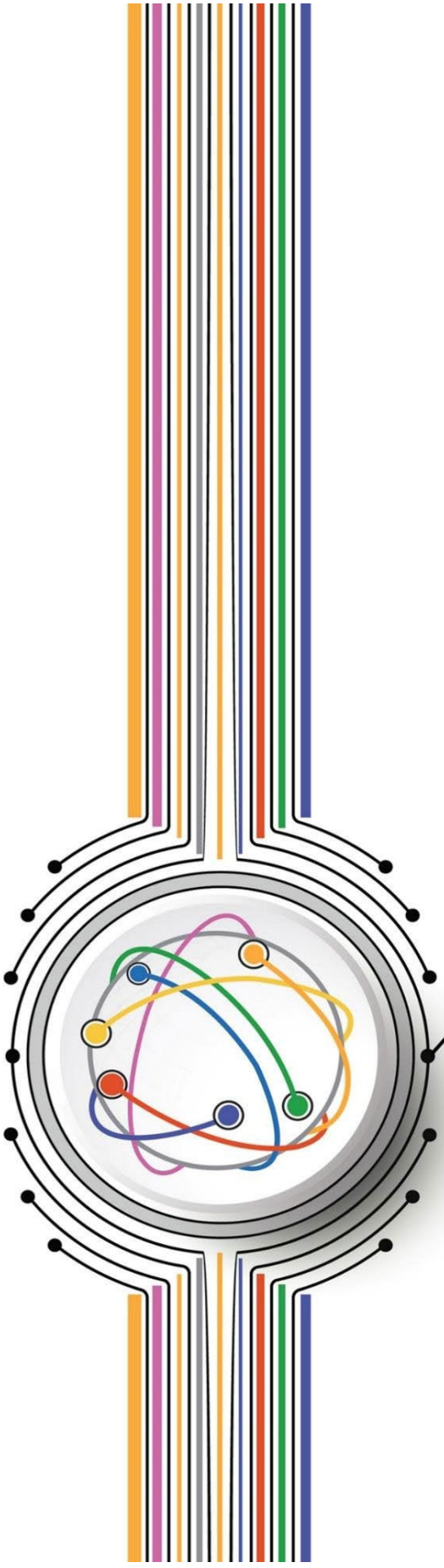


UNECE

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

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.

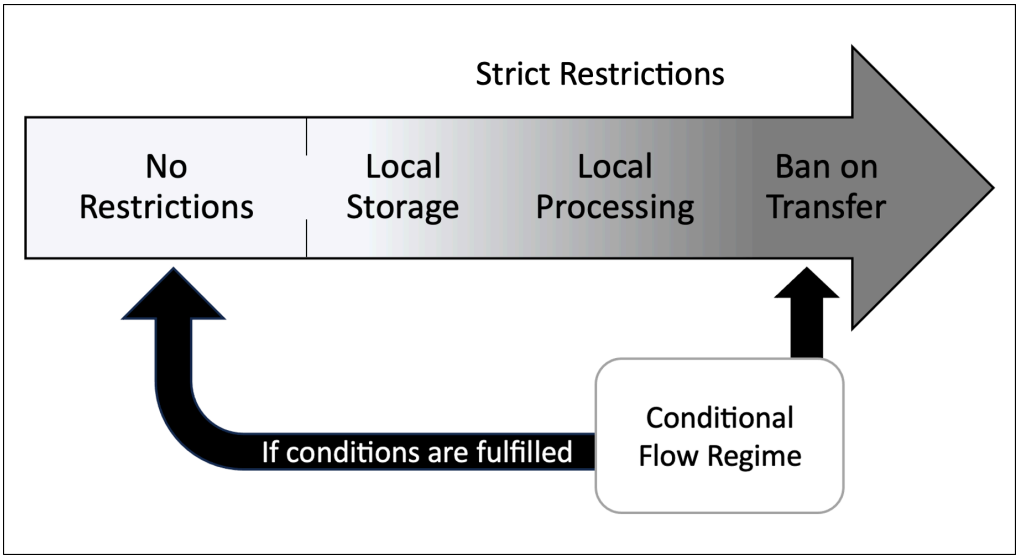
[10] See López González J., Casalini F. and Porras J., "A Preliminary Mapping of Data Localisation Measures", *OECD Trade Policy Papers*, No. 262, OECD Publishing, Paris (2022). Available at https://doi.org/10.1787/c5ca3fed-en.

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.

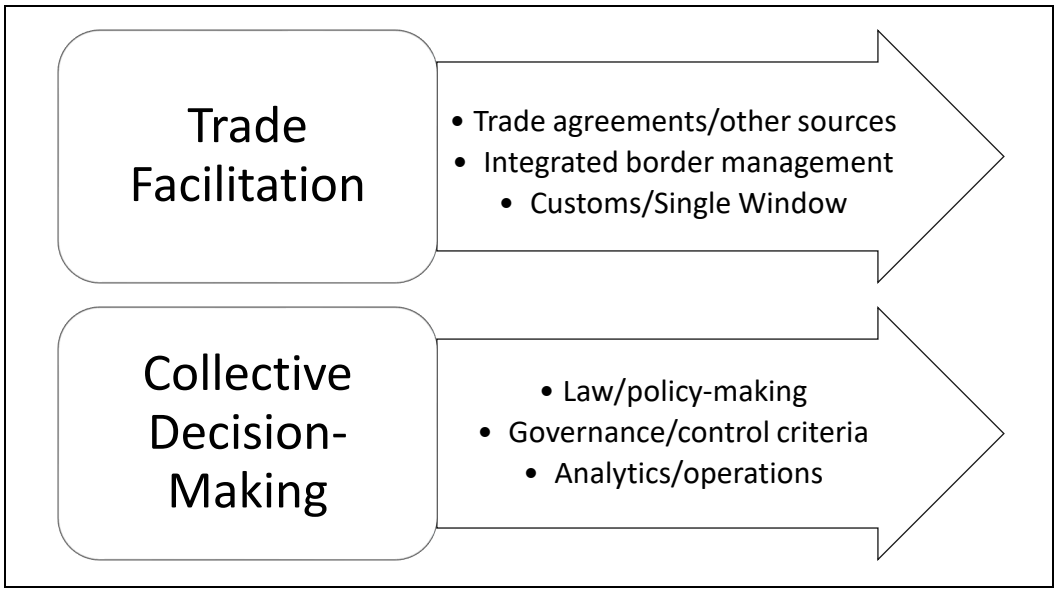
[23] Currently, many sources originate from common law countries, yet civil law jurisdictions are in the process of implementing applicable laws. For example, the 2023 report "Speeding up the Digitalisation of Trade Finance" gives insight on the promulgation of legal recognition of electronic commercial 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

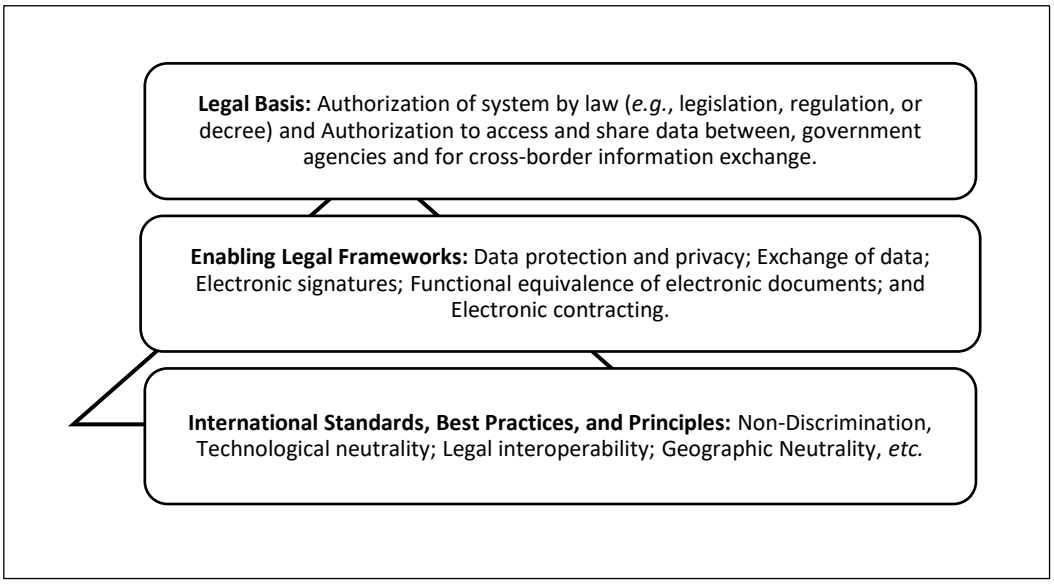
Alignment between sources of law (and non-law sources) is vital for the success of digital public infrastructure[36] (DPI) projects. The implementation of electronic single window systems

[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.