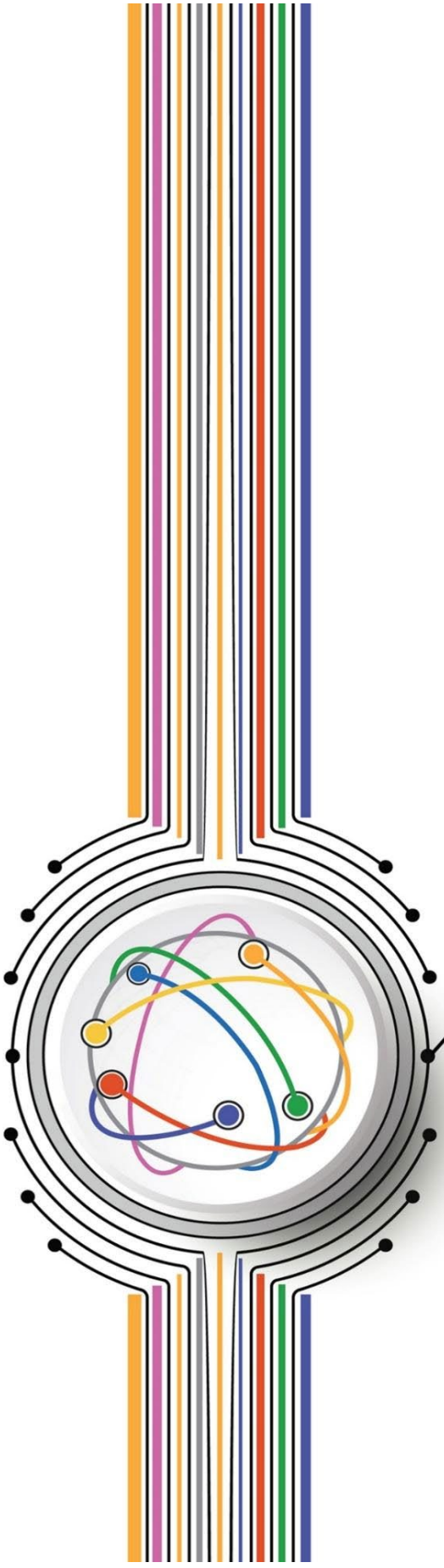


UNECE

White Paper

Data Governance For Trade Facilitation

November 2024

Note

The designations employed and the presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations concerning the legal status of any country, territory, city or area, or of its authorities, or concerning the delimitation of its frontiers or boundaries.

Acknowledgements

The UNECE Trade Facilitation Section and United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT) would like to express its gratitude to the experts who participated in the development of this paper: Sray Agarwal (project leader, Data Governance for Trade Facilitation), Nita Sharma, Kevin Atkinson, Craig Atkinson, Elma Liu, Cleiton Alves dos Santos Joao Simoes, Marco Gervasi, Pankhuri Bansal and Nurbek Maksutov (supporting Vice Chair).

The project team would like to extend their appreciation to the supporting Vice Chair and the UNECE secretariat for their support.

The United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT)

Simple, Transparent and Effective Processes for Global Commerce

The mission of UN/CEFACT is to improve the ability of business, trade and administrative organizations from developed, developing and transitional economies to exchange products and relevant services effectively. Its principal focus is on facilitating national and international transactions through the simplification and harmonization of processes, procedures and information flows in order to contribute to the growth of global commerce.

Participation in UN/CEFACT is open to experts from United Nations Member States, intergovernmental organizations and non-governmental organizations recognized by the United Nations Economic and Social Council (ECOSOC). Through this participation of government and business representatives from around the world, UN/CEFACT has developed a range of trade facilitation and e-business standards, recommendations and tools that are approved within a broad intergovernmental process and implemented globally.

www.unece.org/cefact

Table of Contents

1. What Is Data Governance?

In an era defined by an unprecedented explosion of digital information, data has emerged as a critical asset for businesses and organizations across industries. However, the sheer volume and complexity of data can be overwhelming, making it essential to establish a framework that ensures its quality, integrity, and security. This framework is known as Data Governance.

Data Governance encompasses the policies, processes, and procedures that govern how an organization manages its data assets. It provides a structured approach to ensure that data is accurate, consistent, and aligned with organizational objectives. At its core, Data Governance is about establishing rules and responsibilities for data management.

The primary purpose of Data Governance is to empower organizations to make informed decisions, achieve compliance with regulatory requirements, and derive value from their data assets.

The purpose of this project is to look at Data Governance especially in Trade Facilitation (TF) in the context of UN/CEFACT's mandates and create a whitepaper that focuses on studying existing Data Governance and presenting best practices for existing systems that can act as a guide for future implementation.

Why Data Governance matters

Data governance is vital for organizations in today's data-driven landscape, impacting success, integrity, and sustainability. By establishing processes for data validation, cleaning, and maintenance, it ensures accuracy and reliability, crucial for informed decision-making. Compliance with data privacy regulations like GDPR and CCPA is ensured, shielding organizations from fines and legal risks.

Reliable data forms the bedrock of effective decision-making, empowered by data governance's access to accurate information and clear ownership of data sets. This fosters accountability and trust within the organization. Security protocols and encryption measures protect against data breaches and cyber threats, while streamlined processes enhance efficiency and productivity.

As a strategic asset, data governance enables organizations to extract maximum value from their data, managing its lifecycle responsibly. This prevents data decay and facilitates innovation and revenue generation. Effective data governance builds competitive advantage by enabling swift responses to market changes and fostering a culture where data is valued and respected. Collaboration is facilitated by ensuring data accessibility, promoting seamless teamwork across departments.

Key Components of Data Governance

Data governance encompasses several key components:

1. **Data Stewardship**: Assigning responsibility for data quality and integrity to specific individuals or teams within the organization.
2. **Data Quality Management**: Monitoring, assessing, and improving the quality of data to ensure accuracy and consistency.

3. **Data Security and Privacy**: Safeguarding sensitive information against unauthorized access, breaches, and cyber threats.
4. **Data Lifecycle Management**: Addressing the entire lifecycle of data, from creation to disposal.

Implementing data governance offers numerous benefits:

1. **Improved Data Quality**: Ensuring accurate, consistent, and reliable data for better decision-making.
2. **Enhanced Decision-Making**: Empowering informed choices and effective strategies.
3. **Regulatory Compliance**: Meeting legal and regulatory requirements to mitigate risks.
4. **Reduced Data-Related Risks:** Protecting against security breaches and data loss.
5. **Increased Trust and Accountability**: Building trust and fostering accountability within the organization.
6. **Optimized Operational Efficiency**: Streamlining operations and improving productivity.
7. **Maximized Data Value**: Extracting valuable insights and driving innovation.
8. **Long-term Data Sustainability**: Ensuring data remains relevant and valuable over time.
9. **Facilitated Collaboration**: Breaking down silos and enabling cross-functional teamwork.
10. **Competitive Advantage**: Responding quickly to market changes and capitalizing on opportunities.
11. **Increased Customer Satisfaction**: Understanding and serving customers better.
12. **Facilitates Data-driven Culture**: Fostering a culture where data is valued and respected.
13. **Cost Savings**: Reducing inefficiencies and preventing costly data-related incidents.
14. **Flexibility and Adaptability**: Being agile and responsive to changes in the business environment.

Data Governance & Best Practices

Data governance in trade flows is vital for ensuring efficient, secure, and compliant movement of goods and services across borders. It encompasses various aspects:

1. **Data Accuracy and Integrity**: Ensuring accurate and reliable trade-related data to reduce errors and discrepancies in transactions.
2. **Customs and Regulatory Compliance**: Providing complete and accurate data to customs authorities to expedite clearance and avoid penalties.
3. **Supply Chain Visibility**: Tracking goods throughout the supply chain for optimized logistics and quick response to disruptions.
4. **Risk Management**: Identifying and mitigating risks like trade fraud or supply chain disruptions through robust data controls.
5. **Trade Documentation and Reporting**: Ensuring accuracy and completeness of trade documents to avoid delays or disputes.
6. **Tariff Classification and Duty Calculation**: Correct classification of products to determine import duties accurately.
7. **Data Sharing and Interoperability**: Facilitating data sharing between stakeholders to improve coordination in trade flows.

8. **Data Privacy and Security**: Implementing security measures to protect trade data from unauthorized access or cyber threats.
9. **Audit and Compliance Records**: Maintaining accurate records of trade transactions for audit and compliance purposes.
10. **Trade Analytics and Optimization**: Analyzing trade data to identify trends and optimize supply chain operations.

In summary, data governance ensures that trade data is accurate, secure, and accessible, facilitating smooth trade flows while minimizing risks and compliance challenges. It enables informed decision-making and sustainable growth by harnessing the full potential of data.

2. Data Governance is Imperative in Trade Facilitation

Data Governance facilitates smooth movement of data across entities and borders. In the light of the increased cross border data flows in the context of domestic and cross-border trade along with data localization, privacy issues and guidelines, it becomes imperative to have governance related guidelines and controls in place.

There have been numerous incidents of data breach and leakages – which have put data owners at risk. Adversarial attacks on data models lead to leakage of private and classified information which is not only a privacy issue but also a socio-economic threat. An enterprise level data leakage can lead to economic and financial impact on corporations and international bodies.

Thus, data governance policies and effective controls could ensure:

- Centralized and distributed policies and systems
- Standardization of domestic and cross-border data exchange
- Meeting Compliances
- Incorporating principles of data privacy
- Implementing Cyber security through standard Information Security Management Systems

Data Governance Needed in Trade Facilitation

Recent technological advancements have reshaped international trade, rendering the use of electronic data commonplace. The COVID-19 pandemic accelerated this shift, necessitating new norms like remote work and reduced paperwork. While the private sector swiftly embraced innovative IT solutions to facilitate trade, public sector entities lag behind, struggling to adapt. The World Customs Organization (WCO) advocates for paperless customs processes, promoting the use of electronic documents to streamline clearance procedures. Similarly, the World Trade Organization (WTO) defines trade facilitation as the simplification and harmonization of trade procedures, emphasizing the role of technology in enabling faster and more efficient processes. However, for technology to be effective, trust in data integrity and system security is paramount. Despite the potential benefits, public sector institutions face challenges in adopting and managing advanced technologies, highlighting the need for greater investment in IT infrastructure and workforce development. Without trust in data and systems, enforcement agencies like Customs struggle to effectively manage trade risks.

Threats to that trust, internal and external, can only be addressed with effective data governance in place to serve as an essential role in supporting the facilitation of legitimate trade. Aspects of governance to be considered include mitigation of threats posed by **Enterprise Risk (systems)** comprising:

- Cyber Security
- Internal Integrity
- Data Quality/ Integrity risks (Trust requirements)

Enterprise Risk (Systems)

Cybersecurity is increasingly critical in maintaining data integrity and facilitating legitimate trade, especially with the rise of interconnected IT systems. The UN CEFACT White Paper on IoT Standards for Trade Facilitation highlights the challenges and the lack of universal cybersecurity standards. It suggests collaboration among stakeholders to define and implement effective security measures.

Internally, unauthorized access poses a significant risk, particularly for traders participating in programs like the Authorized Economic Operator. Data governance and regular monitoring are essential to mitigate internal threats and maintain effective trade services.

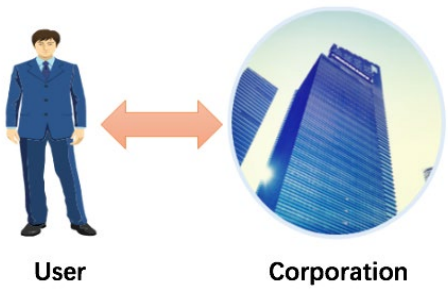
Ensuring data quality and integrity is vital for building trust in cross-border data flows. Trust anchors and other recommendations from UN-CEFACT documents address the importance of data quality and stakeholder integrity in trade processes.

While enhancing data governance improves confidence, it may complicate procedures and pose challenges, particularly for SMEs/MSMEs. Striking a balance between data governance and trade facilitation principles is crucial for sustainable progress in international trade

3. Data Governance Enables Privacy, Protection, Localization and Data Security

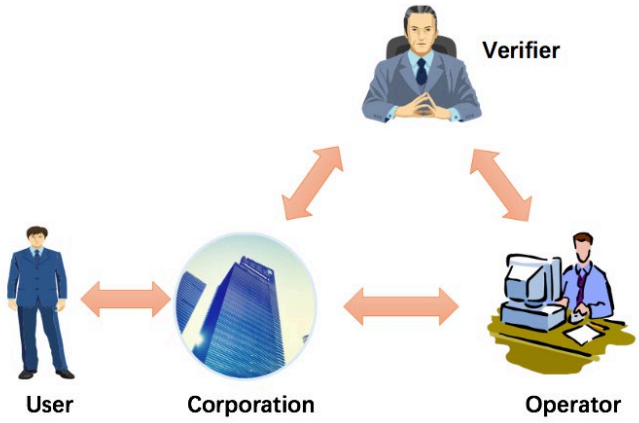
The Basic Idea of Ternary Data Governance System

In the existing business model, when users interact with enterprises or information services, all operations involving user identity authentication, user data processing and other aspects are completed in the enterprise, and users are completely unaware of whether their personal data is stored and managed safely. This model, in which the entire data processing and interaction is done entirely by the enterprise itself, is called the "unary" model, as shown in below figure.



Unary model

In order to better meet the development trend of personal data protection represented by GDPR, how to provide users with more "transparent", more "controllable" and more "secure" data management has become an urgent problem to be solved. Based on the principle of "No one can prove themselves", it is suggested that the service functions such as user identity authentication and personal data processing should be separated from the enterprise, and the corresponding functions should be undertaken by a trusted independent third party. This information service system composed of enterprise, operator and verifier is called "ternary" mode, as shown below.

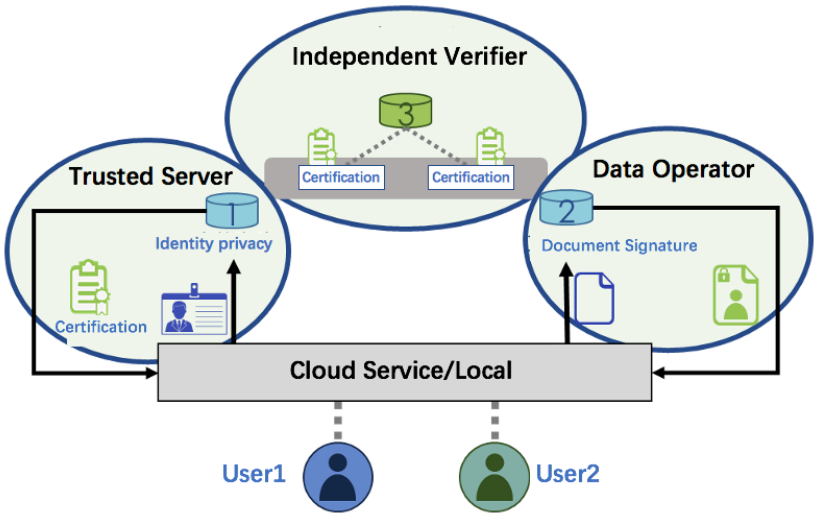


Ternary model

This ternary model can be interpreted as the "separation of powers" in the field of personal information. The essence of the three rights is to transfer part of the enterprise's right for data operation to a third party, and the addition, modification, deletion and check of user data are all handled by professional and compliant independent units, so as to avoid users' distrust of the enterprise and non-compliant operations caused by enterprises' insufficient grasp of policies. At the same time, enterprises can also rest assured to exercise the right to use data, saving manpower and material resources. The processing of user identity and compliance review is handed over to organizations with government or industry background for management and scheduling, which further avoids excessive collection and abuse of user personal information.

Architecture

The core idea of the Ternary Data Governance System divides the traditional enterprise's "unified" function into a "ternary system" composed of enterprise (trusted service providers), independent verifier and data operator. Each part performs its own duties and works closely with each other to ensure the security of data transmission, storage and distribution. Through real-time control of data, comprehensive control of data is realized, which not only meets the protection of users' rights and interests proposed by GDPR, but also meets the requirements of data controllers and processors under GDPR. The architecture Ternary Data Governance System is shown below.



Architecture

Trust Service

It is an enterprise Portal that provides services including registration, authentication, data operation, and data storage for customers and employees through interactive means. Among them, registration and authentication should be applied to the Independent Verifier through the dedicated interface, and the background processing of data operation is completed by the Data Operator through the dedicated interface. The enterprise portal can store the user's personal data, but the data is encrypted by the user's public key, and the enterprise cannot directly use it without the user's permission.

Data Operator

Also known as a Service Provider, it is undertaken by a third party independent of the enterprise. It is responsible for a series of data operations on behalf of the user in the cloud or locally, including data file creation, user key generation, file encryption and decryption, Originality identification, file modification, file deletion, file copying, consent confirmation, cancellation operation, data portability and so on.

Independent verifier (Controller)

Also known as Validation Body, it is mainly responsible for coordinating the work between the security leader and the operator, acting as a scheduler to distribute tasks and review, and responsible for user's identity authentication. To be precise, on the one hand, the controller should inform the trusted service user of the authentication method, authentication results and the contract methods abide by multi-party interaction, etc., on the other hand, the controller should conduct a compliance review of all operation processing of the operator, and after the review is passed, the operational data is written into the private blockchain through its own public key, so as to achieve the characteristics of untampered and traceable operational data.

Digital Identity System and Signature

Digital identity registration involves the issuance of officially signed digital identities, verified by a certification body, with unique registration numbers stored in a directory. These identities are crucial for authentication, licensing, signatures, encryption, and legality verification in transactions.

Authentication requires at least three elements: biometric, association with mobile devices, and public keys. Certification bodies evaluate verification mediums and assign certification levels. Two-dimensional codes enhance identity authentication.

Signature validation involves two types: unpermissioned, which renders online signatures void unless part of an agreed exchange agreement containing specific information, and licensed, requiring document verification or integrity verification.

Online management of trusted services ensures online proof based on identity documents, preventing attacks. Communication protocols are signed and have expiration dates, with data constantly updated.

Rights management involves property change, signature agent change, document/authorization management, and subsequent rights management, ensuring real-time handling according to specific needs.

Cooperative scheduling among multiple parties specifies signatory commitments and controls the situation in real-time, ensuring the validity of transactions.

Signature authentication with extended traceability ensures formal, traceable signatures submitted to independent verifiers, guaranteeing legitimacy and security. Anomalies prompt blocking or non-blocking exceptions, with traceability information returned to trusted services if no issues are found.

The Data of The Ternary Data Governance System

The "ternary architecture" feature of the Ternary Data Governance System determines that each party performs its duties and closely coordinates with each other. Data is stored and used, critical data is encrypted, transmitted, distributed, and not shared, which ensures the security of data transmission, storage and distribution from the mechanism, and realizes the localization of data governance. In addition, the Ternary Data Governance System supports localized deployment around the world, the system is deployed to a local server or computer to achieve local operation and use of the system, and the data is stored on the local server, thereby reducing the risk of data loss and leakage, and ensuring data privacy and security.

4. Data Governance Frameworks

Current Issues to Be Addressed

The global landscape of trade facilitation suffers from a lack of cohesive governance regarding data, resulting in varied approaches across countries. The United States emphasizes private sector control, China focuses on government control, and the European Union prioritizes individual control based on fundamental rights. Moreover, there is a dearth of universally agreed-upon definitions and classifications for data and its flows, leading to confusion and inconsistency.

In the midst of a data-driven digital economy, traditional concepts of ownership and sovereignty are being challenged. Questions arise regarding who owns data versus who has the right to access, control, and utilize it. Furthermore, the proliferation of national regulations on cross-border data flows introduces uncertainty and increases compliance costs, disproportionately affecting micro and small enterprises, particularly in developing countries.

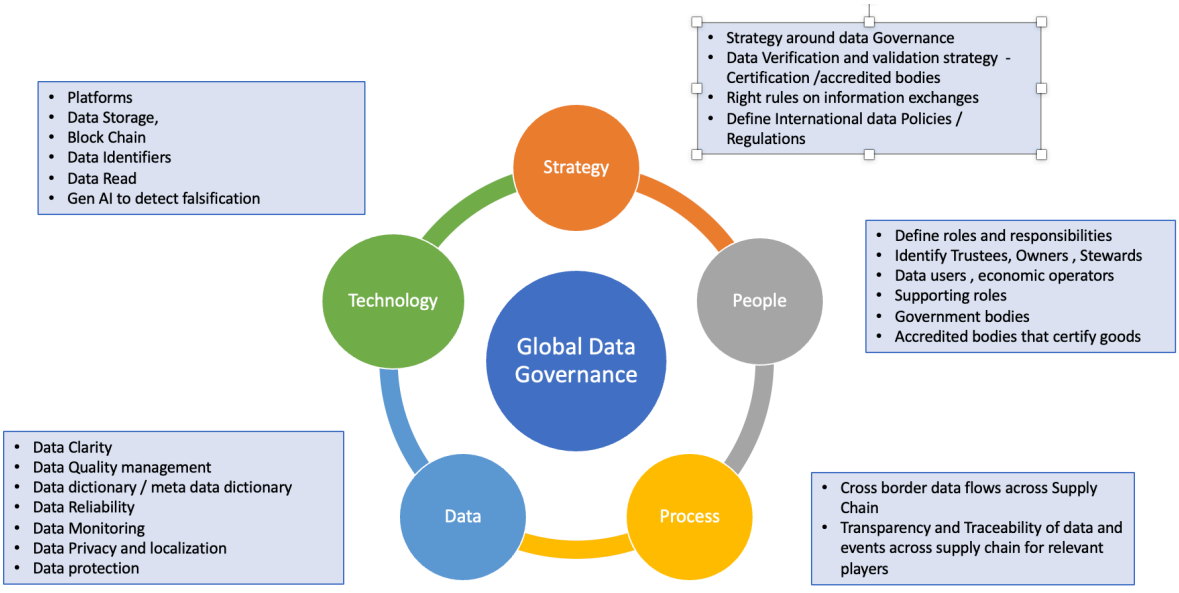
The lack of global governance over digital platforms has resulted in self-regulation by these platforms, often to their own benefit, with significant implications for development and policy. This self-regulation risks leaving developing countries as mere data providers while bearing the costs associated with digital intelligence produced using their data.

Given the intricate interdependencies and global nature of trade facilitation, the future of cross-border data flows should not be dictated solely by a handful of major countries. Such a scenario could marginalize developing countries, relegating them to mere data providers without adequate compensation for the value generated from their data.

Source: UNCTAD- G20 regulations of cross border data flow 2023 https://unctad.org/publication/g20-members-regulations-cross-border-data-flows

Global Data Governance Framework

We need to take a holistic, multidimensional, whole-of-government and multi-stakeholder approach.



Strategy:

- Strategy around data Governance
- Data Verification and validation strategy - Certification /accredited bodies
- Right rules on information exchanges
- Define International data Policies / Regulations
    - Centralized and distributed data governance policies
    - Data privacy policies [e.g. GDPR]

- Policies to define when data breach occurs cross boarder data exchange
- Hard wired accountability between nations – data leak while flowing between countries. Who will be held accountable?
- Future proofing of the policy environment

People:

- Define roles and responsibilities
- Identify Trustees, Owners, Stewards
- Data users, economic operators
- Supporting roles
- Government bodies
- Accredited bodies that certify goods

Process:

- Cross border data flows across Supply Chain
  - Data available to all or on demand
  - Start points / end points
  - Document control
  - Data interoperability
  - Data security – data altering – data original state persisted or illegally changed
  - Data purpose retention
- Transparency and Traceability of data and events across supply chain for relevant players

Data:

- Data Clarity
- Data Quality management
- Data dictionary / meta data dictionary
- Data Reliability
- Data Monitoring - Strengthening the measurement of the value of data and cross-border data flows
- Data Privacy and localization
- Data protection

Technology:

- Platforms
- Data Storage,
- Block Chain
- Data Identifiers
- Data Read
- Gen AI to detect falsification

Data Management Governance Stack

Roles	Definitions

Policy Declarations	Stated policies that span not only data but systems and processes that impact it
Policy Makers	Trustees who create policies that are used to manage data within an enterprise. They may be a group of trusted individuals who legislate policies
Policy Enforcers	These are Stewards of data, processes, and custodians of systems responsible to enforce the legislated policies
Policy Facilitators	Individuals, systems, processes, documents, and organizations that facilitate the communication and enforcement of policies
Policy Audience	Ones who follow data policies including data creators, consumers, and observers

Data Stewardship and Governance

Recommended Operational Guidelines:

- Incorporate Data Governance across supply chain
- Implement Governance through business process changes
- Monitor/audit representative sampling(s) of data periodically
- Maintain currency of data definition, policies, Stakeholder Inventory
- Create Operating Committee(s) for consensus building
- Create Governance Council(s) and/or Steering Committee(s)
- Determine and develop escalation paths, as necessary
- Engage with other domestic as well as cross-functional teams and in-theatre partners
- Monitor data origin across TF – Watermarking should be there to identify origin of info
- Keep up to date with data consumers downstream from you
- Health Check: score and re-certify data annually
- Meta data embedded for traceability of info source
- Catch falsification – AI to detect

5. Data Governance Best Practices

ZIIOT (Zhongguancun Gongxin Two-dimensional Code Technology Research Institute) was jointly approved by three international organizations of the International Organization for Standardization (ISO), the Commission for European Normalization (CEN), and the Association for Automatic Identification and Mobility (AIM) in 2018 to be responsible for the management and maintenance of ISO/IEC 15459 series international standards of MA International Identification Code System and have the right to distribute code globally. MA International Identification Code System can assign the world's only digital identities to tangible and intangible objects in both the real and virtual worlds, such as people, things, objects, data, etc. which is safe, compatible, and international.

Data Aggregation Practice Cases

Technologies such as data infrastructure overlay identification coding can efficiently access, credibly register, and accurately confirm rights for multi-source and multi-dimensional data, effectively improving the universality, convenience, and accuracy of data convergence. Relevant government departments in various countries have promoted the application of identification coding in data aggregation to improve management and service efficiency.

During the COVID-19 pandemic, the health code travel system emerged as a vital tool for digital epidemic prevention and control, swiftly gaining global adoption for its convenience and efficiency. Even post-pandemic, cities like Shanghai and Nanchang in China have explored integrating health codes into broader city and citizen code systems to continue offering convenient services to residents.

In China, the National Drug Administration has been championing the use of unique ID codes to enhance traceability in various sectors, including drug tracking, medical device management, and support during public health emergencies. ZIIOT has been designated as the authority for issuing unique identification codes for medical devices, ensuring professional and standardized coding services.

To regulate industrial Internet identification coding services, the Ministry of Industry and Information Technology implemented measures, enabling ZIIOT to serve as a registration authority for industrial Internet identification. This move aims to standardize and streamline coding services in this sector.

Furthermore, the Ministry of Natural Resources in China is actively advancing the construction of a 3D representation of China in the metaverse. This initiative utilizes the MA coding system to establish unique identities for geographical entities, facilitating seamless information sharing globally. By improving the efficiency of data organization, processing, and analysis, this effort lays the groundwork for a digitally empowered "Digital China."

Practical Cases of Data Confirmation

Data confirmation and validation is the basis of data governance, and the first premise of data validation is to uniquely encode data globally and identify the source of data.

China's strides in industrial data management are exemplified by initiatives such as the China Industrial Internet Research Institute's establishment of an industrial data asset registration platform. This system facilitates registration, evaluation, trading, and cross-border functions, ensuring the uniqueness of industrial data element identities globally. Currently

encompassing major sectors like textiles, glass, and machinery and equipment, the platform has issued over 387 registration certificates, covering more than 530 million valid data values.

Moreover, China's renowned data center, People's Network People's Data, achieved a significant milestone on 12 December 2023. Their "Data Element Identification System" was officially integrated with the MA International Identification Code System. Leveraging internationally certified MA International Identification Codes and advanced technologies, this collaboration aims to enhance the credibility of the data element identification system. It endeavors to enrich the data element "Periodic Table," providing a comprehensive data ID card. This system serves customers in diverse areas such as data storage, confirmation, trading, and consulting. By establishing a robust data identification infrastructure, it aims to catalyze the socialization and value realization of data elements.

Data Security Governance Practices

Data security is the basic guarantee of effective data management. Through the combination of coding and blockchain technology, and relying on the characteristics of traceability, immutable, incentive and multi-party cooperation of blockchain, IDChain Global Technology Co., Ltd. and other units have built a data security governance architecture based on the "identification code + trusted blockchain" code chain integration technology. Based on which people can design key technologies such as reliable data collection, data security sharing & exchange, data access control and data behaviour storage, and can ensure the authenticity and reliability of data before going online and the immutability of data after going online, thus people can achieve the uniqueness, security and sharing of data both on and off the chain, and ensure the security of data management.

Practical Cases of Data Governance in The Field of Smart Cities

Nanhai District in Foshan City, China, is leveraging mobile Internet, two-dimensional codes, big data, and artificial intelligence to enhance urban management through its Nanhai Urban Brain Project. Using the MA International Identification two-dimensional code system, the district is constructing detailed information on "management facilities, responsible entities, and management areas." This facilitates various applications such as code-based data queries, collection, business management, assessment, and citizen participation. By adopting a collaborative model involving urban management departments, social responsibility subjects, and citizens, Nanhai has elevated its urban governance effectiveness.

In Tibet, the "Zangyi Tong" app is also utilizing the MA International Identification Code System along with big data, artificial intelligence, and cloud computing to support the region's economic recovery and daily mobility needs. Its implementation has significantly contributed to the resumption of work and production as well as facilitating everyday travel. The app's integration into urban construction initiatives is promoting data governance and fostering scenario-based big data analysis capabilities. Additionally, it facilitates the sharing of government data across different levels, regions, and departments, unlocking the value of data and enhancing the overall modernization of urban governance systems and capacities.

6. Domestic and Cross Border Data Flow and Governance

In a world where data has become akin to physical goods, flowing freely across geographies and with few constraints, new jurisdictional restrictions on data flows present tensions and challenges. Governments have come to recognize that data holds not only economic value but also strategic significance, leading to the implementation of regulations that limit and govern its exchange.

We now find ourselves amidst a digital cold war involving three different systems called the "Three Digital Kingdoms." These regulations are exerting an impact on data transfers ultimately influencing global trade in goods and services. These restrictions appear to be at odds with the UN/CEFACT principles designed to facilitate international trade and foster seamless business transactions. Consequently, the transfer of data has grown increasingly intricate and burdensome. What lessons can we learn from companies adept at successfully navigating global data transfers, and might there be an alternative approach to data sharing and trade facilitation better suited to the digital economy?

What is Data Transfer

The pace at which data is being generated is nothing short of astounding, with a remarkable 90% of the world's data having emerged in just the past two years, doubling every two years thereafter. This surge in data flow, occurring both domestically and across borders, is a hallmark of the ongoing digital transformation. Whether it's termed domestic transfer within a country or cross-border transfer between nations, data exchange mirrors the movement of physical goods, playing a pivotal role in global trade and production.

Data has become the lifeblood of international commerce, facilitating the coordination of global value chains and enabling small enterprises to tap into global markets through platforms like cross-border e-commerce. Its importance is underscored by its contribution to the global GDP, estimated at $2.8 trillion currently and projected to soar to $11 trillion by 2025, according to OECD figures.

Financial services epitomize the value derived from data transfers, particularly in cross-border payments where insights gleaned from customer data inform tailored offerings and enhance customer experiences. By analyzing extensive data repositories, financial institutions uncover valuable insights into customer preferences and behaviors, enabling the design of products, anticipation of needs, and better risk management. Ultimately, the rapid exchange of data underpins the entire process, driving innovation and efficiency across sectors.

Let's consider another illustration: cloud services. Cloud platforms grant small and medium-sized enterprises (SMEs) access to essential IT services, diminishing the necessity for substantial initial investments in digital infrastructure. For instance, Amazon Web Services (AWS) provides this capability to clients worldwide. Enhanced and swifter access to crucial knowledge and information empowers SMEs to surmount informational gaps. Consequently, this lowers obstacles to participating in international trade and equips them to compete more effectively with their larger counterparts.

Multinational corporations heavily rely on data flows for their day-to-day operations, utilizing information from their global affiliates for various internal tasks and decision-making processes. This includes transferring human resources data, conducting research and development across borders, overseeing production procedures, and providing post-sale services. ADP, a global provider of cloud-based human capital management solutions,

exemplifies this reliance, offering services like HR, payroll, and tax management to clients worldwide.

Cross-border data transfers have also facilitated the rise of micro-SMEs, particularly through platforms like Amazon and Alibaba's Taobao, allowing small businesses to attain international reach by exchanging product and customer data globally. This has led to the emergence of "micro-multinationals," firms that operate globally from inception. China's cross-border e-commerce market, valued at $306.3 billion in 2022, illustrates the significance of such data-driven trade in driving the nation's foreign trade development.

Data exchange is central to various sectors, including financial services, e-commerce, logistics, manufacturing, and agriculture, accounting for about 75% of the total global data value. The increasing recognition of data as a strategic asset, akin to physical goods, is evident, with The Economist and the World Economic Forum highlighting data as the world's most valuable resource. However, unlike tangible goods, the value of data is not quantifiable in units but lies in its ability to improve lives through efficiency gains, product enhancements, consumer appeal, expanded choices, and innovation. Companies and nations that effectively harness their data stand to gain significant advantages in today's data-driven marketplace.

Consumers Privacy and Regulations

Companies that harness data often benefit from what's termed a "data feedback loop," where the accumulation of user data leads to product improvement and user growth. Tesla exemplifies this with its expanding fleet worldwide, gathering data for product enhancement. However, not all data benefits everyone equally, and its unrestricted flow poses challenges. Technologies like IoT and AI collect vast data, raising concerns over sensitivity and transfer restrictions.

Tesla's case in China, where data localization is mandated, illustrates this. Similarly, Apple complied with data storage requests to access the Chinese market. Excessive data accumulation, sensitive data handling, and privileged access pose economic concerns like inequality and market dominance.

UNCTAD notes that nations with diverse, high-quality data can reap significant benefits. Yet, privacy, regulation, and trade constraints are critical. Trust in digital operations is pivotal, as data accumulation threatens privacy. Privacy protection is increasingly vital for consumer trust and business integrity.

Balancing data flow with privacy and security is paramount amidst digital transformation. Governments enact data regulations, with most countries implementing privacy laws and data transfer restrictions. These regulations vary across cultures, addressing personal data, sector-specific data, and emerging categories like "important" data.

Different Types of Approaches

The global landscape of data privacy regulation is heavily influenced by the European General Data Protection Regulation (GDPR). European data privacy laws set a precedent for international data transfers, requiring compliance mechanisms like data adequacy and standard contractual clauses. This model has been adopted by countries within and outside of Europe, shaping regulatory provisions worldwide. The United States takes a contrasting

approach, initially allowing data transfers without strict restrictions, while China adopts a similar regulatory stance to Europe but with more rigorous standard contractual clauses.

There are four main approaches to regulating cross-border data flows globally: absence of regulation, post-transfer accountability, adequacy determination, and case-by-case approval. These approaches vary in their level of regulation and accountability for data transfers. Local storage mandates also play a significant role, requiring data to be stored within specific geographic regions. These mandates range from sector-specific storage requirements to more stringent restrictions on data flow and processing.

Regarding data transfer mechanisms between Europe, China, and the USA, the EU-U.S. Data Privacy Framework replaced the Privacy Shield in July 2023, allowing personal data transfers from the EU to participating U.S. companies without additional protection measures. In China, data protection regulations have distinct characteristics, including stringent privacy safeguards alongside state access to data for national security reasons. From June 2023, Chinese companies have a grace period to comply with procedures for transferring personal data abroad, including signing standard contractual clauses.

Governance and the "Three Steps Approach"

Given the diverse regulations and systems governing data transfer globally, one effective approach is to examine the existing strategies and best practices employed by companies engaged in international data transfers. By identifying common elements among these practices, it is possible to create a reference guide or handbook to navigate this dynamic landscape effectively. This handbook can serve as a valuable resource for staying informed and compliant in an ever-evolving field.

Many companies operating in multiple countries encounter a variety of challenges related to cross-border data transfers. As discussed earlier, these challenges encompass different localization requirements, such as data residency rules and compliance standards, and may even necessitate obtaining regulatory permissions in some cases. Further complications arise when considering onward transfers of data, where data move from one jurisdiction to another, making it challenging to track its origin. Additionally, determining which laws apply and the extent of territorial jurisdiction can be highly complex, especially when it comes to classifying data types and determining the appropriate legal framework. To navigate this complexity, companies require a well-structured plan aimed at simplifying, standardizing, and harmonizing their data transfer processes. In other words, what cannot be achieved through harmonizing regulations, might be achieved through a good plan.

It's insightful to examine how multinational companies like Amazon, Hertz, and ADP, as well as regional SMEs, address the intricate challenge of cross-border data transfers. These companies deal with vast amounts of sensitive data, and their approaches can provide valuable lessons. ADP, which offers human capital management and payroll services worldwide, has established a robust privacy program to safeguard clients' sensitive data, including employee salaries and health records[1]. AWS provides global cloud services, supporting numerous businesses with data storage[2]. AWS adopts a model where customer data remains in the region specified by the client, ensuring data doesn't cross regions. AWS itself doesn't have visibility into the specific data customers store in the cloud. Hertz, a global

[1] ADP.com
[2] AWS.com

car rental company, handles extensive data transfers, including customers' personal information and geolocation data, as well as internal data from its subsidiaries and franchisees worldwide[3].

These companies follow a "Three Steps Approach" to tackle the complexities of data transfer, which involves:

Data Discovery	Building a Regulatory Framework	Data Governance
Identifying and categorizing data	Ensuring data is stored and processed in compliance with relevant local laws and regulations	Implementing robust governance frameworks to manage and protect data throughout its lifecycle, from collection to disposal

This approach helps these companies effectively navigate the challenges associated with cross-border data transfers and maintain data security and compliance on a global scale.

Step 1: Data Discovery and Mapping The initial step in crafting a robust data transfer plan involves conducting comprehensive data discovery and mapping. This process requires engagement from all stakeholders within the organization to grasp the nature of the data held, its collection methods, and its flow across the company and its subsidiaries. Achieving visibility into the data landscape is pivotal for subsequent planning efforts. Tools like AWS assist in this process by aiding in data discovery, pinpointing data locations, trajectories, and suggesting technical safeguards like masking and encryption.

ADP, for instance, leverages data discovery and analytics to understand its data landscape when transferring data across subsidiaries. Separating internal from external data is crucial. The development of a risk metric follows, assessing governance, financial, and reputational risks. For companies like Hertz, dealing with diverse data types, constructing a risk matrix is essential to manage data effectively.

Step 2: Establishing a Regulatory Framework Each company must establish and maintain an updated repository of global privacy laws relevant to its operations to ensure compliance. Collaboration with various internal teams is vital during this step. ADP, for example, initiated this by implementing binding corporate rules (BCR) to address data transfer rights, establishing a comprehensive privacy program. Critical questions regarding data processing, access control, and notification requirements are addressed during this phase.

Step 3: Implementation and Feedback Collection In this phase, the company decides on the execution of policies globally and establishes mechanisms for ongoing monitoring and feedback collection. Companies may adopt either a centralized or decentralized approach. A

[3] Hertz.com

continuous feedback mechanism is crucial for refining the program. ADP conducts compliance audits annually to gather feedback.

Restrictions On Cross-Border Data Flows and Localization

Restrictions may be implemented by governments at all levels and take different forms (*e.g.*, outright bans on cross-border transfers or allowable flows based on conditions). Such measures are enacted for a variety of reasons, including national security; cybersecurity; citizen data protection and privacy; and 'digital protectionism'.[4]

Similarly motivated, as a separate type of measure, localization is broadly defined by regimes that lead to more local data storage than would otherwise be the case (*i.e.*, in *lieu* of the measure in question).[5] Debate surrounds whether data localization should only include 'explicit measures' or if it should also include 'implicit measures'.

In the first case, an Organisation for Economic Co-operation and Development (OECD) study understands data localization as an "explicit requirement that data [*e.g.*, personal data] be stored and/or processed within a domestic [or otherwise specified] territory".[6] Legally defined by jurisdiction and framework, approximately 100 explicit measures for data localization were implemented across 40 countries as of late-2023.[7]

In the second case, data localization is used to refer to the explicit location of data storage and processing *as well as* implicit restrictions[8] on cross border data flows. For example, the GDPR leads to more local storage by setting legal conditions for cross-border data flows but does not mandate local storage.

Whether restrictions on cross-border data flows or explicitly for data localization, these measures impose requirements on public and private actors in discrete ways.[9] Sub-national, national, and supranational sources of law may refer to the physical 'location' of data, especially through industry/sector-specific laws (*e.g.*, telecommunications laws, regulations on cloud computing, financial regulations, and laws for health and government data), or to cross-border transfers. International sources (*e.g.*, treaties) have traditionally emphasized a ban on imposing requirements for the physical location of data centres and computing facilities (with exceptions).[10]

---

[4] Aaronson, S., "What Are We Talking about When We Talk about Digital Protectionism?", *World Trade Review,* 18(4), pp. 541-577 (2019). Available at: https://doi.org/10.1017/S1474745618000198.

[5] Based on communication with Javier López González, leading data governance expert at the OECD.

[6] Measures for data localization are increasing in prevalence and restrictiveness, see Del Giovane, C., Ferencz, J. and López González, J., "The Nature, Evolution and Potential Implications of Data Localisation Measures" *OECD Trade Policy Papers*, No. 278, OECD Publishing, Paris (2023). Available at https://doi.org/10.1787/179f718a-en.

[7] Ibid.

[8] In extreme cases, a tariff that is high enough to induce 'tariff jumping' Foreign Direct Investment (FDI) would lead to more local storage than otherwise necessary and could therefore be considered as a 'data localization' measure. Tariff-jumping refers to FDI that enables a foreign firm to avoid a trade barrier (*e.g.*, a tariff) by locating production within the destination market. See Blonigen, B., Tomlin, K., and Wilson, W., "Tariff-Jumping FDI and Domestic Firms' Profits", *The Canadian Journal of Economics*, 37(3), pp. 656-677 (2004).

[9] See World Economic Forum, "From Fragmentation to Coordination: The Case for an Institutional Mechanism for Cross-Border Data Flows – White Paper" (2023). Available at https://www3.weforum.org/docs/WEF_From_Fragmentation_to_Coordination_2023.pdf.

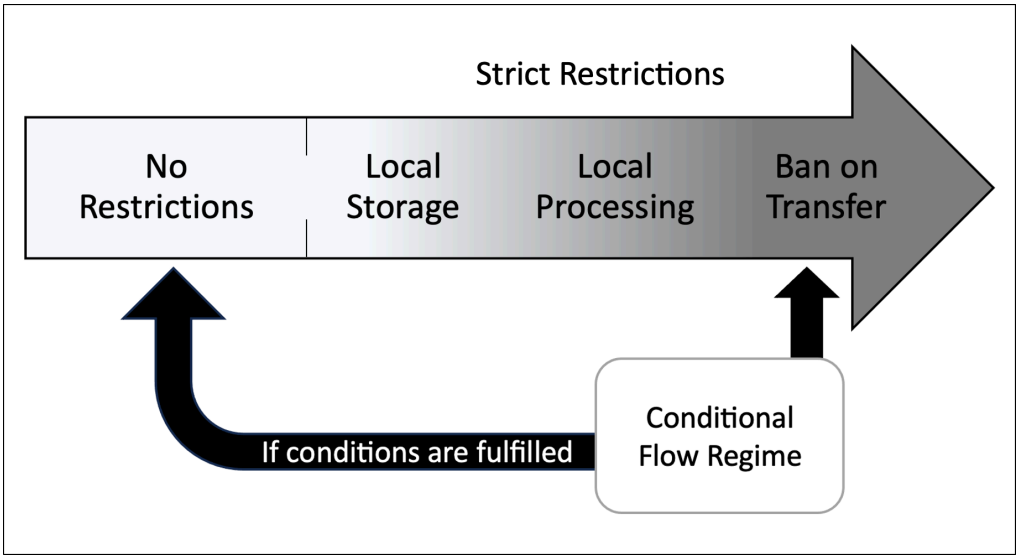
[10] See López González J., Casalini F. and Porras J., "A Preliminary Mapping of Data Localisation Measures", *OECD Trade Policy Papers*, No. 262, OECD Publishing, Paris (2022). Available at https://doi.org/10.1787/c5ca3fed-en.

Although measures are heterogenous, Ferracane (2017) provides a generalized taxonomy of 'strict' and 'conditional' restrictions on cross-border data flows.[11]

Using this taxonomy, the category of strict restrictions includes measures that create local data storage requirement(s); measures for both local data storage and processing requirements; and measures that ban cross-border data transfers (*i.e.*, local storage, processing, and access only).

The category of conditional restrictions on cross-border data flows designates regimes where conditions apply to a recipient country government or to where conditions apply to a 'data controller' or 'data processor'.[12] If these conditions are fulfilled, data may flow or be transferred subject to the data controller maintaining a set of practices to ensure continued protection of the data. If conditions are not met, there is a resultant ban on transfer.

Taxonomy of restrictions on cross-border data flows (From most to least restrictive):[13]



Moreover, *who* decides whether the conditions are met (or not) matters. For instance, compliance costs will vary if a government decides on conditionality (*e.g.*, an 'adequacy decision'[14] under EU data protection law) as compared to if a business itself determines whether a transfer is adequate.

[11] As opposed to 'unconditional' or no restrictions. For more details on the taxonomy, see Ferracane, M., "Restrictions to Cross-Border Data Flows: A Taxonomy", *ECIPE Working Paper*, No. 1 (2017). Available at https://ecipe.org/publications/restrictions-to-cross-border-data-flows-a-taxonomy.

[12] Example definitions of various data roles/actors are provided in chapter *7. Various Laws Around Data Governance*.

[13] Adapted from Ferracane (2017). See also World Economic Forum, "Exploring International Data Flow Governance: Platform for Shaping the Future of Trade and Global Economic Interdependence" (2019). Available at https://www3.weforum.org/docs/WEF_Trade_Policy_Data_Flows_Report.pdf.

[14] An adequacy decision is, "a formal decision made by the EU which recognises that another country, territory, sector or international organisation provides an equivalent level of protection for personal data as the EU…", see https://ico.org.uk/for-organisations/data-protection-and-the-eu/data-protection-and-the-eu-in-detail/adequacy.

As not all local storage requirements refer to flow conditions,[15] Casalini, López González, and Porras (2022) describe three broad categories of explicit data localization measures: local storage requirements where copies of data may be transferred and processed abroad; local storage requirements with transfer or processing of data abroad under defined conditions; and restrictions that require local storage and processing as well as prohibitions of transfers abroad (with *ad hoc* exceptions).

As the most restrictive category, over two-thirds of measures that are presently implemented combine local storage requirements with data flow prohibition.[16]

Ultimately, data flow conditions and local storage requirements meet at the extremes. That is, a fully local storage condition implies that transfers abroad are not allowed. At the same time, a full prohibition of data flows implies local storage.

Restrictions on the cross-border flow of data can be further classified as either 'industry/sector-specific' or 'cross-cutting'. Whereas industry/sector-specific measures apply to certain types of data in the context of a particular sector (*e.g.*, health data) or on an industry-wide basis (*e.g.*, banking, financial services, and electronic payments), cross-cutting measures include more than one (*e.g.*, personal or non-personal data irrespective of the sector).[17] Whether industry/sector-specific or cross-cutting, restrictions on cross-border data flows can increase compliance costs for private actors and complicate public implementation and administration of measures for trade facilitation.

While data localization represents a '*sui generis*',[18] regimes are either imposed or limited/banned through a variety of sources of law and may also include requirements for governments to provide instruments to enable transfers.[19] Notably in the context of international economic law, data flows and localization feature as a topic in preferential trade agreements (PTAs), 'Digital Economy Agreements' (DEAs), other international negotiations (*e.g.*, at the OECD and G20), and through multilateral and plurilateral dialogue under the World Trade Organization (WTO) Work Programme on E-commerce and the Joint Initiative (JI) on E-commerce, respectively.

7. Various Laws Around Data Governance

After connecting data governance concepts with UN/CEFACT deliverables, articulating technical best practices, and exploring data flows, this white paper also recognizes various sources of law.

While certain sources may not have an obvious impact on trade facilitation (*e.g.*, privacy laws), they can include language to affect the utilization of data-driven (or enabled) technologies[20]

[15] Thus, for analytical purposes, it is practical to examine restrictions on data flows and measures for localization as separate issues.
[16] See Del Giovane, C., Ferencz, J. and López González, J. (2023).
[17] Ibid. See also Svantesson, D., "Data localisation trends and challenges", *OECD Digital Economy Papers*, No. 301, OECD Publishing, Paris (2020). Available at https://doi.org/10.1787/7fbaed62-en.
[18] Referring to an independent legal classification, see Cornell Law School Legal Information Institute (LII), "sui generis" (Last updated August 2021), available at https://www.law.cornell.edu/wex/sui_generis.
[19] For example, sources like the EU-UK Trade and Cooperation Agreement (TCA) and instruments such as 'Binding Corporate Rules' (BCRs) for inter-firm cross-border transfers of personal data.
[20] For a taxonomy of legal issues surrounding technologies, including artificial intelligence (AI) and blockchain/distributed ledger technology (DLT), see United Nations Commission on International Trade Law (UNCITRAL), "Taxonomy of legal issues related to the digital economy", UN Publications, Vienna (2023).

when approaching the simplification, harmonization, modernization, and delivery of measures for paperless and cross-border paperless trade.

This guidance material comes at a pivotal time, as the adoption of laws around data governance is accelerating. Worldwide, the Digital Policy Alert (DPA) documented more than 2,000 data governance-related legal developments between 2020 and the end of 2023 (with new laws proposed daily in G20 countries and Europe, on average).[21]

Likewise, according to the United Nations Global Survey on Digital and Sustainable Trade Facilitation, the implementation of measures for 'digital trade facilitation'[22] is on the rise. The result is a fast-moving legal environment and a diverse body of sources applicable to goods trade transactions intermediated by digital technology.

Given the micro and macro implications of data governance, some sources of law widen the conventional scope of trade facilitation beyond business and government interaction to include end consumers, intermediary platforms (*e.g.*, e-commerce platforms), and other digital services/solutions providers.

Distinct categories of sources exhibit overlap in their coverage and are applicable at different levels (*e.g.*, sub-national, national, supranational, and international) and across branches of the law (*i.e.*, both public and private sources, including 'non-law' guidelines or technical standards):

- Digital and Data Governance-specific Law
- International Digital Economy, Trade, and Customs Law
- Electronic Transaction, E-commerce, and Consumer Protection Law
- Cybersecurity and Data Security Policy
- Personal Data Protection and Privacy Law
- Intellectual Property Rights (IPRs)
- Industry and Sector-specific Law
- Private Contracts, Guidelines, and Standards

Characteristics of Legal Sources

Within categories, there is significant variation between laws and rates of adoption under different legal systems (*e.g.*, disparate common law and civil law countries).[23] Sources of international law take binding ('hard law') or non-binding ('soft law') forms.[24]

Available at https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/digitaleconomytaxonomy.pdf.

[21] See the Digital Policy Alert (DPA) Activity Tracker, available at https://digitalpolicyalert.org.

[22] Previously known as 'electronic trade facilitation'. For insights on categories of measures for 'paperless trade' and 'cross-border paperless trade', see United Nations, "Digital and Sustainable Trade Facilitation: Global Report 2023" (2023). Available at https://www.untfsurvey.org/files/documents/report-digital-sustainable-2023-global.pdf.

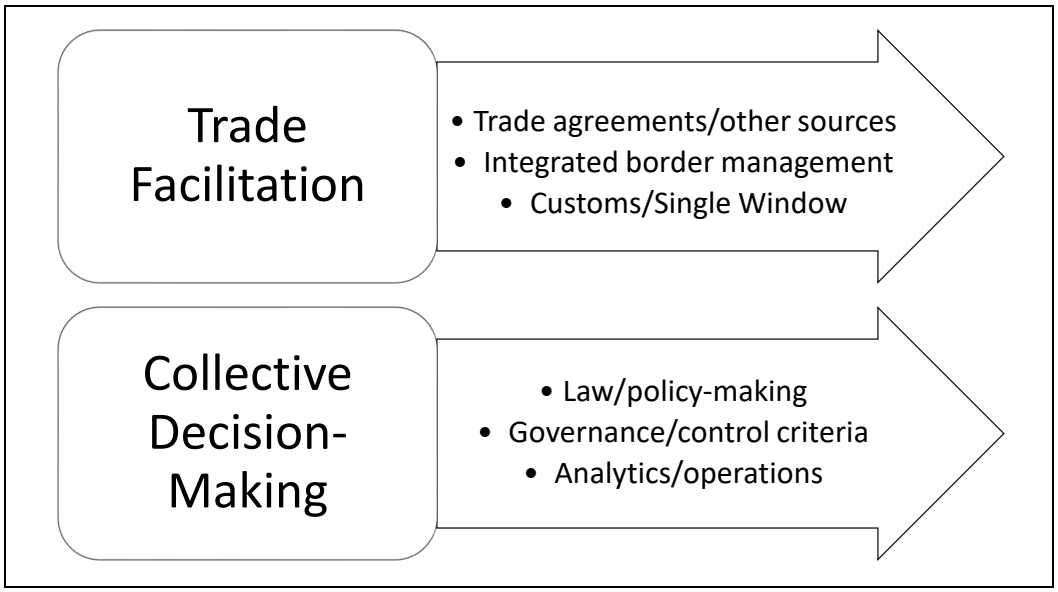
[23] Currently, many sources originate from common law countries, yet civil law jurisdictions are in the process of implementing applicable laws. For example, the 2023 report "Speeding up the Digitalisation of Trade Finance" gives insight on the promulgation of legal recognition of electronic commercial data and transferrable records in France, available at https://www.scribd.com/document/679738367/Speeding-up-the-Digitalisation-of-Trade-Finance.

[24] See Kenneth, A. and Snidal, D., "Hard and Soft Law in International Governance", *International Organization,* 54(3), pp. 421–456 (2000). Available at https://doi.org/10.1162/002081800551280.

For example, new-age 'comprehensive' preferential trade agreements (PTAs) – such as the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) – and 'Digital Economy Agreements' (DEAs)[25] – like the Digital Economy Partnership Agreement (DEPA) – often contain provisions that are the primary focus of other categories of sources (*e.g.*, data flows, cybersecurity, electronic transactions, e-commerce, and intellectual property) with varying binding and non-binding commitments.

Under the supranational framework of the European Union (EU), laws with direct or indirect coverage related to data governance take several forms, including *regulations* (binding legislative acts), *directives* (member countries decide how to transpose these EU aspirations in their national legal frameworks), *decisions* (binding where applicable), and *recommendations* (non-binding).[26]

Data governance for trade facilitation and collective decision-making:[27]



Aside from the traditional actors involved in goods trade transactions, transportation, and compliance, laws concerning data routinely assign roles and responsibilities to new legal actors (*i.e.*, 'persons' or 'subjects)'.[28] The United Nations Commission for International Trade Law (UNCITRAL) describes six actors and roles with potential for overlap: data generator, data subject, data provider, data recipient, data controller, and data processor.[29]

Legal actors: Identifying data roles and responsibilities:[30]

[25] Warren, M. and Ziyang, F., "Digital economy agreements are a new frontier for trade – here's why", World Economic Forum (2022). Available at https://www.weforum.org/agenda/2022/08/digital-economy-agreements-trade. See also M. Burri, M. Callo-Müller and Kugler, K., "The Evolution of Digital Trade Law: Insights from TAPED" *World Trade Review* available at https://doi.org/10.1017/S1474745623000472.
[26] See European Union, "Types of legislation", available at https://european-union.europa.eu/institutions-law-budget/law/types-legislation_en.
[27] Source: Adapted by chapter author, Craig Atkinson, from Peteva, J., "Data Governance and Customs Knowledge Management" presentation to the World Customs Organization (2019).
[28] In international law, 'legal persons' may be primary (*e.g.*, states and international organizations) or secondary (*e.g.*, businesses and individuals).
[29] See UNCITRAL (2023).
[30] Source: Ibid.

Role	Definition
Data generator	Person who generates data, including via of a machine or sensor.
Data subject	Person to whom data relates, whether a 'legal person' or 'natural person'.[31]
Data provider	Person who provides data to another person. Depending on the transaction, the data provider may be the data generator, data subject or data controller.
Data recipient	Person who receives data from another person, including by gaining access to the data shared on an online platform. Depending on the transaction, the data recipient may be the data processor or data controller.
Data controller	Person who 'holds' data or 'controls' how it is processed.
Data processor	Person who processes data, which encompasses almost all other roles, but often refers to persons in 'contradistinction' to the data controller. The data processor may be a platform operator.

Data-specific legal principles[32] and contracts[33] are commonly used to structure private relationships between actors, such as terms to cover liability issues (*e.g.*, data breaches), and for the extraterritorial application of public laws. For instance, private contractual mechanisms – whether standard contractual clauses (SCCs), model contractual clauses[34] (MCCs), or intra-firm Binding Corporate Rules (BCRs) – under certain data protection laws and international regimes may allow, in part, for cross-border transfer, storage, access, and processing.[35]

As 'non-law' sources, guidance texts (*e.g.*, data management frameworks, cybersecurity practices, *etc.*) and industry or technical standards can also have legal implications for data governance in the context of trade facilitation. For example, standards exist for adherence with data protection laws through privacy-enhancing technologies (PETs). Organizational-level systems for data protection and privacy protection may follow standards like ISO/IEC 27001 'privacy information management system' to support measures for digital trade facilitation.

Aligning Data-related Frameworks with the Implementation of Single Windows

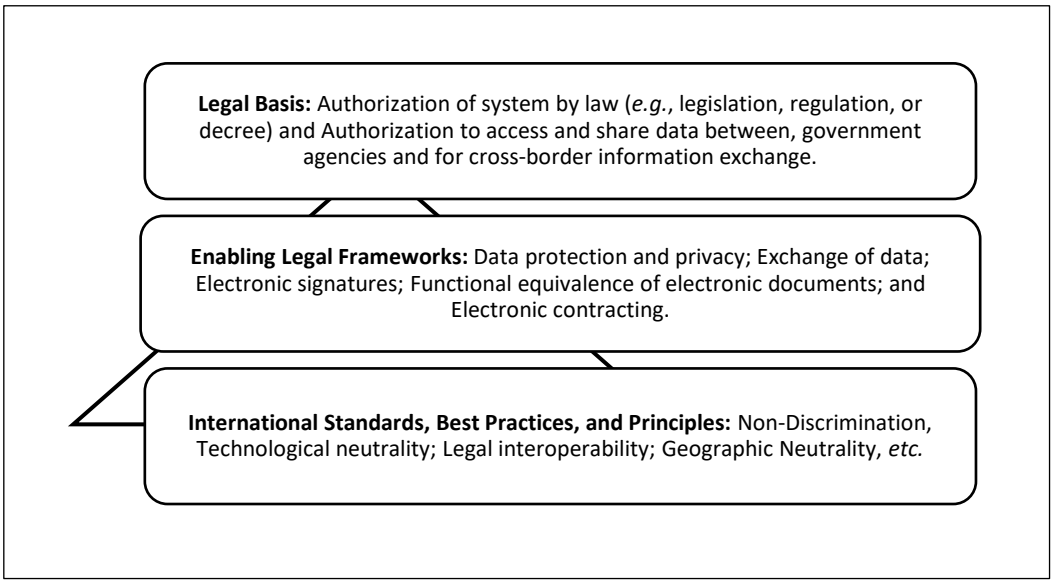
Alignment between sources of law (and non-law sources) is vital for the success of digital public infrastructure[36] (DPI) projects. The implementation of electronic single window systems

[31] See Adriano, E., "Natural Persons, Juridical Persons and Legal Personhood", *Mexican Law Review,* 8(1), pp. 101-118 (2015).
[32] While not the focus of trade facilitation, these also include principles for 'trade in data'. For example, see American Law Institute-European Law Institute, "ALI-ELI Principles for a Data Economy" (2022), available at https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ALI-ELI_Principles_for_a_Data_Economy_Final_Council_Draft.pdf.
[33] Often classified by the role(s) of parties (*e.g.*, 'data provision' contracts, 'data processing' contracts, *etc.*).
[34] See European Commission, "Model clauses around the world", available at https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en.
[35] Processing may refer to a range of operations, including "collecting, recording, organizing, structuring, storing, adapting or altering, retrieving, transmitting, aligning or combining, and restricting, erasing or destroying. One or more of these operations may constitute 'accessing', 'sharing', 'using' or 'disclosing' data", see UNCITRAL (2023).
[36] See United Nations Development Programme (UNDP), "The DPI Approach: A Playbook" (2023). Available at https://www.undp.org/digital/digital-public-infrastructure.

depends on a multilayered legal basis (*i.e.*, law establishing a system), government adoption and enforcement of enabling legal frameworks for data (*e.g.*, UNCITRAL model laws), and adherence to standards.

Supplemental legal guides are valuable resources for system implementations (*e.g.*, UN/CEFACT Recommendation 35)[37] on legal elements for implementing a single window.[38] The recently published Single Window Assessment Methodology (SWAM) also includes a section on institutional governance and legal frameworks.[39]

Data-related requirements to implement an electronic single window system:[40]



Legal Challenges for Digital Trade Facilitation

Ultimately, the various sources of law around data governance demonstrate 'regulatory heterogeneity'.[41] A lack of harmonization creates information asymmetries and hampers the implementation of measures for digital trade facilitation. Salient challenges include:[42]

- *Varying legal definitions*: Definitional challenges include those related to 'types' of data (*e.g.*, definitions of 'personal' and 'non-personal' data); on the meaning of 'data transfer to a third country'; or in the assignment of legal roles and responsibilities (*e.g.*,

[37] See UN/CEFACT, "Recommendation 35: Establishing a Legal Framework for an International Trade Single Window" (2013). Available at https://unece.org/sites/default/files/2023-10/Rec-35-2013-ECE-TRADE-401E.pdf.
[38] See UNESCAP, "Essential Legal Elements for the Implementation of a National Single Window" (2012). Available at https://www.unescap.org/sites/default/d8files/6%20-%202.%20Essential%20Legal%20Elements%20for%20the%20Implementation%20of%20a%20National%20Single%20Window.pdf.
[39] See UN/CEFACT, "White Paper: Single Window Assessment Methodology" (2023). Available at https://unece.org/sites/default/files/2023-10/WhitePaper_SWAM_August2023.pdf.
[40] Source: Adapted from UNESCAP, "Electronic Single Window Legal Issues: A Capacity-Building Guide" (2012). Available at https://www.unescap.org/resources/electronic-single-window-legal-issues-capacity-building-guide.
[41] See Fritz, J. and Giardini, T., "Data Governance Regulation in the G20: A Systematic Comparison of Rules and Their Effect on Digital Fragmentation", Digital Policy Alert (2023). Available at https://digitalpolicyalert.org/report/fragmentation-risk-in-g20-data-governance-regulation.
[42] Based on UNCITRAL (2023).

laws that do not precisely differentiate between the role of data controllers and data processors).

- *Unique legal concepts:* Some laws may refence novel legal concepts. For example, the EU's conceptualization of major Internet platforms as 'gatekeepers'[43] or the concept of '*habeas data'* under Latin American constitutional and privacy law.
- *Access and translation gaps:* Without availability or an authoritative translation of laws, especially at the national level, governments, lawyers, and private solutions providers must implement electronic systems despite a lack of transparency and certainty.
- *Number and frequency of adoption:* Given the dynamism of data governance *vis-à-vis* digital trade facilitation, examples of laws with potential relevance by jurisdiction and category are proliferating.

[43] Under the EU Digital Markets Act, 'gatekeepers' are described as "important market players that hold considerable market power and provide at least one core platform service", see European Commission, "Digital Markets Act – Gatekeepers", available at: https://digital-markets-act-cases.ec.europa.eu/gatekeepers.