GDA SUBMISSION ON DIGITAL PACKAGE ON SIMPLIFICATION

Response to the European Commission's Call for Evidence

14 October 2025

The Global Data Alliance[1] (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 European Commission's effort on digital simplification comes at a critical moment. Today, companies face a dense and fragmented web of cross-border digital regulations, including the General Data Protection Regulation (GDPR), the Data Act, the European Health Data Space, and various other digital and sector-specific laws. While each instrument pursues important policy goals, taken together they create overlapping, sometimes inconsistent, and occasionally contradictory obligations. This is particularly challenging for the movement of data across borders and for the management of mixed datasets that include both personal and non-personal data.

For GDA members – who depend on trusted, responsible, and secure data flows across jurisdictions – such complexity creates barriers to delivering benefits to businesses, consumers, and governments. Simplification should therefore aim not only at reducing administrative burden, but also at harmonizing rules across digital legislation and ensuring consistency in how data-related obligations are framed and applied.

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

The GDA welcomes the European Commission's aim to simplify the EU's data regulatory landscape to support innovation. 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

[1] 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*

recognizes that businesses rely on seamless cross-border data flows, which positively impact the EU economy and contribute to digital trade between the EU and third countries. In line with the EU's simplification agenda, we advocate for free and responsible flow of data, 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, as well as the European Health Data Space, 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. Encourage Free and Responsible Flow of Personal and Non-Personal Data.

The ability to move data securely across borders is essential for innovation, competitiveness, and trust in the digital economy. The EU should reinforce existing tools, expand global cooperation, and remove unnecessary restrictions to ensure the free and responsible flow of both personal and non-personal data.

The GDA Recommends the following:

- **Strengthen the International Personal Data Transfer Toolbox** to support global personal 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. Underutilized GDPR transfer tools, such as Codes of Conduct and Certification mechanisms, should be promoted.
- **Adopt and Expand Adequacy Decisions for Personal Data Transfers.** Adequacy findings have the potential to significantly reduce compliance burdens, enhance legal certainty, and foster cross-border digital trade. However, not only is their current scope too limited, but the EU has also only adopted 16 decisions to date. Additionally, the essential equivalence standard, as per the case-law, should not be interpreted narrowly.
- **Provide Clearer Guidance and Practical Tools to Support Transfer Impact Assessments for Third-Country Legal Systems**. To facilitate personal data transfers and ensure greater legal certainty, companies should be supported in third-country legal assessments, which are highly complex and should not fall disproportionately on individual businesses.
- **Embrace a Multilateral, Principle-Based Approach to International Data Transfers Through Existing Global Forums.** By leveraging structured frameworks such as the OECD Privacy Guidelines and the Global CBPR system, the EU can promote interoperable and certifiable mechanisms that ensure strong privacy protections with practical accountability. Active EU participation in these

forums would shape global standards, foster regulatory cooperation, and give businesses reliable tools to support lawful and secure cross-border data flows.

- **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.
- **Do Not Extend GDPR-style Transfer Rules to Non-Personal Data.** The EU should avoid mirroring the GDPR's essential equivalence approach for non-personal data transfers. Such provisions would restrict the free flow of industrial and business data, undermine companies' ability to operate globally, and run counter to the EU's competitiveness agenda.
- **Ensure EU Global Leadership to Counter Data Localization and Protectionist Policies.** The EU should actively engage in bilateral and multilateral dialogues with key economies to promote convergence and mutual recognition of data protection standards, while pushing back against unjustified data localization mandates and other protectionist measures.
- **Clarify Article 32 of the EU Data Act**, which 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. Current provision risks 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.
- **Prioritize Sector-Specific Data Sharing Frameworks**. 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. Where a sectoral regime applies, it takes precedence over the horizontal framework, ensuring that data access obligations do not undermine sector-specific protections.

2. 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.

3. 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.
- **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.

4. 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:

- **Ensure Meaningful Consultation Before Adopting Guidance.** The competent national and European authorities, including EDPB, national DPAs and others, should, in all cases, consult relevant stakeholders and other competent authorities before adopting opinions, guidelines, recommendations, or best practices. A public summary of the consultation, including how feedback was taken into account, should accompany the final instrument.
- **Address Overly Narrow Interpretations of Laws**. Address overly narrow and divergent interpretations by national authorities, for example, Data Protection Authorities on issues such as processing of special category data, requirements for data protection impact assessments, anonymization, and the treatment of IP addresses, to ensure consistent application of the GDPR across the EU.
- **Minimize the Use of Member State Derogation Clauses Under the GDPR.** Divergent national derogations create conflicting rules, raise compliance costs, and increase regulatory burdens, undermining the GDPR's goal of a harmonized framework.
- **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.

- **Include SMEs in drafting guidelines** to ensure that they are practical and reflective of the realities faced by small businesses.
- **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.
- **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.