GDA SUBMISSION ON THE DIGITAL SIMPLIFICATION OMNIBUS TO SUPPORT CROSS-BORDER DATA FLOWS

Response to the European Commission's Proposal

April 2026

The Global Data Alliance (GDA) appreciates the opportunity to submit its recommendations to the co-legislators as they consider the European Commission's proposal on the Digital Simplification Omnibus (Omnibus).

The GDA[1] 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. GDA supports policies that help instil trust in the digital economy while safeguarding the ability to transfer data across borders and refraining from imposing data localization requirements that restrict trade. 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.

GDA welcomes the European Commission's simplification efforts. The Omnibus introduces several positive developments that respond to long-standing industry concerns, including efforts to reduce fragmentation and conflicting requirements, eliminate redundant administrative obligations, and promote a more coherent and streamlined digital framework.

At the same time, **the Omnibus does not yet fully realize its potential to advance one of the central drivers of economic value in the digital economy: cross-border data flows**. While free and responsible data flows underpin job creation, competitiveness, and innovation across sectors – and are widely recognized as essential to the EU economy and digital trade – the proposal, as currently drafted, leaves a number of long-standing challenges related to the movement, use, and governance of data across borders insufficiently addressed.

This submission therefore sets out targeted legislative and non-legislative recommendations to strengthen the Omnibus framework and ensure that simplification translates into greater legal certainty, operability, and trust for cross-border data flows.

---

[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*

1. Legislative Recommendations to Support Cross-Border Data Flows

To ensure that simplification delivers meaningful improvements for cross-border data flows, targeted legislative clarifications and alignments are required. While the Omnibus takes important steps toward reducing fragmentation, further adjustments are needed to strengthen legal certainty, prevent duplicative obligations, and ensure coherent application of EU data laws. The following recommendations focus on areas where legislative refinement can most effectively support trusted and seamless cross-border data flows.

1.1. Streamline International Data Transfer Obligations Across Data Laws, Including for Mixed Datasets

The Omnibus aims to reduce fragmentation across the EU digital framework. However, overlapping international transfer provisions in the GDPR, the Data Act, and the Data Governance Act continue to create legal uncertainty and duplicative compliance obligations, particularly for mixed datasets containing both personal and non-personal data. For example, combining customer orders and payment details with non-personal data, such as product catalogs, inventory levels, shipping logistics, in daily transactions creates costly legal uncertainty regarding compliance and fragmented risk.

If simplification is to deliver practical benefits, the Omnibus should clarify that where a mixed dataset is transferred under a valid GDPR transfer mechanism, no additional or parallel transfer requirements apply under other EU instruments.

GDA recommends:

- Clarifying that compliance with a valid GDPR transfer mechanism satisfies any corresponding international transfer requirements under the Data Act and the Data Governance Act for mixed datasets.
- Ensuring that no additional or duplicative transfer conditions apply where GDPR-compliant safeguards are already in place.

This alignment would reduce duplication, strengthen legal certainty, and support trusted cross-border data flows.

1.2. Preserve the Distinction Between Personal and Non-Personal Data in International Transfers

As the EU continues to refine its digital framework, it is essential to maintain a clear separation between transfer rules for personal and non-personal data.

The GDPR's international transfer regime is specifically designed to safeguard fundamental rights in relation to personal data. Non-personal data, such as industrial, machine-generated, and business data, does not raise the same fundamental rights considerations and has long benefited from the EU's commitment to the free flow of non-personal data.

In broader policy discussions, suggestions have emerged that could mirror GDPR-style transfer conditions for non-personal data. Such an approach would risk introducing de facto localization requirements, increasing costs for EU companies, and undermining Europe's competitiveness in global digital markets.

GDA recommends:

- Reaffirming that GDPR-style international transfer restrictions should not be extended to non-personal data.

- Preserving the EU's commitment to the free flow of non-personal data, consistent with its trade obligations.
- Maintaining a clear and predictable separation between personal and non-personal data transfer regimes in future initiatives.

Maintaining this distinction is essential to ensure that simplification does not inadvertently restrict cross-border data flows.

1.3. Clarify Article 32 of the Data Act

Article 32 of the Data Act lacks sufficient clarity and operational predictability regarding international transfers of non-personal data. While intended to address risks of unlawful third-country access, the provision does not clearly define the scope of its obligations, the circumstances in which they apply, or the specific compliance measures required.

This ambiguity creates operational uncertainty for providers of cross-border data services. In practice, it may encourage overly cautious interpretations that restrict the use of global infrastructure or lead to de facto localization outcomes, contrary to the EU's commitment to the free flow of non-personal data and its competitiveness objectives.

In the online business context, overly broad or ambiguous interpretations of Article 32 could effectively prevent companies from leveraging global infrastructure to serve European merchants, undermining the EU's own objectives of supporting SME internationalization and cross-border trade. The provision should be clarified to ensure it does not inadvertently restrict legitimate commercial data processing activities that are essential to the functioning of cross-border digital commerce.

To ensure that simplification delivers meaningful improvements, Article 32 should be clarified and narrowly framed.

GDA recommends:

- Defining clear scope, triggers, and compliance expectations under Article 32 to enhance legal certainty.
- Ensuring that obligations are proportionate and do not result in de facto localization requirements.
- Aligning Article 32 with the EU's international trade commitments.

Greater precision would reduce uncertainty, support consistent implementation, and strengthen trusted cross-border data services.

1.4. Strengthen Harmonization and Consistency of Terminology

While the Omnibus seeks to reduce fragmentation across the EU digital framework, two structural issues continue to undermine legal certainty for cross-border data flows: divergent Member State derogations under the GDPR and inconsistent terminology across digital legislation.

First, broad GDPR derogation clauses have led to materially different national rules in key areas. For example, Article 23 permits Member States to restrict data subject rights for public security, regulatory supervision, or financial interests, while Article 9(4), Article 88, and Article 89 – among other GDPR derogation provisions – allow national variation in the processing of health and biometric data, employment data, and scientific research. In practice, this has resulted in divergent national requirements across multiple areas of GDPR implementation, including employee data processing, health data use, and research-related pseudonymization and consent waivers.

These divergences increase compliance costs, complicate cross-border operations, and weaken the GDPR's objective of harmonization.

Second, key EU digital instruments use overlapping but not consistently aligned definitions, such as "data controller," "data holder," "provider," "user," and references to "significant" or "severe" incidents. Divergent terminology creates interpretative uncertainty and risks duplicative or conflicting compliance obligations for companies operating across multiple regulatory regimes.

If simplification is to deliver meaningful operational benefits, greater harmonization and definitional alignment are essential.

GDA recommends:

- Limiting the use of broad GDPR derogation clauses and promoting greater convergence in the application of the GDPR across the EU.
- Aligning core definitions across EU digital legislation by establishing a shared digital lexicon, building on established GDPR concepts.
- Ensuring that future legislative initiatives prioritize consistency of terminology and scope across instruments.

Improved harmonization and clearer definitions would reduce fragmentation and enable the free flow of data.

1.5. Support GDPR Amendments on Pseudonymisation, and Scientific Research

GDA welcomes the Omnibus' clarifications to the GDPR that improve legal certainty without weakening fundamental rights. Clarifying that identifiability must be assessed relative to a controller's means and legal powers reflects established legal interpretation and reduces unnecessary over-classification of data as personal.

It is essential that industry stakeholders are involved in the development of pseudonymization means and criteria to ensure they are practical, technically feasible and capable of delivering strong privacy protection without creating disproportionate burdens or stifling innovation.

Similarly, providing a clear, operative definition of scientific research, applicable to both public and private actors, supports responsible innovation in areas such as health, cybersecurity, and AI, where private-sector research plays a central role. The key criterion should be a broader positive impact on society, allowing research that improves safety, security, efficiency, or accessibility of goods and services. Clarifying the scope of research in the GDPR would help remove unjustified barriers that have held back projects that are fully compatible with the GDPR.

Taken together, these changes enhance predictability, reduce inconsistent enforcement, and enable legitimate data use under existing GDPR safeguards.

GDA recommends:

- Preserving the Commission's proposed clarifications on identifiability and pseudonymization, while ensuring meaningful involvement of industry stakeholders in developing pseudonymization means and criteria that are practical and technically feasible.
- Maintaining the operative definition of scientific research, while ensuring it captures research with broader positive societal impacts, including improvements to safety, security, efficiency, and accessibility.

Adopting these amendments will strengthen legal certainty, incentivize privacy-enhancing safeguards, and support trusted cross-border data flows consistent with the GDPR's fundamental rights framework.

1.6. Further Streamline Incident Reporting to Support Cross-Border Operations

GDA supports the creation of a single-entry point for incident reporting across the GDPR, NIS2, DORA, eIDAS, and the Critical Entities Resilience Directive. GDA believes this should be extended to the AI Act and the Cyber Resilience Act. The principle of "report once, share where necessary" can significantly reduce duplication and improve coordination among authorities.

However, simplification must extend beyond the reporting interface. Companies operating across borders continue to face multiple reporting triggers, staggered timelines, and overlapping templates under different legal regimes. These inconsistencies increase compliance burdens, create legal uncertainty, and complicate cross-border incident management. The financial sector, for instance, would dual-report under the Cyber Resilience Act and the Digital Operational Resilience Act (DORA) and these forms of inconsistencies should be removed in the Omnibus.

If the Omnibus is to deliver meaningful simplification, it should align both the reporting channel and the underlying obligations.

GDA recommends:

- Extend the single-entry point to all incident reporting regimes in the EU.
- Establishing legal equivalence of the single-entry point, so that a notification submitted in good faith satisfies reporting obligations under all applicable EU regimes.
- Establish the principle that companies should report under a single regime for their sector.
- Converging on a single substantive reporting timeline aligned with the GDPR's 72-hour standard.
- Requiring one harmonized core reporting template, with clearly delimited sector-specific modules only where strictly necessary.
- Ensuring coordinated information-sharing among competent authorities to prevent parallel follow-up reporting requests.
- Embedding strong confidentiality and data-minimization safeguards to protect sensitive information.

A harmonized incident-reporting framework would reduce duplication and support seamless cross-border data flows while maintaining high standards of accountability.

1.7. Clarify the Interaction Between Sector-Specific and Horizontal Data Frameworks

While EU law contains established principles for resolving conflicts between legislative instruments, the practical interaction between sector-specific and horizontal data frameworks is not always clear.

Sector-specific regimes, such as the European Health Data Space (EHDS), include tailored rules for data access and sharing that reflect sector-specific safeguards and risks. At the same time, horizontal instruments such as the Data Act introduce broader obligations that may overlap with sectoral frameworks. In practice, this can create uncertainty or duplicative compliance expectations, particularly in cross-border operations. The DORA applies an all-encompassing risk management framework covering the IT infrastructure of financial entities and yet the Cyber Resilience Act creates separate rules to products with digital elements, with product-related requirements that do not interpret clearly for financial services.

Greater clarity on how these instruments interact would support simplification and legal predictability.

GDA recommends:

- Clarifying, where appropriate, the relationship between sector-specific regimes such as the EHDS or DORA and horizontal instruments to prevent duplicative or conflicting data access and sharing obligations.
- Providing interpretative guidance on how *lex specialis* principles apply in practice.
- Promoting coordination among relevant European Commission services and supervisory authorities to ensure consistent cross-sector application.

Clearer articulation of the interaction between sectoral and horizontal frameworks would reduce compliance complexity and support seamless cross-border data flows.

1.8. Strengthen Legislative Coordination and Governance in EU Data Law

While the Omnibus seeks to simplify the EU digital framework, fragmentation often begins at the drafting stage, where overlapping mandates, parallel governance structures, and uncoordinated timelines create unnecessary complexity.

EU data legislation increasingly spans multiple policy domains and institutional actors. Without stronger coordination, new measures risk creating duplicative obligations, inconsistent interpretation, and overlapping enforcement structures.

If simplification is to deliver durable results, legislative governance and sequencing must improve.

GDA recommends:

- Establishing a formal inter-service coordination mechanism to ensure coherence across DGs and supervisory bodies from drafting through enforcement.
- Introducing a structured review process to assess proposed data legislation for conflicts, duplication, and interaction with existing frameworks.
- Streamlining EU data governance structures to avoid redundant supervisory mechanisms.
- Aligning implementation timelines with the adoption of necessary secondary legislation and guidance.
- Stronger coordination and sequencing would reduce compliance burdens and support more seamless cross-border data flows.

Stronger legislative coordination and governance would support cross-border data flows.

1.9. Promote Open and Non-Protectionist Approaches to Digital Sovereignty

As debates around digital sovereignty continue to shape EU legislation, there is a growing risk that resilience objectives may be interpreted in ways that inadvertently encourage geographic restrictions, localization requirements, or origin-based limitations. While strengthening resilience and trust is a legitimate and important goal, sovereignty should not be equated with isolation.

GDA believes that Europe's digital sovereignty is best achieved through openness, interoperability, risk-based governance, and international cooperation, not through exclusionary or protectionist measures.

Excessive localization requirements or origin-based criteria risk fragmenting the Digital Single Market, reducing competition, increasing costs, and weakening Europe's global competitiveness.

For simplification to support cross-border data flows, EU legislation should reinforce trust-based and risk-based approaches rather than introduce or expand geographic or other protectionist restrictions.

GDA recommends:

- Avoiding origin-based or "European-only" requirements in data-related legislation, except where strictly necessary and proportionate based on clearly identified risk.
- Ensuring that any sovereignty-related controls are grounded in objective, risk-based assessments rather than the geographic origin of technology providers.
- Promoting interoperability, open standards, and mutual recognition mechanisms that enhance resilience while preserving openness.
- Ensuring that sovereignty-based measures remain carefully targeted to clearly justified cases, avoid broad "European preference" requirements, and are designed to be consistent with EU commitments under the WTO Government Procurement Agreement and other international norms.
- Continuing to advance international cooperation, including adequacy decisions and regulatory dialogues, to counter unjustified data localization and protectionist measures globally.

A sovereignty framework grounded in openness, accountability, and global cooperation would strengthen resilience without undermining the seamless cross-border data flows that are essential to Europe's economic growth and digital leadership.

2. Non-Legislative Recommendations to Support Cross-Border Data Flows

In addition to the targeted legislative amendments outlined above, complementary non-legislative measures can further strengthen legal certainty, coherence, and operability across the EU digital framework. Effective simplification depends not only on the text of the law, but also on coordinated implementation, practical guidance, and structured cooperation among institutions and stakeholders. The following recommendations focus on implementation tools that can enhance interoperability, reduce fragmentation, and support cross-border data flows.

2.1. Strengthen and Expand the International Personal Data Transfer Toolbox

Effective support for cross-border data flows depends on the usability, expansion, and predictability of the GDPR's international transfer mechanisms.

The GDPR provides a comprehensive framework, including adequacy decisions, Standard Contractual Clauses (SCCs), Binding Corporate Rules (BCRs), certifications, and codes of conduct. However, several of these tools remain underutilized or lack sufficient operational support. Strengthening and promoting these mechanisms would enhance legal certainty and reinforce the EU's global leadership in data protection.

Because they permit transfers without additional Chapter V safeguards, adequacy decisions are a practical and effective mechanism. A broader and more strategically deployed adequacy network would reduce fragmentation and reliance on resource-intensive data transfer assessments.

GDA recommends:

- Promoting and streamlining the approval of GDPR Codes of Conduct and Certification mechanisms as scalable transfer solutions.
- Providing clearer, practical guidance on transfer impact assessments to reduce unnecessary complexity and compliance burdens.

- Accelerating the adoption of adequacy decisions with key trading partners and maintaining support for existing frameworks, including the EU-US Data Privacy Framework.
- Increasing transparency and predictability in adequacy assessment, review, and renewal processes.

A strengthened and expanded transfer framework would enhance legal certainty, reduce compliance burdens, and support responsible data flows consistent with EU law

2.2. Provide Clearer Guidance and Practical Tools for Transfer Impact Assessments

Where adequacy decisions are not in place, companies must rely on other GDPR transfer mechanisms, often requiring case-by-case assessments of third-country legal systems. These transfer impact assessments (TIAs) are complex, resource-intensive, and frequently require legal analysis beyond the capacity of many organizations, particularly smaller companies.

In practice, due to legal uncertainty and divergent supervisory expectations, companies often apply disproportionate TIA processes to routine or low-risk transfers, including transfers of non-sensitive data or data categories that individuals reasonably expect as part of normal service delivery. This reflects a lack of clear, proportionate, and harmonized regulatory guidance. Introducing clearer and more risk-based rules would reduce unnecessary burdens while maintaining strong protections. In particular, TIAs could be calibrated to the actual likelihood and severity of transfer-related risks, with simplified requirements for low-risk or operationally necessary transfers. This would ensure that compliance efforts focus on scenarios where meaningful risks exist, rather than diverting resources into procedural exercises that do not materially enhance data protection.

Greater clarity and practical support from EU institutions would enhance legal certainty and reduce disproportionate compliance burdens, while maintaining high standards of data protection.

GDA recommends:

- Providing more detailed and practical guidance on conducting TIAs, including illustrative examples and risk-based methodologies.
- Introducing clearer exemptions or lighter-touch, risk-based TIA requirements for routine and operationally necessary transfers, including those involving non-sensitive data or presenting a demonstrably low likelihood and severity of harm to individuals.
- Developing centralized resources or reference materials to support consistent assessment of third-country legal frameworks.
- Encouraging coordinated interpretation among supervisory authorities to reduce divergent expectations across Member States.

Improved guidance and practical tools would help companies apply existing transfer mechanisms more consistently and confidently, thereby supporting responsible cross-border data flows.

2.3. Strengthen Practical and Inclusive Implementation

Legislative clarity must be matched by practical, timely, and transparent guidance. Effective implementation tools are essential to reduce compliance burdens and ensure that data laws function smoothly in cross-border contexts.

GDA recommends:

- Developing horizontal implementation guidance, in consultation with stakeholders, to clarify how key instruments, such as the GDPR and the Data Act, interact in practical scenarios involving personal data, mixed datasets, AI systems, or cloud infrastructure.
- Ensuring meaningful consultation before adopting guidelines or recommendations, and publishing summaries explaining how stakeholder input was considered.
- Publishing simplified templates, FAQs, and sector-specific toolkits to support cost-effective compliance, particularly for SMEs.
- Issuing guidance well in advance of application deadlines.

Practical, inclusive, and transparent implementation would enhance consistency and support cross-border data flows.

2.4. Promote Consistent and Proportionate Interpretation Across the EU

Fragmentation also arises from divergent or overly restrictive interpretations of EU digital legislation by supervisory authorities. Differences in enforcement practice in the Member States, particularly in areas such as special category data, data protection impact assessments, anonymization standards, and the treatment of IP addresses, can undermine harmonization and create uncertainty for cross-border operators.

In some instances, guidance adopted at EU or national level has been interpreted in a manner that narrows lawful data use beyond what is required by the text of the legislation or the case law of the Court of Justice.

GDA recommends:

- Strengthening coordination within the EDPB and among national authorities to promote consistent application of the GDPR and related digital legislation.
- Encouraging proportionate, risk-based interpretation that reflects both the objectives of the legislation and the operational realities of cross-border data use.
- Providing clearer alignment between EDPB guidance and Court of Justice jurisprudence to avoid interpretative divergence.

Greater consistency and proportionality in enforcement would enhance legal certainty, preserve harmonization, and reinforce the functioning of the Digital Single Market.

2.5. Strengthen Standards-Based and Collaborative Implementation

Greater reliance on internationally recognized standards and structured stakeholder engagement can improve coherence and interoperability across the EU digital framework. A standards-based approach reduces duplication and aligns EU requirements with global best practices.

GDA recommends:

- Leveraging internationally recognized standards, including relevant ISO/IEC standards, in EU certification schemes and implementing measures to avoid parallel technical frameworks.
- Encouraging voluntary co-regulatory mechanisms, such as codes of conduct and industry-developed standards under EU oversight, to support risk-based compliance.
- Establishing permanent EU-level regulatory forums to enable structured dialogue among policymakers, regulators, industry, and civil society.
- Promoting interoperable technical infrastructure, including common APIs and open frameworks, to facilitate cross-border compliance and data portability.

A standards-based and collaborative approach would enhance legal certainty, strengthen resilience, and support global interoperability.

2.6. Advance a Multilateral, Principle-Based Approach to International Data Transfers

Trusted cross-border data flows require not only coherent EU rules, but also greater international alignment. As global data exchanges expand, interoperable and accountable transfer frameworks are essential to reduce fragmentation while maintaining high standards of protection.

The EU should actively engage in multilateral initiatives, such as the OECD Privacy Guidelines and the Global Cross-Border Privacy Rules (CBPR) system, to promote convergence around principle-based and certifiable approaches to data protection.

GDA recommends:

- Strengthening EU participation in international data governance forums to foster regulatory cooperation and interoperability.
- Supporting certifiable and interoperable transfer mechanisms that enable lawful cross-border data flows while ensuring accountability.
- Encouraging mutual recognition approaches that reduce jurisdictional fragmentation.

A multilateral and principle-based strategy would reinforce the EU's global leadership and support secure, predictable cross-border data flows.

Conclusion: Reaching the Omnibus' Potential

The Digital Simplification Omnibus presents an important opportunity to strengthen coherence across the EU's digital framework. As currently proposed, it does not yet fully realize its potential to advance cross-border data flows – one of the central drivers of Europe's competitiveness and digital resilience.

By clarifying the interaction of cross-border transfer rules, preserving the distinction between personal and non-personal data, aligning incident reporting obligations, improving legislative coordination, and reinforcing

open and non-protectionist approaches, co-legislators can ensure that simplification delivers greater legal certainty and operational coherence.

Complementary non-legislative measures, including strengthening the international transfer toolbox, expanding adequacy decisions, improving practical guidance, promoting consistent interpretation, leveraging international standards, and deepening multilateral cooperation, can further support trusted and seamless cross-border data flows.

Together, these steps would allow the EU to uphold high standards of protection while preserving openness, innovation, and global competitiveness. GDA stands ready to engage constructively with EU institutions to advance these objectives.

For further information, please contact

Irma Gudžiūnaitė,

Director, Policy – EMEA, at irmag@bsa.org.