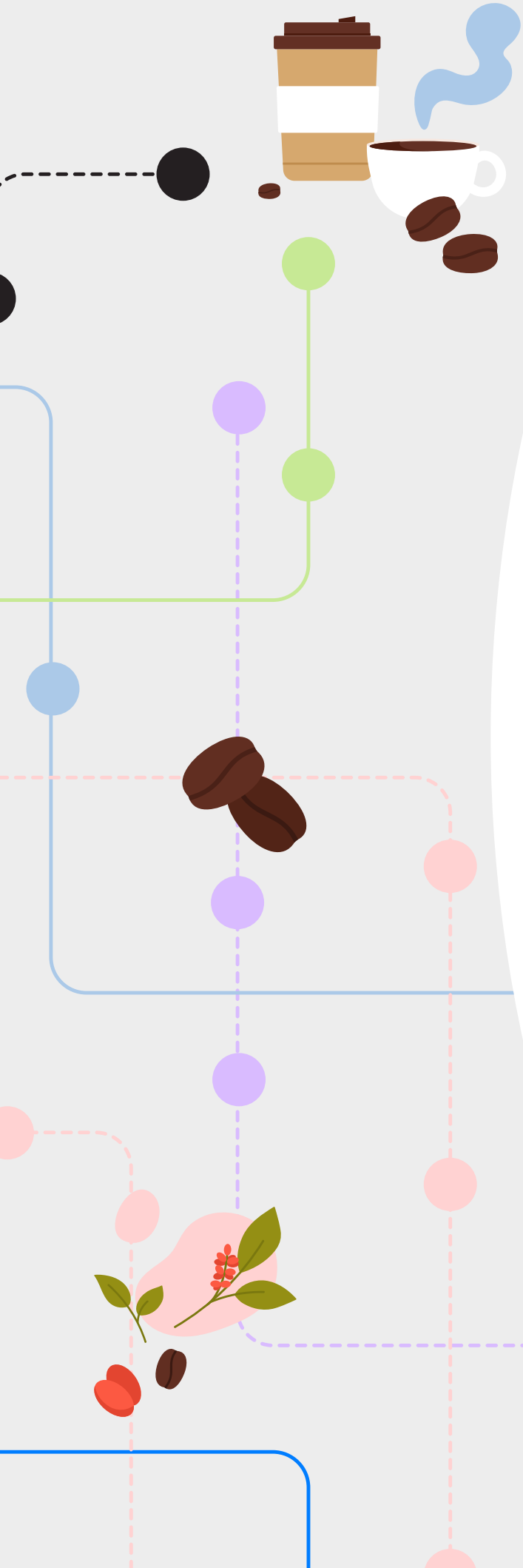


Data flows in supply chains

Policy brief

Table of contents

Executive summary 3

Introduction 4

Key trade policy challenges for data flows in global supply chains – and what they mean in practice 8

ICC recommendations to promote the free flow of data in global supply chains 10

Industry insights 12

Conclusion 13

Additional resources 13

Executive summary

- Cross-border data flows are essential to modern supply chains, enabling real-time coordination, logistics, compliance, and customer responsiveness.
- Growing regulatory fragmentation, including data localisation mandates, inconsistent privacy laws, and incompatible standards, acts as a non-tariff barrier to trade. These restrictions increase costs, reduce supply chain visibility, and undermine global competitiveness.
- Micro-, Small and Medium-sized Enterprises (MSMEs) are disproportionately affected by digital trade barriers, often lacking the resources to navigate complex data compliance requirements. This limits their ability to participate in global value chains and hinders inclusive trade.
- Data flow restrictions impair key supply chain functions, including traceability, customs clearance, risk analysis, and the deployment of digital tools such as IoT and predictive analytics.
- Inconsistent rules also put sensitive commercial data at risk, with forced disclosure and weak protections threatening business confidentiality and trust.
- To preserve cross-border data flows and ensure resilient, efficient global supply chains, ICC calls for coordinated international action to address growing regulatory fragmentation. Specifically, ICC recommends:

    - Pursue multilateral rules at the WTO to enable trusted, secure, and predictable cross-border data flows.
    - Promote risk and evidence-based approaches to determine when there should be an exception to the default position of allowing data to flow across borders.
    - Ensure open and interoperable data frameworks by avoiding blanket data localisation and supporting mutual recognition of standards.
    - Safeguard Confidential Business Information (CBI) in trade and data policies through enforceable protections.
    - Support a digital trade enabling environment, including harmonised documentation standards and trusted trader certifications to reduce friction and increase participation, especially for MSMEs.

The full set of recommendations is provided on page 10.

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].

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].

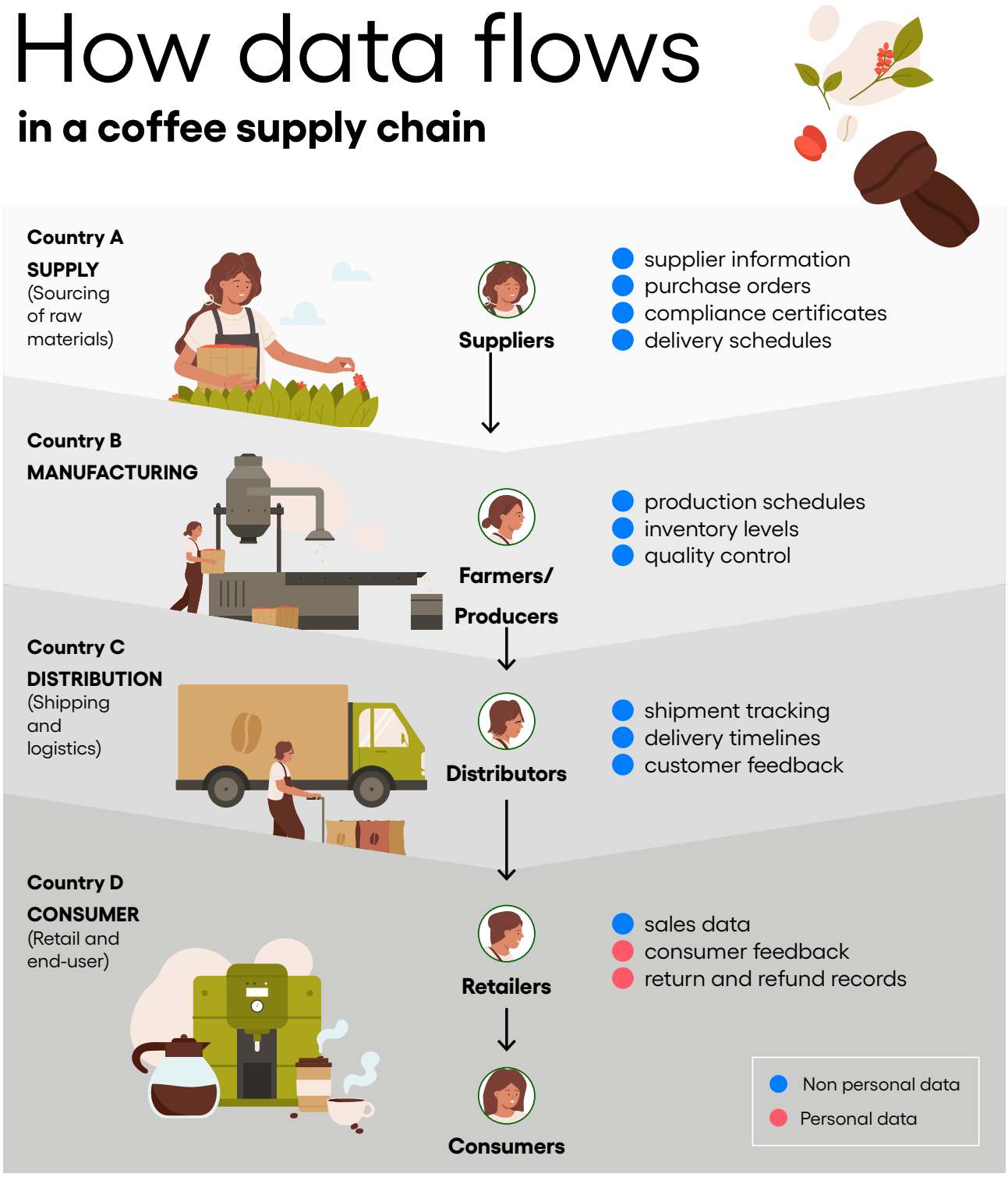
Such restrictive and fragmented data policies are driving up costs, creating inefficiencies, and limiting business opportunities, undermining companies' ability to optimise supply chain operations, remain competitive and scale internationally. Acting as non-tariff barriers, they reduce firms' ability to expand into global markets and slow the 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 is a supply chain imperative.

1 OECD (2023) Of Bytes and Trade: Quantifying the Impact of Digitalisation on Trade, https://read.oecd.org/10.1787/11889f2a-en?format=pdf.

2 OECD/WTO (2025), *Economic Implications of Data Regulation: Balancing Openness and Trust*, OECD Publishing, Paris, https://doi.org/10.1787/aa285504-en.

Figure 1:
Data flows in the coffee supply chain – Key stages, data types and business interactions



Source: ICC (2025), Policy brief: Data Flows in Supply Chains

This diagram (see Figure 1) 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.

Regulatory barriers to data flows and their impact on supply chain connectivity

The table below illustrates how regulations hinder data flows and create a fragmented environment for businesses to operate in.

✖ Barrier	● What it is	! Impact on supply chains
Regulatory fragmentation	Lack of a unified global framework, with each country enforcing different rules on data flows.	Legal uncertainty, higher compliance costs, operational silos.
Data localisation requirements	Rules that require data to be stored or processed within a specific country.	Delays in shipping, customs, and inventory management. Reduces ability to use centralised systems, which is especially burdensome for SMEs and MSMEs.
Restrictive data policies	Overlapping or conflicting standards for personal and non-personal data, that restrict their seamless transfers.	Increases operational costs, hinders supply chain visibility, and causes delays.
Lack of interoperable standards	Incompatible rules, formats, or technical requirements for digital systems across jurisdictions.	Disrupts automation, increases manual paperwork, forces redundant systems, and limits integration across global supply chains.
Forced disclosure and weak confidentiality protections	Requirements that expose sensitive commercial information without adequate legal or technical safeguards.	Risks of data misuse, loss of competitive advantage, and reduced trust in cross-border collaboration.
Barriers to data traceability	Restrictions on cross-border data flows or lack of harmonised frameworks that enable end-to-end tracking of goods, services, and data.	Hinders the ability to track goods in real time, confirm their origin and ensure they meet compliance standards.

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 • Sensor data from IoT-enabled products	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	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.

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. It is important to note that, not all data policies intentionally restrict the movement of operational or supply chain data. In fact, many regulatory frameworks, including privacy laws, focus specifically on personal data. However, due to legal ambiguities, mixed-use systems, and compliance practices, these frameworks can have unintended consequences for broader data flows critical to supply chain performance.

Regulatory fragmentation creates supply chain complexity

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. Businesses must also navigate overlapping or conflicting regulatory obligations, often requiring legal experts and costly workarounds to remain compliant—undermining efficiency, reducing agility, and diverting resources from innovation and growth.

Data localisation 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. While, data privacy laws are essential to protect individuals, without clear carve-outs or tailored frameworks, they can inadvertently hinder global supply chains. Many jurisdictions require personal data to be stored or processed locally. This directly affects supply chain systems like centralised logistics platforms or cloud enterprise resource planning (ERP), forcing businesses to create country-specific data silos.

This is particularly challenging because personal and non-personal data are processed together in supply chain systems. For instance, a shipping record may include both container data and the name of the customs broker or driver. As a result, restrictions aimed at personal data can trigger broader compliance burdens or force companies to silo operational systems locally, even when the vast majority of data is non-sensitive or commercial in nature.

Because of these restrictions, 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 and complexity

Modern supply chains depend on seamless data transfers for tracking shipments, optimising 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. Data privacy laws such as EU's General Data Protection Regulation (GDPR) can make this even more complex. They often require that personal data be collected only for specified purposes, and that individuals consent to transferring the data to third parties and/or overseas. In supply chains, where data is shared between logistics providers, customs brokers, and vendors, ensuring consent and purpose alignment can be operationally challenging.

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 digitalisation

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 for use in multiple jurisdictions may need to comply with multiple layers of data privacy and cybersecurity rules across those different jurisdictions. Without legal support or digital infrastructure, many MSMEs are simply unable to comply, cutting them off from global value chains.

Fragmented data flows undermine supply chain traceability compliance

Supply chain data flows are essential for compliance with laws that require upstream supply chain traceability, such as the EU Deforestation Regulation (EUDR) and the US Uyghur Forced Labor Prevention Act (UFLPA). To comply with these regulations companies need to prove the origin and ethical sourcing of goods well beyond their immediate suppliers, which is only feasible if data can move efficiently and securely across borders and between tiers. Interoperable, timely, and standardised data exchange allows businesses to gather the necessary documentation, conduct due diligence, and respond to audits or enforcement actions.

Confidential business information and compliance risks

Supply chain data flows often involve the transfer of highly sensitive commercial information, including data that may qualify as Confidential Business Information (CBI), under applicable laws. This includes information such as supplier networks, inventory levels, logistics routes, trade finance records, profit margins, customer lists, purchase histories, supplier contracts, pricing agreements, and product designs. While all of these data categories may carry strategic or competitive value, in many jurisdictions, only CBI is eligible for legal protection. As such, businesses often seek to treat these types of information as CBI, when engaging with governments or third parties. However, when this data moves across jurisdictions, it may be subject to forced disclosure requirements 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, sometimes in the absence of adequate protection mechanisms. This increases the risk that proprietary supply chain information, such as pricing or customer data, could be accessed by unauthorised 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 stabilised text on digital trade facilitation provisions represents an important first step toward delivering concrete benefits for supply chain efficiency and predictability. However, 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. A universal data flow framework with proper safeguards to protect data privacy are imperative for unhindered global trade.

Promote risk-based, differentiated regulatory approaches between personal and non-personal data

Regulatory approaches should be risk-based and evidence-based to avoid unnecessary trade barriers. Recognising the differences between types of data is essential for ensuring proportional and workable regulations. It is imperative to create a carve-out and treat non-personal supply chain data differently from personal data to avoid unnecessary friction with data privacy laws. 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 non-personal data plays a vital role in day-to-day operations and should not be subject to the same protections as personal data.

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. Targeted data localisation mandates have similarly deleterious effects on supply chains since often specific categories of data subject to such a requirement cannot be easily or effectively segregated from broader data sets. 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 commercial business information. Forced data-sharing mandates that require businesses to disclose such data with governments risk undermining trust and deterring business participation in cross-border supply chains. Where data-sharing is required, the requirement should only extend to sharing data with the government who must have a binding and enforceable obligation to safeguard the data against disclosure, and the data required to be shared must be limited to only what is necessary to meet a legitimate public policy objective. There should also be self-judging mechanisms on the designation of CBI. Trade agreements and regulatory frameworks should include strong protections against the misuse of commercial business information and ensure that trade-related data transfers are subject to 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 programmes 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.

Industry insights

"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 to scale internationally and integrate global supply chains."

Founder,
SME Logistics Platform

"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

"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

Efficient, trusted, and secure cross-border data flows are indispensable to the functioning of modern global supply chains. Without clear, interoperable, and risk-based policy frameworks, supply chain actors, especially MSMEs, will continue to face high barriers to participation.

ICC urges policymakers to prioritize multilateral cooperation, embrace global standards, and avoid overregulation that fragments the digital trade ecosystem. Data must move across borders with the same urgency and security as goods and services.

Delivering on this imperative is not just a matter of digital policy — it is a prerequisite for resilient, inclusive, and sustainable trade.

Additional resources

ICC White Paper on Trusted Government Access to Personal Data Held by the Private Sector

ICC Policy Primer on Non-Personal Data

ICC Digital Standards Initiative (DSI) Key Trade Documents and Data Elements

Please cite as:

ICC (2025), Data flows in supply chains,
www.iccwbo.org/news-publications/policies-reports/data-flows-in-supply-chains/

Copyright © 2025 International Chamber of Commerce

All rights reserved. ICC holds all copyright and other intellectual property rights in this work.

No part of this work may be reproduced, distributed, transmitted, translated or adapted in any form or by any means, except as permitted by law, without the written permission of ICC.
Permission can be requested from ICC through publications@iccwbo.org.

This document, as well as any data and map included herein, are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

About the International Chamber of Commerce

The International Chamber of Commerce (ICC) is the institutional representative of more than 45 million companies in over 170 countries. ICC's core mission is to make business work for everyone, every day, everywhere. Through a unique mix of advocacy, solutions and standard setting, we promote international trade, responsible business conduct and a global approach to regulation, in addition to providing market-leading dispute resolution services. Our members include many of the world's leading companies, SMEs, business associations and local chambers of commerce.

33-43 avenue du Président Wilson, 75116 Paris, France
T +33 (0)1 49 53 28 28 E icc@iccwbo.org
www.iccwbo.org @iccwbo