Organisation for Economic Co-operation and Development

TAD/TC/WP(2022)2/FINAL

Unclassified **English - Or. English**

13 June 2022

TRADE AND AGRICULTURE DIRECTORATE
TRADE COMMITTEE

Working Party of the Trade Committee

A preliminary mapping of data localisation measures

Digital Trade Inventory Pillar II

This document was declassified by Delegations under written procedure on 6 June 2022.

It maps the evolving data localisation environment with a view to supporting ongoing discussions on approaches that can balance different policy objectives and enable what has come to be known as *data free flows with trust* (DFFT).

The work has been prepared by a team led by Javier Lopez-Gonzalez and involving Francesca Casalini and Juan Porras.

This project is foreseen under the 2021-22 PWB item 3.1.1.2 Trade in the Digital Era. The work is part of Pillar II of the Digital Trade Inventory, financed by a voluntary contribution from the Japanese Government. The work also contributes to ongoing discussions under Module 2 on cross-border data flows of the OECD Horizontal Project on Data Governance – Going Digital III.

Javier LOPEZ-GONZALEZ (javier.lopezgonzalez@oecd.org)

JT03497621

Table of contents

Tables

Figures

Boxes

Key messages

- There is no single or official definition of data localisation. For the purposes of this paper, it is defined as an explicit requirement that data be stored and/or processed within the domestic territory.
- There are three broad types of data localisation measures. The first relates to measures that mandate local storage but allow copies to be sent and processing to take place abroad. The second relates to measures that mandate local storage and allow transfer or processing abroad under clearly defined conditions. The third relates to measures that mandate local storage and processing and prohibit transfers abroad (with ad-hoc exceptions).
- An analysis of existing measures reveals that data localisation is on the rise. By 2021, there were a total of 92 data localisation measures in place across 39 countries. More than half of these have emerged over the last 5 years. Importantly, the measures themselves are becoming more restrictive; by 2021, two thirds of measures in place involved a storage requirement with a flow prohibition (often implemented by non-OECD countries).
- Data localisation measures apply to a range of different sectors and data types. In terms of sectors, 33% of measures identified are cross-cutting. Half of these (i.e. around 16% of all measures) require that business data be stored domestically for access by relevant authorities (with no flow restriction). However, the other half include prohibitions on transfers in the context of personal or "important/critical" data. Another 23% of measures apply to financial, banking or payments and 15% to public sector data, both of which tend to involve storage requirements with flow prohibitions.
- International discussions on data localisation have largely taken place in the context of preferential trade agreements (PTAs). By April 2022, there were 21 agreements with provisions banning data localisation (albeit each with different exceptions).
- Although there is wide acknowledgement that data localisation can have negative economic implications, there is very little empirical evidence of the economic and societal implications of these measures. While benefits can be assessed against the stated objectives (e.g., whether the measure increases data or national security, or helps enable access by regulators), costs and the impacts on firm activity are likely to depend on both the nature of the measure and the extent to which firms rely on data to support their economic activities.
- There is a need to better understand and monitor the evolving regulatory environment to enable better empirical analysis of the economic and societal implications of data localisation. This will also help in the context of devising rules on data localisation, including in PTAs or in the context of the WTO in discussions at the Joint Statement Initiative on e-commerce.

1. Introduction

1. As data becomes a growing part of economic and social interactions, governments have become increasingly concerned about its use and misuse. Indeed, data raises specific challenges across a number of policy areas, including privacy and data protection, national security, digital security, intellectual property protection, regulatory reach, competition policy and industrial policy. These challenges are exacerbated when data crosses international jurisdictions; while the internet is, in many ways, borderless, regulations are not.

2. As a result of growing cross-border data flows, governments have been updating and adapting their data policies, leading to a rising number of cross-border data regulations (Casalini and López González, 2019[1]). To date, much of the work in this area has focused on measures that condition the movement of data across borders, with less analysis on policies that mandate that data be stored locally – also known as local storage requirements or data localisation.

3. Against this backdrop, the aim of this short paper is to provide a better understanding of the evolving range of data localisation regulation. The work aims to support ongoing discussions on approaches that can balance different policy objectives and enable what has come to be known as *data free flows with trust* (DFFT). This work draws on an updated database of data localisation measures (Casalini and López González, 2019[1]) and focuses on measures that have an explicit requirement that data is stored or processed in specific locations.

4. The next section discusses different definitions of data localisation. Section 3 then provides a review of some of the objectives of data localisation measures. Section 4 proposes a typology that categorises data localisation into three broad types. Section 5 explores the nature and evolution of data localisation measures, focusing on types of approaches, sectors and types of data. Section 6 offers a discussion of approaches to data localisation in the context of preferential trade agreements (PTAs) and other international agreements. Section 7 looks at what we know about the possible impacts of data localisation. Section 8 concludes, providing a summary of the findings and calling for more work and dialogue in this important area.

5. This work is part of Pillar II of the Digital Trade Inventory, financed through a voluntary contribution from the Government of Japan. The work builds on and complements the other pillars, including the mapping of regulatory approaches to cross-border data transfers (Casalini, López González and Nemoto, 2021[2]) and the Digital Trade Inventory (Nemoto and López-González, 2021[3]). It also aims to contribute to ongoing discussions under Module 2 on cross-border data flows of the OECD Horizontal Project on Data Governance – Going Digital III.

2. What is data localisation?

6. There is no single or definition of data localisation. At first, the term was understood to refer to any measure that could affect the location of data. However, as discussions on data localisation have evolved, more targeted definitions have emerged. More recently, data localisation is used to refer to more *explicit requirement that data be stored and/or processed within the domestic territory*. In the context of trade agreements, discussions on data localisation tend to fall under the heading 'location of computing facilities', understood to be requirements to "use or locate computing facilities in [a] Party's territory as a condition for conducting business in that territory" (see Box 1).

7. Distinctions between forms of data localisation are often drawn on the basis of what is considered wither 'legitimate' or an 'unjustified' or 'forced' data localisation measure (see (Cory and Dascoli, 2021[4])). This reflects a degree of ambiguity as to whether or not all forms of data localisation might raise concerns. A recent useful summary states the issue thus: "Though some localization policies may be used to achieve legitimate public policy objectives, including national security or personal data protection, some are designed to protect, favor, or stimulate domestic industries, service providers, or intellectual property at the expense of foreign counterparts and, in doing so, function as NTBs [non-tariff barriers] to market access" (Congressional Research Service, 2021[5]).

Box 1. Definitions of data localisation

Although there is wide agreement that the consequence of data localisation is more local storage or processing, there are differing views as to what types of measures fall under the category of data localisation. Some consider more implicit measures, such as restrictions on cross-border data flows, to be a form of data localisation since they can lead to more data being stored or processed locally (see (Cory and Dascoli, 2021[4]) and (Svantesson, 2020[6]). However, others focus on more explicit measures which directly legislate on the location or processing of data (Casalini and López González, 2019[1]). This paper focuses on the latter, more explicit requirements, with a view to avoiding discussions about what other measures might or might not lead to local storage or processing (including whether emerging privacy and data protection regulation could be classified as data localisation measures).

In this context, a number of definitions for data localisation have been proposed, including:

- "Forced local data-residency requirements that confine data within a country's borders, a concept known as "data localization,"" -- (Cory and Dascoli, 2021[4]).
- "A mandatory legal or administrative requirement directly or indirectly stipulating that data be stored or processed, exclusively or non-exclusively, within a specified jurisdiction" – (Svantesson, 2020[6]).
- "Any legal or administrative measure which states that data processing must take place in a specific EU territory" – EU Regulation on the free flow of non-personal data.[1]
- In trade agreements, data localisation often falls under articles entitled 'Location of computing facilitates':
  - Article 19.12 of USMCA specifies that "No Party shall require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory."
  - Article 14.13 of CPTPP has similar language ("No Party shall require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory.") although exceptions for legitimate public policy objectives are included.

[1] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R1807&from=EN).

- Article 201 of the EU-UK TCA: "The Parties are committed to ensuring cross-border data flows to facilitate trade in the digital economy. To that end, cross-border data flows shall not be restricted between the Parties by a Party:

  (a) requiring the use of computing facilities or network elements in the Party's territory for processing, including by imposing the use of computing facilities or network elements that are certified or approved in the territory of a Party;

  (b) requiring the localisation of data in the Party's territory for storage or processing;

  (c) prohibiting the storage or processing in the territory of the other Party; or

  (d) making the cross-border transfer of data contingent upon use of computing facilities or network elements in the Parties' territory or upon localisation requirements in the Parties' territory.

3. Why is data localisation emerging?

8. There are a number of different reasons for governments to legislate on the location of data, reflecting a range of different objectives (Casalini and López González, 2019[1]).

   - They may require data to be stored domestically as a means of ensuring that domestic **privacy and data protection** principles and rights of individuals are respected.
   - They may mandate that data be stored locally with a view to ensuring access to information for **regulatory purposes**. That is, for example, to ensure that tax authorities can access information needed for tax purposes, or that telecommunication, banking or insurance regulators can avail themselves of the information they need to oversee activities in these sectors.
   - Data localisation might also be sought as a means of protecting information that may be deemed to be sensitive from a **national security** perspective – whether to enable access and review of data by national security services, or to prevent or protect data from access by distrusted agents or governments.
   - Governments also promote local storage and processing with a view to ensuring **data security** on the rationale that data security can best be guaranteed when storage and processing is domestic.
   - Last, data localisation is increasingly being deployed in the context of industrial policies or **digital protectionism**, where countries believe that these measures can help develop domestic capacity in digitally intensive sectors.

9. When thinking about data localisation, the underlying objective for applying the measure is important. First, because it helps determine whether or not data localisation might be applied in the context of what is considered to be a legitimate public policy objective. Traditionally, these can include issues related to privacy protection, national security or indeed regulatory reach. Second, it is important to assess how effective the measure might be in achieving its stated objective. This is especially important from a trade perspective, to assess whether the same policy objective could equally be achieved in a less trade restrictive way.

4. How are countries approaching data localisation policies?

10. Data localisation measures that are in place today vary widely, often in relation to their underlying policy objectives (as noted above); the sectors or types of data targeted; and the wider legal and policy environment. In addition, even within a particular country, or regions within countries, different types of data localisation measures can apply to different types of data (e.g. personal data, health data, telecommunication data, banking or payment processing data; insurance data; or satellite and mapping data to name but a few). There are also cases where data localisation requirements are aimed at less well defined data categories such as "important data" or "critical data" and operators such as "critical information infrastructure operators" or "network operators".

11. Overall, data localisation measures can be grouped into three broad, although not sharply delineated, categories – Figure 1.[2] These reflect the fact that data localisation requirements are often paired with different types of processing and/or flow restrictions. For instance, some approaches may require that health data be stored and processed locally and that it only be allowed to move out of the country provided that certain requirements are met. At the extreme, a complete prohibition on the transfer of data amounts to a de facto requirement for local storage and processing. At the same time, a requirement that data be stored and processed only domestically can also correspond to a complete prohibition of cross-border transfer.

12. The first category of approaches refers to measures that require a copy of the relevant data to be kept within the country's territory, without prohibiting storage or processing in other countries. These measures are often applied in the context of ensuring that regulators do not encounter issues related to jurisdictional reach. Approaches falling under this category often target business data (accounts) or telecommunication metadata, including in the context of data retention policies. For example, Sweden's Accounting Act[3] stipulates that accounting information is to be retained and stored for seven years in Sweden.[4]

13. The second category of measures requires a copy of the data to be kept within the country, but allows it to be transmitted abroad on the basis of clearly defined transfer or access conditions. For example, the Electronic Health Records Act in Australia requires that health record information be stored in Australia but provides for access overseas in cases where access is needed by users (the data subjects) or by registered healthcare providers overseas.

14. The third category of approaches refers to measures that mandate local storage of data while also prohibiting transfers to other countries (or only on the basis of ad-hoc authorisations). These more sweeping restrictions can apply to a range of data, including banking, telecommunications or payment data, as well as to broader categories of information. For instance, in Indonesia, Regulation 71 (2019) concerning the implementation of electronic systems and transactions[5] foresees that all data is to be managed, processed and stored in Indonesia. Exceptions to this rule arise in the event that storage technology are not available

[2] Although presented as distinct, the boundaries between these categories can be blurry and even overlap.

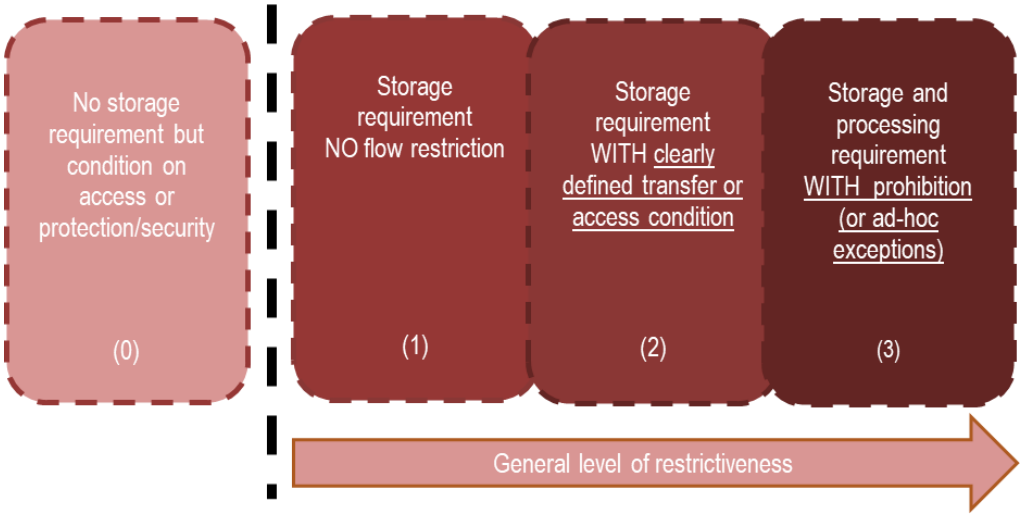
[3] Bokföringslag (1999:1078), accepted 1999-12-02 , last amended 2017-06-07, chapter 7 section 2, https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/bokforingslag-19991078_sfs-1999-1078

[4] Such rules can be thought of as transpositions of analogue rules such as enabling physical access to a firm's financial data for audit purposes, to the digital world.

[5] Government Regulation Number 71 Dated October 10, 2019 concerning the Implementation of Electronic Systems and Transactions JDIH KEMKOMINFO.

domestically, the criteria for which is determined by a government authority. Another example is China's Cybersecurity Law where article 37 requires "critical information infrastructure operators" to store "important data" in China.[6]

Figure 1. A typology of data localisation measures and requirements for data flow



Note: Figure is schematic; elements do not singularly identify any given country's approach to data localisation. Different approaches tend to apply to different types of data, even within a same jurisdiction.
Source: Authors' compilation updating (Casalini and López González, 2019[1]).

15. Outside this typology, a new category of approaches is emerging (Category 0). These are measures where there is no requirement for data to be stored locally, but firms are required to guarantee access to data. For instance, Mexico's Federal Telecommunications Law requires data to be made available for 12 months, without stipulating that it must be stored in Mexico.[7] Similarly, New Zealand's data retention regulation for business records allows for data to be stored outside of New Zealand provided it meets certain data integrity and access criteria.[8] Within the EU, legislation on the movement of non-personal data forbids data localisation within the EU, but requires that data be made accessible to the relevant authorities.[9]

[6] There are also a number of other draft legislations which mandate local storage with transfer prohibitions. These include the Draft Data Security Law as well as more sectoral regulation such as article 6 of the Effective Protection of Personal Financial Information by Banking Institutions or article 10 of the Administration of Population Health Information.

[7] Ley federal de Telecommunications y Radiodifusión, 14 July, amended on 24 January, Article 190 (II)): https://www.gob.mx/cms/uploads/attachment/file/346846/LEY_FEDERAL_DE_TELECOMUNICACIONES_Y_RADIODIFUSION.pdf

[8] https://www.taxtechnical.ird.govt.nz/-/media/project/ir/tt/pdfs/standard-practice-statements/general/sps-21-02.pdf?modified=20210506215836.

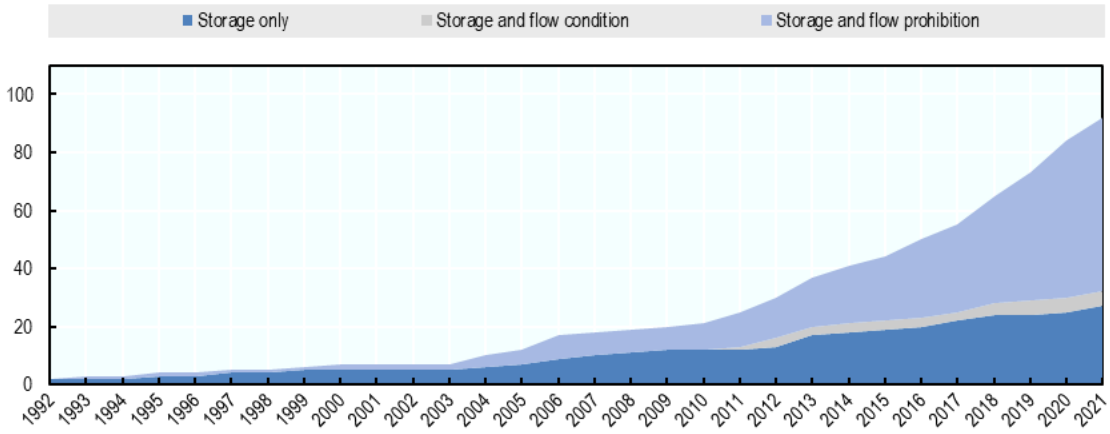
[9] REGULATION (EU) 2018/1807 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 November 2018 on a framework for the free flow of non-personal data in the European Union (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R1807&from=EN)

5. What do we know about the nature and evolution of data localisation?

16. Data on the number of explicit data localisation measures in place show an upward trend (Figure 2). By 2021, 92 measures across 39 countries were identified that explicitly mandated that data be stored or processed domestically. More than half of the identified data localisation measures emerged in the last 5 years. Importantly, the measures themselves are becoming more restrictive; by 2021, two thirds of identified measures involved a storage requirement with a flow prohibition.

17. Measures appear to be more restrictive across non-OECD countries (Figure 3). Indeed, overall, 60% of the measures applied by OECD countries involve storage requirements only, while in non-OECD countries, measures taking the form of storage requirements with flow prohibitions dominate (representing 83% of identified data localisation measures).

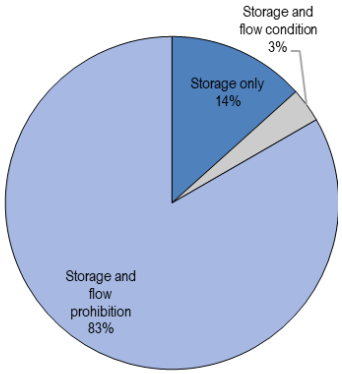
Figure 2. Data localisation is growing and becoming more restrictive



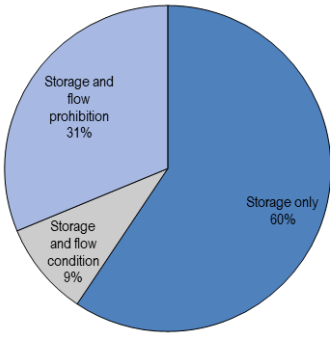
Note: Data localisation measures are defined as explicit requirements that data be stored or processed domestically.
Source: Own calculations based on own compilation including through the Digital Trade Alert, the OECD Digital STRI and (Cory and Dascoli, 2021[4]).

Figure 3. Data localisation measures tend to be more restrictive in non-OECD countries

a. Non-OECD countries



b. OECD countries



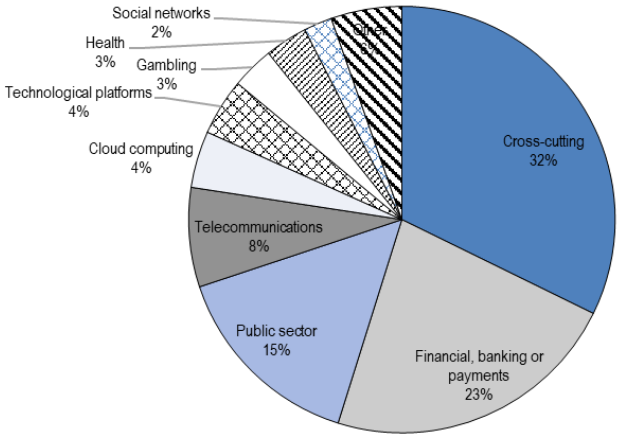
Note: Data localisation measures are defined as explicit requirements that data be stored or processed domestically. In the order of least restrictive to most restrictive: Storage only refers to category 1 in Figure 1. Storage and flow condition refers to category 2 in Figure 1 and Storage and flow prohibition to category 3 in Figure 1.
Source: Own calculations based on own compilation including through the Digital Trade Alert, the OECD Digital STRI and (Cory and Dascoli, 2021[4]).

18. Data localisation also affects a diverse range of data and sectors (Figure 4). This stands in contrast with findings from recent work which suggest that conditions on cross-border data flows largely target transfers of personal data in the context of privacy protection and apply across the entire economy (see (Casalini and López González, 2019[1]) and (Casalini, López González and Nemoto, 2021[2])).

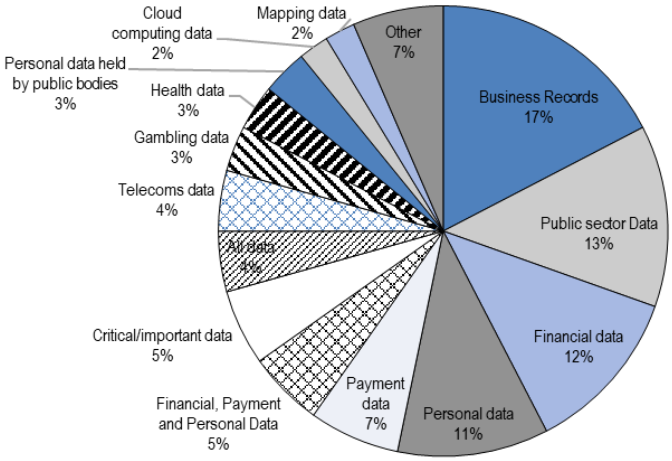
19. In terms of sectors, 33% of data localisation measures identified are cross-cutting, meaning that they have implications for a number of sectors. Half of these (i.e. around 16% of all measures) require that business data be stored domestically to enable access by relevant authorities (with no flow restriction). However, the other half (a further approximately 16% of all measures) include prohibitions on transfers in the context of personal or 'critical or important' data. Around 23% of the total number of measures identified apply to financial, banking or payments and a further 15% of the total to the public sector. In both cases, measures tend to combine storage requirements with flow prohibitions. The remaining 29% of measures identified apply to telecommunications, cloud computing, health, gambling, tech platforms and other sectors. Where data types are concerned, the four largest categories are: business records (17% of measures), public sector data (13%), financial data (12%) and personal data (11%).

Figure 4. Data localisation measures by sector and data type

a. Targeted sectors



b. Targeted data



Note: Sectors and data types are identified from the regulation or measures and have been grouped to enable easier analysis (e.g., measures referring to personal information or personal data are grouped under the common heading of personal data).
Source: Author's compilation based on 92 identified data localisation measures.

20. Cross tabulating the measures across data types and sectors provides further insights into the nature of data localisation (Table 1). Out of the 30 cross-cutting measures identified, 13 relate to business records, requiring that these be stored locally for audit; 7 relate to personal data. Two other important categories are financial data, applying largely to the financial or banking sectors, and localisation measures for public sector data or personal information held by the private sector.

Table 1. Data localisation measures by sector and data type

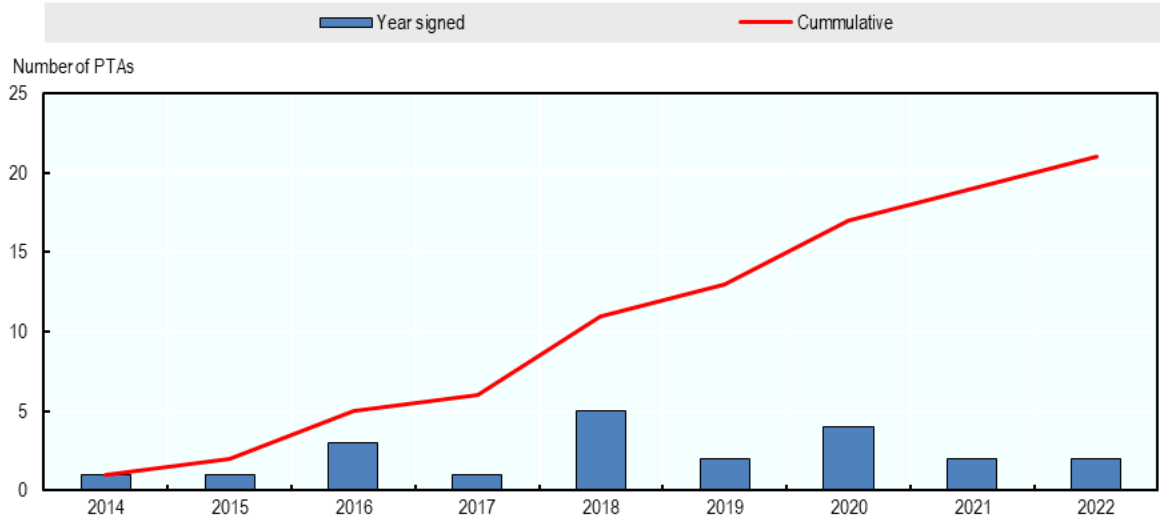
Data type (rows)/sector (columns)	Cloud computing	Cross-cutting	Financial, banking or payments	Gambling	Health	Insurance	Mapping Services	Public sector	Publishing	R&D	Social networks	Technological platforms	Telecoms	Grand Total
All data		2									1		1	4
Business Records		13	1									1	1	16
Cloud computing data	2													2
Critical/important data		3						1				1		5
data from technological platforms												1		1
Domain names		1												1
Electronic Systems and Electronic Data		1												1
Financial data		1	10											11
Financial, Payment and Personal Data			5											5
Gambling data				3										3
Health data					3									3
Mapping data							1					1		2
Official information		1												1
Payment data		1	5											6
Personal data		7				1					1		1	10
Personal data held by public bodies								3						3
Public sector Data	2							10						12
Publishing data									1					1
Scientific data										1				1
Telecoms data													4	4
Total	4	30	21	3	3	1	1	14	1	1	2	4	7	92

Note: Sectors and data types are identified from the regulation or measures and have been grouped to enable easier analysis (e.g. measures referring to personal information or personal data are grouped under the common heading of personal data).
Source: Author's compilation based on 92 identified data localisation measures.

6. How are countries approaching data localisation in their trade agreements and other international discussions?

21. Discussions on data localisation often arise in the context of preferential trade agreements. Indeed, as of April 2022, 21 agreements had provisions prohibiting data localisation as a condition for conducting business (Figure 5).[10] These either ban or limit data localisation, often under headings entitled 'location of computing facilities'. These provisions have only started emerging since 2014, perhaps in reaction to the rise in data localisation measures, as noted in Figure 2.

Figure 5. Data localisation provisions in PTAs



Note: See Annex Table A1 for a list of agreements.
Source: Author's compilation based on TAPED database (Burri and Polanco, 2020[7]).

22. While all trade agreements stipulate that using or locating computing facilities in a party's territory shall not be required; they differ in their exceptions for achieving legitimate public policy objectives (LPPO). At one extreme, agreements such as the United States-Mexico-Canada Agreement (USMCA) or the EU-UK Trade and Cooperation Agreement (TCA) provide for no exceptions in the provisions (although GATT and GATS exceptions continue to apply).[11] At the other extreme, agreements such as the Regional Comprehensive Economic Partnership (RCEP) agreement provide for wider exceptions, including through language whereby the country implementing the measure determines whether said measure is legitimate or not. Across most agreements, the data localisation provisions are subject to dispute settlement (Table 2).

[10] See Annex Table A1 for a list of agreements (based on the TAPED database (Burri and Polanco, 2020[7]) but updated with recent agreements). Number includes Korea-Singapore Digital Partnership Agreement although text has yet to be published as of the 4th of April 2022. Inclusion of data localisation provision is explained here: https://www.mti.gov.sg/Improving-Trade/Digital-Economy-Agreements/KSDPA

[11] The EU-UK TCA also contains a specific exception for privacy.

Table 2. Exceptions to data localisation provisions in trade agreements

Types of exceptions	Number of agreements	Examples	Number of economies that have signed the agreements	Number of agreements that subject data localisation rules to dispute settlement
LPPO - Non-discrimination - Not-unnecessarily trade restrictive	7	- Comprehensive and Progressive Trans-Pacific Partnership Agreement (CPTPP). - Updated Singapore-Australia Free Trade Agreement (SAFTA) - Chile New Zealand Singapore Digital Economy Partnership Agreement (DEPA) -UK-SGP DEA, UK-NZL and UK-AUS	27	7
LPPO - Necessary to - Non-discrimination	2	- Japan-Mongolia FTA, - Japan-UK FTA	4	2
LPPO - Non-discrimination	5	- Chile-Uruguay FTA, - Singapore-Sri-Lanka FTA, - Australia-Peru FTA, - Brazil-Chile FTA	10	5
LPPO - Non-discrimination - Essential security interests	1	- Indonesia-Australia FTA	2	1
LPPO - It considers necessary to - Non-discrimination - Essential security interests	1	- RCEP	15	0
No exceptions (except for GATT and GATS exceptions)	3	- US-Japan Digital Trade Agreement, - United States Mexico Canada Agreement (USMCA). - EU-UK TCA	6	3

Note: LPPO refers to legitimate public policy objectives. Non-discrimination refers to exceptions for LPPO, which cannot be applied "in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade". Not-unnecessarily trade restrictive relates to language such as: "does not impose restrictions on the use or location of computing facilities greater than are required to achieve the objective". Necessary to: "Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with [ban on data localisation] that are necessary to achieve a legitimate public policy objective". Essential security interests: "any measure that it considers necessary for the protection of its essential security interests." It considers: "any measure inconsistent with [ban on data localisation] that it considers necessary to achieve a legitimate public policy objective". GATT and GATS exceptions refer to there not being specific exceptions other than exceptions specified under GATT or GATS.
Source: Own from TAPED database (Burri and Polanco, 2020[7]).

23. Discussions on data localisation have also taken place in the context of the G7. Under the UK Presidency in 2021, the G7 Trade Ministers agreed on a set of Digital Trade Principles. Within these, countries express concern "about situations where data localisation requirements are being used for protectionist and discriminatory purposes, as well as to undermine open societies and democratic values, including freedom of expression."

24. Rules stipulating that countries cannot impose local storage requirements do not appear to have been developed in other intergovernmental fora or agreements beyond those discussed above.

7. What do we know about the impact of data localisation measures?

25. Identifying the economic and societal impact of data localisation is complex. Many data localisation measures are put in place to meet legitimate public policy objectives, including enabling access by relevant authorities or in the context of national or digital security. Identifying the 'dollar value' of these benefits is not straightforward – nor is identifying what may or may not be a legitimate public policy objective. In any event, such policies need to be assessed against their stated objectives: that is, whether localisation leads to greater data security or whether data localisation enables better privacy and data protection. From a trade perspective, it is also important to assess whether the stated objectives can equally be achieved in a less trade restrictive way.

26. Assessing the cost of data localisation measures can be more straightforward. By imposing requirements on the storage and processing of data, data localisation measures are likely to alter the way businesses operate, in turn affecting their costs and, in some instances, their ability to benefit from economies of scale from more centralised data storage or processing solutions.

27. The overall costs will depend on a number of factors, including how important data is to the activities of the firm and the extent to which this might disrupt economic activity in the context of highly integrated supply chains. However, another key factor will be the nature of the measures in place. Storage requirements with no flow restrictions (see Figure 1) are likely to lead to an increase in operational costs related to having to store data domestically. Since the cost of storage is low and falling, and data can still move unimpeded, the overall increase in cost is expected to be low as it would only be about finding storage solutions (notwithstanding costs related to duplication of cybersecurity or data protection). However, where data localisation is combined with data flow restrictions, economic and societal impacts are likely to increase, including in the context of having to duplicate both storage and also processing activities, which can have wider operational implications as well as a reduction in the ability to take advantage of economies of scale from more centralised storage and processing. At the extreme, full localisation (with a flow prohibition) will imply complete duplication of activities, loss of scale and could also mean an inability to engage in economic activity.

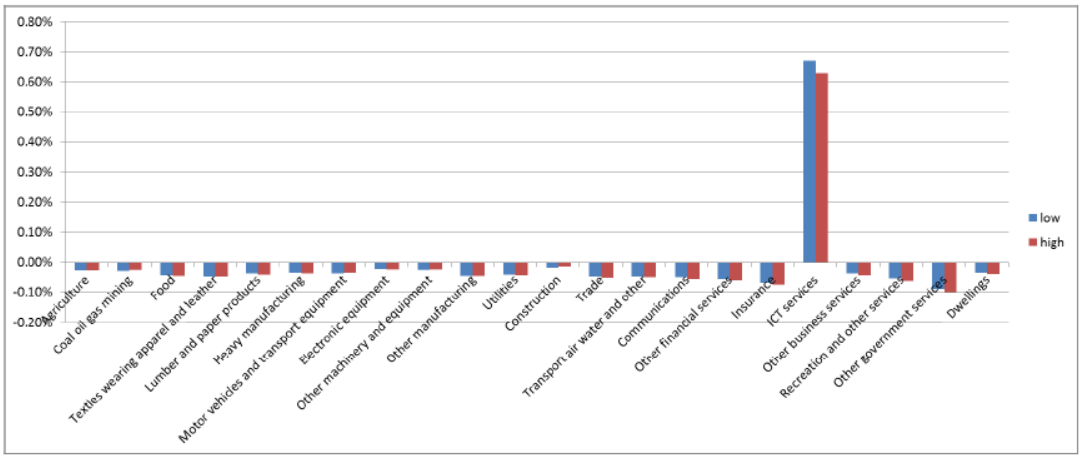
28. For firms operating across a range of markets, transparency in how the measure is formulated and implemented will be key in avoiding higher than necessary costs of compliance. There will also be costs related to complexity and fragmentation. If each market has a different rule for similar, yet differently defined data types, this will lead to higher operational and compliance costs for firms, rising with the degree of fragmentation and complexity. These costs are likely to fall disproportionately on smaller firms, women entrepreneurs and developing countries, which often lack the technical capacity needed to keep up with regulation and where compliance costs can represent a higher share of overall costs. This can jeopardise their ability to benefit from digital trade.

29. While it is widely acknowledged that data localisation may have economic and societal implications, the impact of these measures has received little attention in the empirical literature. To date, most of the empirical work has focused on the impact of measures that condition the movement of data across international borders (e.g. (Bauer et al., 2014[8]) (Cory and Dascoli, 2021[4])). USITC (2019[9]) jointly modelled the impact of data flows and

data localisation provisions in the USMCA. They find that the reduction in trade costs from these provisions range between 1.1 and 1.4 percentage points, depending on the country.[12]

30. Flaig et al. (2016[10]) model the impact of local storage requirements more directly using a computable general equilibrium (CGE) model (the OECD METRO model). Data localisation as modelled as a local content requirement (see (Stone, Messent and Flaig, 2015[11])) that increases the cost of Information Communication Technology (ICT) inputs.[13] The size of the shock, the amount by which ICT costs increase, is based on a business questionnaire (see Annex Table 2). Overall, the impact of these measures is to raise demand for domestic ICT services, but, at the same time, to raise the costs of ICT inputs for other using sectors. (Flaig et al., 2016[10]) and (Lopez-Gonzalez et al., 2016[12]) find that the negative impact on other sectors outweighs the positive impact on domestic data services (see Figure 6).

Figure 6. The impact of a data localisation measure without a flow restriction



Note: Figure shows sectoral effects on global production (% change) from a data localisation requirement with no flow restriction into a CGE modelling framework.
Source: (Flaig et al., 2016[10]) and (Lopez-Gonzalez et al., 2016[12]).

8. What do we learn from this analysis?

31. Data localisation means different things to different people – there is no single, and widely accepted, definition of data localisation. For the purposes of this report, data localisation is understood to be an explicit condition that data be stored and/or processed within the domestic territory. On the basis of this definition, this work identifies that data localisation is on the rise and becoming increasingly restrictive.

32. Data localisation also involves a range of different approaches, which can be grouped into three categories: i) measures that mandate that data be stored domestically, but do not provide for any flow restriction; ii) measures that mandate local storage, but allow transfer

[12] (USITC, 2019[9]) quantifies the impact of data localisation and data transfer measures using the OECD STRI. They use the weight that is assigned to these measures in the STRI to calculate ad-valorem equivalents (AVEs) for services sectors. For non-services sectors, they use additional weights, including related to digital intensity.

[13] The cost increase is to be satisfied by increasing domestic consumption.

or processing abroad under clearly defined conditions; and iii) measures that mandate local storage and processing and only allow transfer or processing on an ad-hoc basis.

33. Data localisation measures target an array of sectors and data types. Many of the more cross-cutting measures refer to requirements that business data be stored domestically for access by relevant authorities. However, most measures tend to be sector specific; these include localisation requirement or data retention policies for telecommunications data or for financial or payments. However, there are also a number of more sweeping measures that target ill-defined types of data (such as 'critical' or 'important' information), which also tend to be combined with ad-hoc exceptions for foreign storage or processing.

34. International discussions on data localisation have largely taken place in the context of PTAs. By April 2022, there were 21 such agreements with provisions banning data localisation (albeit with different exceptions). This is a recent trend, which seems to have emerged in response to the growing number of measures.

35. Although there is wide acknowledgement that data localisation can have negative economic implications, there is very little empirical evidence of the economic and societal implications of these measures. While benefits need to be assessed against the stated objectives (e.g. whether they increase data or national security or if they enable access by regulators), costs, and the impact on firm activity are likely to depend on the nature of the measure, as well as the extent to which firms rely on data to support their economic activities.

36. There is a need to better understand and monitor the evolving regulatory environment with a view to enabling better empirical analysis of the economic and societal implications of data localisation. This is particularly important in the context of ongoing discussion on data localisation, be they in PTAs or in the context of discussions at the WTO Joint Statement Initiative on e-commerce.

References

Bauer, M. et al. (2014), "The costs of data localisation: friendly fire on economic recovery", *ECIPE Occasional Paper. No. 3/2014*, http://www.ecipe.org/app/uploads/2014/12/OCC32014__1.pdf. [8]

Burri, M. and R. Polanco (2020), "Digital Trade Provisions in Preferential Trade Agreements: Introducing a New Dataset", *Journal of International Economic Law, Oxford University Press,*, Vol. 23(1), pp. 187-220, http://hdl.handle.net/10.1093/jiel/jgz044. [7]

Casalini, F. and J. López González (2019), "Trade and Cross-Border Data Flows", *OECD Trade Policy Papers*, No. 220, OECD Publishing, Paris, https://dx.doi.org/10.1787/b2023a47-en. [1]

Casalini, F., J. López González and T. Nemoto (2021), "Mapping commonalities in regulatory approaches to cross-border data transfers", *OECD Trade Policy Papers*, No. 248, OECD Publishing, Paris, https://dx.doi.org/10.1787/ca9f974e-en. [2]

Congressional Research Service (2021), "Digital Trade and U.S. Trade Policy", *Congressional Research Service R44565*, https://sgp.fas.org/crs/misc/R44565.pdf. [5]

Cory, N. (2017), "Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?", *INFORMATION TECHNOLOGY & INNOVATION FOUNDATION*, http://www2.itif.org/2017-cross-border-data-flows.pdf?_ga=2.170878624.1422429408.1619522271-643310589.1613547417. [13]

Cory, N. and L. Dascoli (2021), "How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them", *Information Technology & Inovation Foundation*, https://itif.org/sites/default/files/2021-data-localization.pdf. [4]

Ferracane, F. and E. Van der Marel (2018), "Do data policy restrictions inhibity trade in services?", *European Centre for International Political Economy, Brussels*, https://ecipe.org/wp-content/uploads/2018/10/Do-Data-Policy-Restrictions-Inhibit-Trade-in-Services-final.pdf. [14]

Flaig, D. et al. (2016), "Modelling data localisation measures", *Paper prepared for the 19th Annual conference on Global Economic Analysis*, https://www.gtap.agecon.purdue.edu/resources/download/8275.pdf. [10]

Lopez-Gonzalez, J. et al. (2016), "LOCALISING DATA IN A GLOBALISED WORLD", *Working Party of the Trade Committee TAD/TC/WP(2016)8/REV2*. [12]

Nemoto, T. and J. López-González (2021), "Digital trade inventory: Rules, standards and principles", *OECD Trade Policy Papers*, Vol. No. 251/OECD Publishing, https://doi.org/10.1787/9a9821e0-en. [3]

Stone, S., J. Messent and D. Flaig (2015), "Emerging Policy Issues: Localisation Barriers to Trade", *OECD Trade Policy Papers*, No. 180, OECD Publishing, Paris, https://dx.doi.org/10.1787/5js1m6v5qd5j-en. [11]

Svantesson, D. (2020), "Data localisation trends and challenges: Considerations for the review of the Privacy Guidelines", *OECD Digital Economy Papers, No. 301, OECD Publishing, Paris,* https://doi.org/10.1787/7fbaed62-en. [6]

USITC (2019), *U.S.-Mexico-Canada Trade Agreement: Likely Impact on the US Economy and on Specific Industry Sectors*, https://www.usitc.gov/publications/332/pub4889.pdf. [9]

Annex A

Annex Table A1. Agreements with data localisation provisions

Long title	Short title	Type	Parties	Year signed
Protocolo Adicional al Acuerdo Marco de la Alianza del Pacífico	Pacific Alliance Additional Protocol (PAAP)	FTA	CHL, COL, PER, MEX	2014
Agreement between Japan and Mongolia for an Economic Partnership	Japan Mongolia FTA	FTA	JPN, MNG	2015
Comprehensive and Progressive Trans-Pacific Partnership Agreement	Transpacific Partnership (CPTPP)	FTA	AUS, BRN, CAN, CHL, JPN, MYS, MEX, NZL, PER, SGP, VNM	2016
Acuerdo de Libre Comercio entre la República de Chile y la República Oriental del Uruguay	Chile Uruguay FTA	FTA	CHL, URY	2016
Updated Singapore-Australia Free Trade Agreement (SAFTA)	Australia Singapore	FTA	AUS, SGP	2016
Trade Agreement between the Argentine Republic and the Republic of Chile	Argentina Chile FTA	FTA	ARG, CHL	2017
Free Trade Agreement between the Democratic Socialist Republic of Sri Lanka and the Republic of Singapore	Singapore Sri Lanka FTA	FTA	LKA, SGP	2018
Australia-Peru Free Trade Agreement	Australia Peru FTA	FTA	AUS, PER	2018
Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP)	CPTPP	FTA	AUS, BRN, CAN, CHL, JPN, MYS, MEX, NZL, PER, SGP, VNM	2018
United States - Mexico - Canada Agreement	USMCA	FTA	USA, MEX, CAN	2018
Chile - Brazil Bilateral Trade Agreement	Brazil Chile FTA	FTA	BRA, CHL	2018
Indonesia - Australia Comprehensive Economic Partnership Agreement	Australia-Indonesia CEPA	EPA	AUS, IDN	2019
Agreement Between The United States Of America And Japan Concerning Digital Trade	Japan US Digital Trade Agreement (DTA)	DTA	JPN, USA	2019
Australia-Singapore Digital Economy Agreement	Australia Singapore Digital Economy Agreement (ASDEA)	EA	AUS, SGP	2020
Digital Economy Partnership Agreement ("DEPA") Between Singapore, Chile & New Zealand	Chile New Zealand Singapore Digital Economy Partnership Agreement (DEPA)	EPA	CHL, NZL, SGP	2020
Regional Comprehensive Economic Partnership ("RCEP")	RCEP	EPA	AUS, BRN, KHM, CHN, IDN, JPN, KOR, LAO, MYS, NZL, PHL, SGP, THA, VNM	2020
Trade and Cooperation Agreement between the European Union and the European Atomic Energy Community, of the One Part, and the United Kingdom of Great Britain and Northern Ireland, of the Other Part	EU UK TCA	FTA	EU, UK	2020
UK-Australia FTA	AUS-UK FTA	FTA	AUS,UK	2021
Korea-Singapore Digital Partnership Agreement (KSDPA)	KSDPA	DEA	KOR, SGP	2021
UK-New Zealand Free Trade Agreement	UK-NZL FTA	FTA	UK, NZL	2022
UK-Singapore Digital Economy Agreement	UK-SGP DEA	DEA	UK, SGP	2022

Source: Own from TAPED database (Burri and Polanco, 2020[7]).

Annex Table A2. Perceived costs of measures across sectors

	High		Low	
Sector	**Data Transfer** (as share of total costs)	**Storage** (as share of ICT costs)	**Data Transfer** (as share of total costs)	**Storage** (as share of ICT costs)
Agriculture	0.31%	34%	0.00%	25%
Coal oil gas mining	0.63%	1%	0.00%	0%
Food	3.84%*	23%*	2.68%*	14%*
Textiles wearing apparel and leather	3.84%*	1%	2.68%	0%
Lumber and paper products	1.26%	1%	0.10%	0%
Heavy manufacturing	3.84%*	0%*	2.68%*	0%*
Motor vehicles and transport equipment	0.01%	21%	0.00%	12%
Electronic equipment	2.29%	21%	1.13%	12%
Other machinery and equipment	5.07%	31%	3.91%	22%
Other manufacturing	3.84%*	21%*	2.68%*	12%*
Utilities	2.31%	21%	1.15%	12%
Construction	6.51%	23%	5.35%	14%
Trade	7.58%	41%	6.42%	32%
Transport air water and other	3.84%*	23%*	2.68%*	14%*
Communications	7.50%	34%	6.34%	25%
Other financial services	3.88%	24%	2.72%	15%
Insurance	3.84%*	21%*	2.68%*	12%*
ICT services	3.37%	22%	2.21%	13%
Other business services	3.85%	19%	2.69%	10%
Recreation and other services	2.46%	21%	1.30%	12%
Other government services	0.19%	21%	0.00%	12%
Standard deviation	2.18%	11%		
Mean-Stdev	1.16%	9%		

Note: Data from a business questionnaire administered in 2016. * identifies missing data which is instrumented by the average across all sectors but checked against other variables in the questionnaire to ensure consistency of responses. Throughout, the lowest response values from the Business Questionnaire were taken to reduce upward bias from respondents. The figures for the low scenario are obtained by subtracting the sample mean minus the standard deviation from the high-scenario values. When this causes the value to be negative, this is replaced by zero. Lumber and paper products, Construction, Motor vehicles and transport equipment, Recreation and other services, utilities are represented by a single firm; Electronic equipment, Coal oil gas mining, Other government services (2 firms); Communications, other financial services, other machinery equipment (4); The remainder by 5 or more with; Other business services (10) and ICT services (16) being most represented in terms of firm coverage.
Source: (Lopez-Gonzalez et al., 2016[12]).