
- **Reduce fragmentation among Member States** by addressing diverging – and at times conflicting – interpretations by national data protection authorities.
- **Ensure consistency and coherence between the GDPR and other EU data-related legislation** to foster innovation and the development of new technologies. This includes clarifying the interplay between the GDPR and the Data Act, particularly in relation to the GDPR’s principles-based approach to issues such as personal data, data minimisation, anonymisation, proportionality, and consent.

At the same time, to facilitate personal data transfers under the current EU *acquis*, the GDA encourages European policymakers to enhance legal clarity when **evaluating the legal system of third countries**. Currently, data exporters and importers are required to conduct a detailed assessment of the legal framework in the recipient country – a responsibility that, in practice, falls on private companies. Many lack the resources or expertise to evaluate foreign legal systems comprehensively.

- The EU should therefore **develop tools to support businesses by reducing the complexity and burden of assessing third-country legal systems**.

The GDA supports policies that build trust in the digital economy while ensuring the transfer of data across borders. This means avoiding the imposition of **data localization** requirements, which can hinder the free flow of data. Contrary to common beliefs, data localization does not enhance data protection, security measures do. Whether it pertains to privacy legislation, health data spaces, certification schemes, or rules for non-personal data transfers, data localization risks undermining the objectives of European data laws.

**Regarding non-personal data**, it is important to remove any ambiguous data use provisions under current legislative framework. Namely, Article 32 of the **EU Data Act** introduces vague and potentially far-reaching restrictions on international transfers of non-personal data, raising serious concerns for legal clarity, innovation, and Europe’s global competitiveness. Unlike personal data, non-personal data is generally low-risk and not protected under the Charter of Fundamental Rights of the EU. Measures of Article 32 risk creating *de facto* data localization requirements, which could conflict with the EU’s international trade obligations and hamper the ability of EU businesses to access state-of-the-art cross-border technologies. This is particularly challenging for companies handling mixed data sets (personal and non-personal) and creates administrative burdens that are not commensurate with the risks presented. Therefore, while the European Commission’s interpretation – that Article 32 does not cover international data transfers between businesses

or within organisations<sup>2</sup> – is helpful, the Article itself must be clarified to ensure that it applies only to foreign government access requests for client data held by cloud service providers, and that non-personal data can move freely across borders.

- The Data Act – just as any other current and future legislative and non-legislative initiative – should promote – not hinder – **collaborative innovation** by aligning with Europe’s free flow of data framework and trade commitments, and by **eliminating any unjustified restrictions on non-personal data transfers**.
- **The EU should not aim to mirror the GDPR’s approach to international personal data transfers (based on essential equivalence) and apply it to non-personal data.** Introducing additional requirements for the transfer of non-personal data would inevitably reduce companies’ ability to move data in and out of the EU, which would go against the competitiveness agenda of the European Commission.

**Sector-specific data sharing frameworks**, such as the European Health Data Space (EHDS), are designed to reflect the unique needs, risks, and regulatory contexts of their sectors. The EHDS, for example, supports secure and privacy-compliant health data use by addressing clinical and safety considerations – nuance that horizontal instruments like the Data Act cannot offer.

To ensure legal clarity and prevent conflicting obligations, sectoral regimes should take precedence where they exist. Extending generic data access rights – such as mandatory sharing of raw, pre-processed, or uninterpreted data – to sensitive domains like healthcare risks undermining data integrity, safety, and trust, particularly where improper use could result in clinical misinterpretation or compromised device performance. Prioritising sector-specific legislation allows for responsible data sharing while preserving critical safeguards.

- The EU Data Union Strategy should therefore **establish a clear legal hierarchy that gives precedence to sector-specific frameworks** – such as the EHDS – over the horizontal provisions of the Data Act, ensuring that data access obligations do not override tailored protections.

Data – both personal and non-personal – is foundational to **digital transformation**. The GDA supports policies that incentivize voluntary **data sharing**, particularly through greater publication of open government data and open research and scientific datasets. Broader **data availability** is essential. In particular, Europe’s AI ecosystem will benefit significantly from improved access to multilingual, sector-specific, and industrial datasets. Beyond data scarcity, the Data Union Strategy should also aim to address **data quality issues**. Standardized data formats and interoperability would play a key role in enhancing data quality across the board. Data catalogues, data models and data access protocols should be prioritized to boost data sharing in the EU.

---

<sup>2</sup> Data Act, Frequently Asked Questions (FAQs), Point 61, [FAQs\\_Data\\_Act\\_lvzHhIWD6898kQriOIh8SMbPco4\\_108144.pdf](#)

Importantly, it is critical to ensure that **national application of various data laws** (the GDPR, Data Governance Act, Data Act and many others), is **fully harmonized**, avoiding divergence between the EU Member States that would fragment the internal market.

- The EU Data Union Strategy should therefore **ensure full harmonization of the national application of EU data laws** to prevent internal market fragmentation.

### **Advancing strategic autonomy through international cooperation, not protectionism.**

*The GDA encourages the European Commission to continue advancing an open, trusted global digital economy by advancing interoperable, risk-based governance frameworks that reflect EU values. We urge caution against restrictive data sovereignty measures that could hinder innovation and competitiveness. International cooperation and trust-based mechanisms are essential to facilitate secure cross-border data flows and reinforce Europe’s leadership in the global digital landscape.*

The EU is a global leader in advancing data policies, enabling cross-border data flows, building digital partnerships, and promoting free and open trade. The EU has also been the world’s largest exporter and importer of digitally deliverable services for the past decade. Digitally deliverable services support tens of millions of jobs within the EU and account for a significant portion of both outbound and inbound foreign direct investment. The EU’s trade strategy has rightfully recognized that “data are the lifeline of many businesses and a critical component of the EU’s supply chains.”

**All businesses – including those operating and headquartered in the European Union – rely on seamless cross-border data flows.** Free flow of data is crucial for a thriving data economy, enabling innovation, economic growth, and societal benefits by facilitating the movement of non-personal data across borders. The data flows foster digital transformation, enhance competitiveness, and allow businesses to create new services and models, while also supporting public authorities in their regulatory functions. The GDA, therefore, advocates for policies that enable the free flow of data, which directly supports job creation, economic competitiveness, and innovation across all sectors.

At the same time, the GDA relates to the **EU’s goal of reducing dependencies**. While we support the EU’s aim to increase open strategic autonomy in the digital sector, we caution against sovereignty requirements that lean toward **isolationism or protectionism**. If endorsed, these requirements would negatively affect not only European companies offering digital services – such as cloud computing or AI solutions – globally, but also the customers and users of many global digital services. This includes private companies, public organizations, and citizens who rely on the ability to assess, compare, and choose the best available service providers. Users should be able to make these choices based on performance-driven criteria such as cybersecurity assurances, data confidentiality standards, capacity for innovation, potential for digital transformation, and other indicators of technical excellence. Merely protectionist criteria should not be impeding these choices.

Overly rigid and exclusive requirements – such as **corporate ownership requirements, strict barriers to the international movement of data and information, and mandates for immunity from foreign legal**

**jurisdiction** – would undermine innovation, restrict user choice and weaken EU completeness. They would disproportionately harm European companies that have global supply chains and depend on competitive global services to develop or sell their products or services. Moreover, protectionist measures would exacerbate disparities among EU Member States by favoring those with more advanced technological infrastructures and placing undue pressure on less developed national ecosystems.

**Strategic autonomy should empower – not restrict – European actors.** By fostering a trusted, open, and globally connected digital environment, the EU can remain at the forefront of digital innovation while upholding its core values and reinforcing its economic resilience. We advocate for a risk-based framework anchored in interoperability, voluntary certification schemes, and robust technical safeguards, such as confidential computing, encryption, privacy-enhancing technologies, and privacy-preserving machine learning.

As the European Commission aims to secure Free Trade Agreements with a range of countries in the coming months (India, Indonesia, Australia, etc.), it should negotiate ambitious Digital Trade Chapters that remove barriers to cross-border data flows. Digital trade provisions should hold free and trusted cross-border data flows at their center.

The GDA urges the European Commission to ensure that the pursuit of strategic autonomy is not conflated with protectionism, but remains firmly grounded in **openness, international cooperation, and global engagement**. This is essential not only to protect Europe’s economic competitiveness, but also to demonstrate global leadership in building a secure, rights-respecting, and innovation-driven digital ecosystem. By taking this approach, the EU can lead by example – showing that strategic autonomy and global integration are mutually reinforcing pillars of long-term digital success.

## **Simplifying EU Data Regulation to Support Cross-Border Data Flows.**

***The GDA urges the European Commission to simplify the EU’s data regulatory landscape to support innovation and the trusted flow of data across borders. In line with the EU’s simplification agenda, we advocate for streamlined rules, reduced compliance obligations, and clearer guidance on how data laws interact.***

Aligning frameworks such as the GDPR, Data Governance Act, Data Act, Free Flow of Non-Personal Data Regulation, and Open Data Directive will ease cross-border operations, reduce legal complexity, and enhance digital innovation. A more coherent and innovation-friendly regulatory environment is essential for maintaining Europe’s competitiveness and global leadership in data governance.

**In that context, the GDA proposes the following recommendations for data related regulation simplification.**

### **1. Ensure Cross-Legislation Consistency**

Data-related legislation often uses **inconsistent terminology** and establishes overlapping rights or obligations without clear reconciliation. This increases compliance costs and creates uncertainty in interpretation.

### The GDA recommends the following:

- **Standardize core definitions** across all digital legislation (e.g., “data controller”, “data holder”, “provider”, “gatekeeper”, “user”, “significant/severe incidents”) by establishing a shared digital lexicon.
- **Develop horizontal implementation guidance, involving industry representatives**, to clarify how different laws (e.g., GDPR and Data Act) interact in practical scenarios involving personal data, mixed data sets, AI models, or cloud infrastructure with the goal to ensure uniform interpretation and application of existing laws.
- **Establish an inter-agency coordination taskforce** involving relevant DGs (such as, DG CONNECT, DG JUST, DG COMP, DG FISMA), and agencies or supervisory bodies (such as, ENISA, EDPS, EDPB) to ensure legal coherence from draft to enforcement, including guidance to national authorities.
- **Facilitate a “legislation interoperation” review process** where proposed laws are assessed for conflicts or duplication with existing frameworks.
- **Conduct a Dedicated Analysis of Regulatory Governance** through a targeted analysis to avoid the creation of redundant or overlapping regulatory governance structures. This will help streamline enforcement and implementation for both regulators and companies.
- **Carry out a detailed assessment of the appropriate timing for new legislation to enter into force.** This should ensure that companies have sufficient time to adapt and that any necessary secondary laws or standards are adopted beforehand to support effective implementation.

## 2. Reduce Overlaps and Compliance Duplication

Companies – especially those providing cross-border, business-facing software and services – are increasingly subject to **multiple, overlapping compliance obligations** from different legislative instruments.

### The GDA recommends the following:

- **Map, consolidate and harmonize reporting requirements** under GDPR and other EU laws into a unified incident notification procedure, supported by one harmonized template for incident notification and a harmonized reporting timeline.
- **Establish an EU-wide one-stop-shop allowing businesses to address** overlapping digital obligations, particularly for common requirements like transparency, documentation, and audits.
- **Streamline obligations on access to data**, where the GDPR and Data Act both impose rights and responsibilities, at the risk of diverging double compliance on hybrid datasets, and where legal uncertainty durably affects business models.
- **Streamline international data transfer obligations across GDPR, Data Act and Data Governance Act.** The Data Act and the Data Governance Act (DGA) should be updated to reflect that where a

provider's systems store personal data, any valid transfer mechanism under GDPR should suffice for compliance, without the duplication of obligations under the Data Act and the DGA.

- **Clarifying when and how risk-based approaches should apply** to ensure consistent thresholds and obligations.
- **Establish a legal obligation for all digital regulators to pursue compromise solutions** when making decisions in areas that overlap with other digital legislation. This would reflect the principle of sincere cooperation as enshrined in Article 4(3) of the Treaty on European Union (TEU).
- **Promote Harmonized Decision-Making Across the EU** through statutory duties on all digital regulators to aim – where relevant and proportionate – for a harmonized decision-making practice across the EU. This, too, should align with the principle of sincere cooperation under Article 4(3) TEU.
- **Develop simplified compliance templates**, FAQs, and sector-specific toolkits to help smaller businesses meet obligations cost-effectively.
- **Provide implementing guidance** well ahead of implementation deadlines.
- **Promote voluntary certification mechanisms** as scalable alternatives to prescriptive regulation, especially in the AI and cybersecurity domains.

### 3. Foster a Culture of Co-Regulation, Partnership and Dialogue.

The pace of digital innovation often outstrips the legislative cycle, while enforcement remains siloed across Member States and regulatory domains.

#### The GDA Recommends the following:

- **Scale up regulatory sandboxes** (like those piloted in the AI Act and DGA) to provide safe, flexible environments for testing innovative services under real-world conditions.
- **Create permanent digital regulatory forums** at EU level (modeled after the EU AI Alliance or the Cloud Rulebook initiative) to maintain ongoing dialogue with industry and civil society.
- **Encourage voluntary co-regulatory mechanisms**, where the private sector helps develop implementation standards and codes of conduct under EU oversight.
- **Invest in shared public-private infrastructure**, such as standard APIs, open datasets, and interoperability frameworks, to facilitate seamless compliance and uptake of emerging tech across sectors.
- **Leverage existing international standards in EU cyber certification schemes and elsewhere** to foster global interoperability and reduce unnecessary compliance burdens for businesses. Draft schemes often lacked reference to international standards, such as those developed by ISO/IEC JTC1 SC27 (ISO/IEC 27000 series) and ISO/IEC JTC1 SC38, leading to ambiguous terminology and requirements not grounded in industry best practices and standards.

- **Mandate Stakeholder Consultation Prior to Regulatory Decisions** through a statutory obligation requiring all digital regulators to consult and engage with relevant stakeholders before adopting decisions that affect them. This will ensure that regulators adequately consider the real-world implications.
- **Include SMEs in drafting guidelines** to ensure that they are practical and reflective of the realities faced by small businesses.
- **Require Clear and Practical Regulatory Guidance** that is operational, easy to understand, and pragmatic – enabling effective and consistent implementation by those subject to the rules.

In conclusion, the European Data Union Strategy presents an opportunity to build a globally competitive, secure, and value-driven European data ecosystem. By embracing international cooperation, balanced digital policies, and robust support for digital infrastructure and innovative companies, the EU can drive innovation, economic growth, and digital transformation.

The GDA stands ready to collaborate with the European Commission and stakeholders to realize this vision.

---

For further information, please contact Irma Gudžiūnaitė,  
Director, Policy – EMEA, at [irmag@bsa.org](mailto:irmag@bsa.org).