**Policy brief**

**Data flows in supply chains**

**FIRST DRAFT**

**Executive Summary**

**[To come]**

**Introduction**

Cross-border data flows are essential for efficient, resilient and interconnected global supply chains. All industries, including information services, high-value manufacturing, financial services, and e-commerce, depend heavily on real-time data exchange to manage all aspects of their operations. According to recent studies, cross-border data flows can drive a 145% increase in exports for every 0.1-point reduction in digital restrictions[[1]](#footnote-2).

Despite their critical role, cross-border data flows face growing regulatory hurdles. The lack of multilateral coordination and a fragmented regulatory landscape create barriers to trade and disrupt supply chains. Key issues -- ranging from data localisation requirements to varying data protection laws and cybersecurity rules - pose costly compliance issues. According to the OECD, data autarky - or full fragmentation, where all economies fully restrict their data flows -- could reduce global GDP by 4.5% and cut exports by 8.5%[[2]](#footnote-3).

Such restrictive and fragmented data policies are driving up costs, creating inefficiencies, and limiting business opportunities, undermining companies’ ability to optimise supply chain operations, remain competitive and scale internationally. Acting as non-tariff barriers, they reduce firms’ ability to expand into global markets and slthe ow growth of digital trade –ultimately, weakening supply chain resilience.

This policy brief examines the critical role of data flows in the functioning of global supply chains and the adverse impacts of restrictive data policies on trade. It provides recommendations for fostering trade policies that allow secure and trusted cross-border data flows. Without them , supply chains cannot operate efficiently or at scale. In short, moving data across borders is as essential to supply chains as the movement of goods and services – it isa supply chain imperative.



**Diagram 1: Data Flows in Coffee Supply Chain – Key Stages, Data Types, and Business Interactions**

This diagram illustrates how cross-border data flows underpin each stage of the coffee supply chain – from sourcing raw materials to delivering products to end consumers. It highlights how both non-personal and personal data are used to coordinate production, manage logistics, and respond to consumer needs. Efficient data flows enable companies to optimise operations, reduce delays, and enhance customer satisfaction—making data a critical input for modern, resilient supply chains.

**[VISUAL TO BE ADDED HERE – COFFEE PRODUCTION EXAMPLE AND THE BARRIERS CAUSED BY DATA FLOW RESTRICTIONS ACROSS THE SUPPLY CHAIN LIFECYCLE]**

**Diagram 2: Regulatory Barriers to Data Flows – Impact on Supply Chain** **Connectivity**

This diagram illustrateshow regulations hinder data flows and create a fragmented environment for businesses to operate in.

**Key stages in supply chain ‘trade lifecycle’ and the types of data typically transferred**

The table below is a non-exhaustive overview of the types of data that crosses borders.

|  |  |  |
| --- | --- | --- |
| **Supply chain stage** | **Type of data transferred** | **Data classification** |
| Supply (sourcing of raw material) | - Supplier information- Material specifications- Compliance certificates- Purchase orders- Delivery schedules | Non personal data |
| Manufacturing | - Production schedules- Bill of materials- Equipment maintenance records- Quality control data- Inventory levels | Non personal data |
| Distribution (shipping and logistics) | - Shipping manifests- Tracking information- Customs documentation- Carrier contracts- Delivery timelines | Non personal data |
| Consumer (retail and end-user) | - Sales data- Customer feedback- Warranty information- Return and refund records- Marketing analytics | Personal data (minus the Sales data) |
| Post-Sale / End-of-Lifecycle | * Product usage data (e.g. performance logs, error reports)
* Return and repair data
* Recycling or disposal tracking
* Sensor data from IoT-enabled products
 | Non personal data |
| Business operations that support all above stages | Workforce management (i.e. production, logistics, sales, training, recruitment and performance) | Personal data (employee information, financial data linked to employees), and non-personal data (trainings, workforce analytics at aggregate level) |

**Key Trade Policy Challenges for Data Flows in Global Supply Chains – and What They Mean in Practice**

Despite their critical role in enabling supply chain integration and efficiency, cross-border data flows face growing regulatory constraints. This section outlines key trade policy challenges businesses encounter in moving data across borders — and what those challenges mean in operational terms.

**Regulatory fragmentation creates supply chain uncertainty**

In the absence of a global framework for cross-border data flows, governments have adopted divergent approaches through national laws and trade agreements. This patchwork of rules creates legal risk and operational complexity, driving up compliance costs and making it harder for businesses to integrate supply chains across markets. Firms are often forced to maintain separate data handling protocols, duplicate IT systems, and hire additional compliance staff—undermining efficiency and competitiveness.

**Data Localization as a Barrier to Supply Chain Efficiency**

Restrictions on where data can be stored or processed limit supply chain visibility and delay time-sensitive operations such as shipping, customs clearance, and trade finance. Businesses may be unable to share real-time data with partners across borders, leading to slower delivery times, missed deadlines, and higher costs. Localisation measures also prevent companies from using centralized systems, forcing them to fragment their operations—an especially difficult burden for MSMEs.

**Restrictive Data Policies Increase Supply Chain Costs & Complexity**

Modern supply chains depend on seamless data transfers for tracking shipments, optimizing logistics, and managing supplier relationships. These data flows are not linear or static – they are updated, enriched, or shared across multiple actors in real time. For example, a company shipping goods internationally needs to share real-time updates across ports, customs, and warehouses. If data cannot flow freely, goods may be held up at borders, customers left waiting, and supplier performance impacted.

At the same time, companies must navigate overlapping or conflicting rules across jurisdictions, often requiring legal experts, duplicate operational systems and costly workarounds - reducing agility and diverting resources from innovation and growth. Data flow restrictions also limit the use of digital supply chain innovations—such as IoT tracking, predictive inventory, and supply risk analytics—making it harder for businesses to detect delays, avoid shortages, or adapt to supplier issues. The result is a less agile, more vulnerable supply chain.

**Lack of Interoperable Standards Limits Supply Chain Digitalization**

Cross-border data flows depend not just on permission to transfer data, but also on compatible rules and systems that allow supply chain partners to exchange and act on that data. Conflicting regulations and inconsistent standards make it harder to implement end-to-end digital solutions across markets. For example, a multinational logistics company may want to use a single cloud-based system to coordinate shipping, customs clearance, and delivery across countries. But if one country restricts the transfer of logistics data or requires local data storage, the company must build a separate system for that country - increasing costs, delaying upgrades, and reducing visibility across the supply chain.

MSMEs in supply networks face even greater challenges. A small manufacturer selling inputs to a multinational buyer may need to comply with multiple layers of data privacy and cybersecurity rules across jurisdictions. Without legal support or digital infrastructure, many MSMEs are simply unable to comply, cutting them off from global value chains.

 Even in digital-first environments, inconsistent standards for electronic documentation disrupt data flows by making it harder for supply chain partners to transmit and process electronic information across borders. A business shipping goods may have to print and courier paper documents to meet local customs requirements, even if its internal systems are fully digital. This causes delays at the border, increases the chance of human errors, and undermines efficiency gains from automated digital tools and processes.

**Confidential Business Information (CBI) & Compliance Risks**

Supply chain data flows often involve the transfer of highly sensitive commercial information, ranging from supplier networks, inventory levels, logistics routes, and trade finance records, to Confidential Business Information (CBI), such as profit margins, customer lists, purchase histories, supplier contracts, pricing agreements, and product designs. When this data moves across jurisdictions, it may be subject to forced disclosure or weak protection frameworks—exposing businesses to competitive and compliance risks.

For example, a global retailer may need to share its inventory levels and trade finance records with international partners to coordinate shipments and payments. In jurisdictions with forced disclosure, such data flows could inadvertently expose sensitive data, such as pricing strategies and supplier agreements – information that competitors could use to undercut market position.

In some countries, businesses are required to share supply chain data with government agencies or third-party vendors, even where protections are inadequate. This increases the risk that proprietary supply chain information, such as pricing or customer data, could be accessed by unauthorized actors. In jurisdictions with weak data protections, breaches can lead to the exposure of customer lists or strategic business plans - causing reputational harm, legal liability, and a loss of competitive advantage.

**ICC Recommendations to promote the free flow of data in global supply chains**

**Pursue Multilateral Rules at the WTO**

Multilateral efforts—particularly through the WTO Joint Statement Initiative on E-Commerce—should be used to advance clear, trade-focused rules on cross-border data flows. The stabilized text on digital trade facilitation provisions[[3]](#footnote-4) represents a critical achievement and deserves strong support. It should be swiftly integrated into the WTO framework to deliver concrete benefits for supply chain efficiency and predictability. At the same time, resumed negotiations on cross-border data flows are urgently needed. Businesses rely on the ability to move data securely and seamlessly across borders, and the absence of multilateral rules continues to create uncertainty and fragmentation in global supply chains.

**Promote Risk-Based and Differentiated Regulatory Approaches**

Regulatory approaches should be risk-based and evidence-based to avoid unnecessary trade barriers. Recognizing the differences between types of data is essential for ensuring proportional and workable regulations. Differentiated obligations based on actual risk levels and operational needs can help avoid unnecessary trade barriers. This is particularly important for global supply chains, where low-risk, non-personal data plays a vital role in day-to-day operations and should not be subject to the same restrictions as sensitive personal information.

**Ensure Open and Interoperable Cross-Border Data Frameworks**

Open and interoperable data frameworks are essential to the functioning of modern supply chains. Indiscriminate data localisation mandates that require all data—regardless of type—to be stored locally disrupt global supply chains. Trade agreements should promote flexible and innovation-friendly data governance frameworks that do not mandate specific technologies or systems.

Regulatory coherence and mutual recognition of standards should be prioritised to reduce trade frictions. Security and privacy protections are critical, but they must be designed in way that do not impose unnecessary restrictions on trade and data-driven business models.

**Safeguard Confidential Business Information in Cross-Border Data Regulations**

Cross-border data regulations must include safeguards to prevent misuse, breaches, or unfair access of highly sensitive commercial information. Forced data-sharing mandates that require businesses to disclose such data without adequate protections and systems controls risk undermining trust and deterring business participation in cross-border supply chains. Trade agreements and regulatory frameworks should include strong protections against the misuse of commercially sensitive data and ensure that trade-related data transfers are subject to privacy, security, and non-discriminatory treatment provisions. Clear and enforceable mechanisms are essential to protect CBI and maintain the integrity of digitally connected global supply chains.

**Support a Digital Trade Enabling Environment**
A supportive digital trade environment is essential for reducing friction and improving efficiency across global supply chains. Harmonised digital trade documentation standards are essential to reducing friction in supply chains. Trade agreements should include provisions that promote supply chain digitalisation and reflect the operational needs of today’s data-driven economy.

Governments should also encourage the development of data handling certification programs within trusted trader frameworks to enhance supply chain security and efficiency. These can enhance compliance, build confidence in cross-border data exchanges, and improve supply chain security without adding unnecessary administrative burdens. Together, these measures help ensure that businesses—especially MSMEs—can fully benefit from digital trade opportunities.

**Quotes and other supporting messages**

**Quotes from companies in break-out boxes providing real-life reflections on the adverse effects of data flow restrictions (e.g. SMEs in developing countries, multinational).**

*Fictional example 1*

We’re a small logistics tech start-up in Kenya. Every time we expand into a new market, we face completely different data compliance rules. We don’t have the in-house legal resources to keep up and that slows down our ability scale internationally and integrate global supply chains.

Founder, SME Logistics Platform

*Fictional example 2*

We had to redesign our entire inventory management system to meet local data localisation rules. It doubled our IT costs and broke the real-time coordination we had across our regional warehouses. The disruption to our supply chain visibility has made it harder to deliver on time and serve our customers efficiently.

Multinational Electronics Manufacturer

*Fictional example 3*

Our supply chain spans more than 20 countries, and we rely on continuous data flows to coordinate suppliers, manage production timelines, and track shipments. But conflicting data regulations force us to maintain separate systems in different markets. It’s costly, inefficient, and makes it harder to respond quickly to disruptions—especially when every second counts in electronics manufacturing.

Multinational Electronics Manufacturer

**Conclusion**

**[To come]**

**Additional Resources**

[ICC White Paper on Trusted Government Access to Personal Data Held by the Private Sector](https://iccwbo.org/news-publications/policies-reports/icc-white-paper-on-trusted-government-access-to-personal-data-held-by-the-private-sector/)

[ICC Policy primer on non-personal data](https://iccwbo.org/news-publications/policies-reports/policy-primer-on-non-personal-data/)

[ICC Digital Standards Initiative (DSI) Key Trade Documents and Data Elements](https://www.dsi.iccwbo.org/_files/ugd/8e49a6_9f8444133fc64fc9b59fc2eaaca2888e.pdf)

1. OECD (2023) Of Bytes and Trade: Quantifying the Impact of Digitilisation on Trade, https://read.oecd. org/10.1787/11889f2a-en?format=pdf. [↑](#footnote-ref-2)
2. OECD/WTO (2025), *Economic Implications of Data Regulation: Balancing Openness and Trust*, OECD Publishing, Paris, <https://doi.org/10.1787/aa285504-en>. [↑](#footnote-ref-3)
3. [directdoc.aspx](https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/INF/ECOM/87.pdf&Open=True), (26 July 2024) [↑](#footnote-ref-4)