Organisation for Economic Co-operation and Development

**TAD/TC/WP(2023)7/FINAL**

**Unclassified** **English - Or. English**

**10 November 2023**

**TRADE AND AGRICULTURE DIRECTORATE**
**TRADE COMMITTEE**

**Working Party of the Trade Committee**

# The nature, evolution and potential implications of data localisation measures

Purpose: Building on previous work of the Trade Committee, this final draft paper on data localisation has been prepared to advance discussions at the G7. It is entirely funded by a voluntary contribution from the Government of Japan.

Preparation: This final draft was prepared by Chiara DEL GIOVANE, Janos FERENCZ and Javier LOPEZ-GONZALEZ of the Trade Policy Division.

Background: The work is foreseen under Output Area 3.1.1.2.3 (Data and data flows) of the 2023-24 PWB.

Communication and dissemination: It is envisaged to publish this work as part of the OECD Trade Policy Paper series.

This paper has been declassified by the Working Party of the Trade Committee in September 2023.

Javier LOPEZ-GONZALEZ (javier.lopezgonzalez@oecd.org)
Janos FERENCZ (janos.ferencz@oecd.org )
Chiara DEL GIOVANE (chiara.delgiovane@oecd.org)

**JT03531379**

# *Table of contents*



## Tables



## Figures



## Boxes

# Key messages

- **Data localisation requirements are growing**. By early 2023, close to a hundred data localisation measures across 40 countries were in place. More than half of these have emerged since 2015.
- **Data localisation measures are becoming increasingly restrictive.** By 2023, more than two thirds of measures in place imposed a local storage and processing requirement without the possibility for data to flow outside the country, the most restrictive form of data localisation identified.
- **Non-OECD countries are the main drivers of more restrictive approaches**. Nine in ten data localisation measures applied by non-OECD countries combine local storage with a flow prohibition (by contrast only one third of measures in OECD countries are in this category).
- **Different types of data attract different types of data localisation measures.** More sensitive data, including health data or data held by the public sector, is associated with more restrictive data localisation measures across both OECD and non-OECD countries. By contrast, business records or telecommunications data are associated with less restrictive data localisation measures in OECD countries but not in non-OECD countries.
- **International discussions on data localisation have largely taken place in the context of regional trade agreements** (RTAs). By 2022, there were 27 agreements involving 32 countries with provisions banning data localisation (each with different exceptions).
- **The business community has been outspoken about some of the implications of data localisation measures:**
  - Findings from an OECD-WTO business questionnaire highlight that, depending on the type of measure in place, data localisation could **raise data management costs by 15-55%**. In addition, over 70% of respondents did not think, or were uncertain about, links between data localisation and other public policy objectives such as domestic innovation, privacy protection or data security.
  - Data localisation measures feature prominently in the e-payments sector, especially in non-OECD countries. This not only affects the ability of firms to operate international networks but also: **increases costs for consumers, including smaller firms; raises vulnerabilities to fraud and cybersecurity risks; and reduces resilience**.
  - Data localisation requirements are also particularly burdensome for cloud service providers who rely on economies of scale to offer cheaper and more secure digital solutions. Data localisation measures can lead to **higher costs and reduced service offerings, affecting downstream users, especially SMEs, the most**. In addition, data localisation can lead to greater cybersecurity risks by reducing the ability to share 'threat data' – metadata used to identify specific types of threats or system vulnerabilities.

- Insights on air travel underscore a highly regulated and standardised set of practices supporting the processing, transfer and storage of data, especially passenger data, across different entities (airlines, booking intermediaries, airports and government agencies). **Increasing uncertainties about the growing volume of cross-cutting data localisation measures are affecting global business operations, hampering innovation and the quality of services**.

- Potential actions include:
  - Continued **monitoring of the evolving regulatory environment** to stay on top of emerging trends and wider engagement in transparency exercises.
  - Foster **discussions around moving, in principle, towards less restrictive forms of data localisation measures where possible**. For example, the use of access conditions rather than local storage requirements for non-personal data could be explored to reduce some of the unintended consequences of data localisation. Or moving from more restrictive data localisation measures which prohibit transfers towards data localisation measures with transparent conditions for transfers.
  - **Continued cooperation on these issues, in dialogue** with regulators, trade policy makers and other relevant stakeholders, including from the private sector.
  - **Continued effort to realise global rules that address data localisation** and take into account legitimate public policy objectives while avoiding excessive fragmentation, especially through discussion at the **WTO under the Joint Statement Initiative on e-commerce**.

# *The nature, evolution and potential implications of data localisation measures*

## 1. Introduction

Today, our economies and societies are digitally intertwined; connected by data flows that support how we socialise, how we produce, how we trade, and how we tackle global issues (such as the COVID-19 pandemic or the green transition). However, cross-border data flows also raise challenges across different policy domains, including how to ensure protection of privacy and personal data, national security, regulatory reach, intellectual property protection, and trade. In response to these, governments have been adopting regulations which either condition the movement of data across borders or which mandate that data is stored domestically (Casalini and López González, 2019[1])

Although the policy issues raised by data flows are diverse, a common challenge emerges: the need to ensure that, when data crosses a border, it receives the desired degree of oversight and/or protection. This combination of enabling cross-border data transfers and ensuring these take place in the context of trusted relationships has come to be known as *data free flows with trust* (DFFT).[1]

This paper aims to provide a better understanding of one important aspect of the regulatory environment that has an impact on DFFT – data localisation. The paper documents the growth in the use of data localisation measures and categorises approaches, creating a taxonomy of existing data localisation measures. It then provides a qualitative analysis of some of the perceived consequences of data localisation, connecting, through targeted business consultations, regulatory approaches to real world business examples in the e-payments, cloud computing, and air travel sectors.

The overarching aim of this work is to strengthen the evidence base on the issue of data localisation with a view to feeding into ongoing discussions, whether at the G7, under the leadership of Japan and in support to discussions on DFFT, at the WTO's Joint Statement Initiative on e-commerce, or in the context of ongoing discussions on e-commerce provisions in trade agreements.

The paper is organised as follows. The next section delves into the *what, how and why* of data localisation, identifying what it is, what the main elements of different approaches are and how these have evolved in time. Section three then provides insights on the implications of data localisation measures for business, drawing on a recent business questionnaire as well as three specific case studies and targeted consultations with businesses operating in e-payments services, cloud computing and air travel. The last section aims to identify key take-away messages for policy discussions.

[1] The term, coined by former Prime Minister Shinzo Abe in 2019 in a speech at the annual meeting of the World Economic Forum and subsequently endorsed by the G20 in the same year: https://www.mofa.go.jp/ecm/ec/page4e_000973.html

# 2. Identifying the nature and evolution of data localisation

## 2.1. What is data localisation?

There is no single, and widely accepted, definition 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 (Box 1). 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[2]) and (Svantesson, 2020[3]). However, others focus on more explicit measures which directly legislate on the location or processing of data within a particular territory (see (Casalini and López González, 2019[1]) and (Lopez-Gonzalez, Casalini and Porras, 2022[4])).

This paper focuses on the latter, defining data localisation as an *explicit requirement that data be stored and/or processed within the domestic territory* (Lopez-Gonzalez, Casalini and Porras, 2022[4]). This narrower definition avoids subjective discussions about what other measures might or might not lead to more local storage or processing .[2]

Distinctions are often made between different forms of data localisation through the use of qualifiers such as 'unjustified' or 'forced' data localisation (see (Cory and Dascoli, 2021[2])). This reflects that there is no consensus on what data localisation measures are considered to be justified. 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

**A number of definitions for data localisation have been proposed in the literature, including:**

- "Forced local data-residency requirements that confine data within a country's borders, a concept known as "data localization,"" (Cory and Dascoli, 2021[2]).
- "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[3]).
- "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]
- "We define 'data localization' measures as those that specifically encumber the transfer of data across national borders. These measures take a wide variety of

[2] Including whether emerging privacy and data protection regulation could, in some cases, be classified as data localisation measures Or even whether prohibitive tariffs that lead to tariff jumping FDI may be considered as data localisation because they might lead to more local storage than would have been the case if companies could access markets duty free from abroad.

forms - including rules preventing information from being sent outside the country, rules requiring prior consent of the data subject before information is transmitted across national borders, rules requiring copies of information to be stored domestically, and even a tax on the export of data." (Chander and Lê, 2015[6])

- "Data localization has two meanings. The first is a policy whereby national governments compel Internet content hosts to store data about Internet users in their country on servers located within the jurisdiction of that national government (localized data hosting). The data stored in the local jurisdiction may be either the sole copy of the data or a required local copy of data sent for storage or processing in another jurisdiction. The second form of data localization is a policy, whereby national governments compel Internet service providers to route data packets sent between Internet users located in their jurisdictions across networks located only within their jurisdiction (localized data routing)." (Selby, 2017[7])
- In trade agreements, data localisation often falls under articles entitled 'Location of computing facilities':
  - 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.
  - 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

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).

## 2.2. Why is data localisation emerging?

There are different reasons governments invoke as justification to adopt data localisation measures, referring to a range of different objectives, below, some of the most discussed (Casalini and López González, 2019[1]).

- They may require data to be stored domestically, citing domestic **privacy and data protection** grounds.
- 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 and integrity and continuity of critical systems 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.

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 justified public policy objective . Second, it is important to assess whether the actual objective of a measure corresponds to its stated objective. For explicit and highly restrictive data localisation measures, it is important, from a trade perspective, to assess whether the same policy objective could be achieved in a less trade restrictive way.

However, it is often difficult to assess the ultimate objective of data localisation measures. Stated objectives might not always be the ultimate objective of the measures and there might be multiple and different ultimate objectives. For instance, governments may invoke the use of data localisation policies for cybersecurity reasons but ultimately seek to use this as a means of furthering a protectionist digital industrial policy.

## 2.3. What are the main approaches to data localisation?

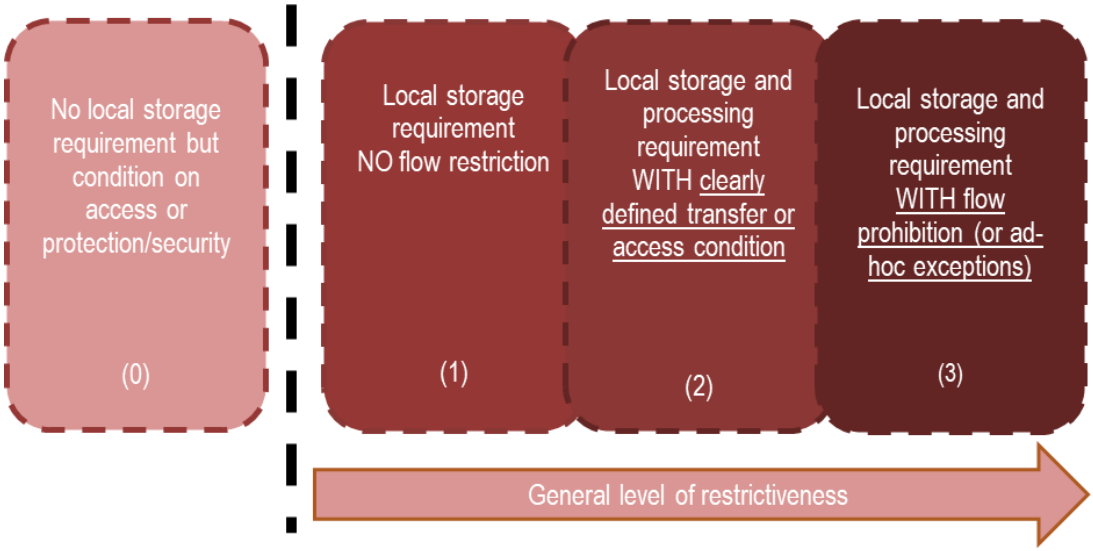
Data localisation measures in place today vary widely, often in relation to their underlying policy objectives; the sectors or types of data targeted; and the wider legal and policy environment. Even within a particular country, or across regions, different types of data localisation measures can apply to different types of data (e.g. personal data or non-personal, data pertaining to different sectors such as: health data, telecommunication data, banking or payment processing data; insurance data; or satellite and mapping data to name but a few).[3] There are also cases where data localisation requirements are aimed at less

[3] Notwithstanding the fact that it can be difficult to separate personal and non-personal data.

well-defined data categories such as "important data" or "critical data" and operators such as "critical information infrastructure operators" or "network operators".

Overall, data localisation measures can be grouped into three broad, although not sharply delineated, categories (Figure 1).[4] 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.[5]

## Figure 1. A typology of approaches to storage and processing requirements




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: Adapted from (Lopez-Gonzalez, Casalini and Porras, 2022[4]).

The first category of approaches refers to **measures that require local storage of data, without prohibiting storage or processing in other countries** (Category 1). 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 tend to target business records (accounts), telecommunications or financial data, including in the context of data retention policies. For example, Sweden's Accounting Act stipulates that accounting information is to be retained and stored for seven years in Sweden.[6] Similarly, the United Kingdom's Company's Act (2006) stipulates that accounting information can

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

[5] 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. It is worth recalling that, for the purposes of this work only explicit requirements to store locally are taken into consideration.

[6] 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

be stored abroad but that a copy must be kept in the UK at all times.[7] To some extent, some of the emerging rules in this category 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.

The second category of measures are those that **require local storage and processing but allow international access or transfers on the basis of clearly defined conditions** (Category 2). These are relatively new approaches. They include the Electronic Health Records Act in Australia which 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. The conditions for transfer relate, either to the characteristics or integrity of the data or to ensuring access (see Box 2 for examples of these measures).

### Box 2. Examples of storage requirements with flow conditions (Category 2)

To date, storage requirements with flow conditions are relatively rare, 2 instances have been found, both in the case of health data, across OECD countries.

Australia's **Personally Controlled Electronic Health Records Act** requires that personal health records be stored only in Australia. Nevertheless it foresees the possibility of transfers where the data subject or the registered healthcare provider organisation need access while overseas. Moreover, the Act specifies the following conditions:

*The System Operator is authorised, for the purposes of the operation or administration of the My Health Record system:*

*a) to hold and take such records outside Australia, provided that the records do not include:*

*i. personal information in relation to a healthcare recipient or a participant in the My Health Record system; or*

*ii. identifying information of an individual or entity; and*

*b) to process and handle such information outside Australia, provided that the information is neither of the following:*

*i. personal information in relation to a healthcare recipient or a participant in the My Health Record system;*

*ii. identifying information of an individual or entity.*

**The Personal Health Information and Access Act** in New Brunswick, Canada, requires local storage but also foresees conditions for access outside Canada under specific conditions:

Unless otherwise provided in the regulations, a public body shall ensure that personal health information in its custody or under its control is stored only in Canada and accessed only in Canada, unless one of the following applies:

[7] See Companies Act 2006 c.46, part 15, Chapter 2, section 388 (Companies Act 2006 (legislation.gov.uk).

*a) if the individual to whom the information relates has identified the information and has consented, in the manner prescribed by regulation, to it being stored in another jurisdiction;*

*b) if the information is stored in another jurisdiction for the purpose of disclosure allowed under this Act;*

*c) if the information was disclosed for the purposes of (i) a payment to be made to or by the Province or a public body, (ii) authorizing, administering, processing, verifying or cancelling a payment to be made to or by the Province or a public body, or (iii) resolving an issue regarding a payment to be made to or by the Province of or a public body*

As can be seen, both instances provide for strong localisation requirements, nevertheless, they also provide language that helps identify the specific conditions under which a transfer would be allowed.

The third category of approaches refers to **measures that mandate local storage and processing of data while also prohibiting transfers to other countries (or only on the basis of ad-hoc authorisations)** – Category 3. 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. Often, these approaches are less transparent and more ambiguous in terms of the scope of application. They include, for instance, in Indonesia, Regulation 71 (2019) concerning the implementation of electronic systems and transactions[8] which 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 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 (see Box 3) which is included here by virtue of the broad definition and ambiguous standard which can make these measures more restrictive than necessary and undermine regulatory transparency. There are also a number of other draft legislation which mandate local storage with transfer prohibitions in China. These include article 6 of the Effective Protection of Personal Financial Information by Banking Institutions or Article 10 of the Administration of Population Health Information.

### Box 3. Recent developments in China on security assessments for the transfer of certain types of data abroad

The 2017 Cybersecurity Law of the People's Republic of China (PRC), the 2021 Personal Information Protection Law (PIPL), and the 2021 Data Security Law jointly form the main regulatory framework governing the collection, processing, transfer and storage of data in China. All three instruments impose a requirement that personal information and *important data* collected and generated in China by *critical information infrastructure* operators must be stored domestically, and if transfer abroad is necessary,

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

a *security assessment* must be carried out (see Article 37 of the Cybersecurity Law, Article 38 and 40 of the PIPL, and Article 31 of the Data Security Law).

In July 2022, the Cyberspace Administration of China (CAC), the cyberspace regulator, released new Measures for Security Assessment for Outbound Data Transfer that came into force on 1 September 2022. The aim of this instrument is to specify the circumstances when a security assessment is needed and provide some details on the process. Outbound transfer is defined both as the sending of data abroad as well as the accessing, retrieving, and downloading of such data from abroad.

Article 4 of the Measures outlines four situations where a security assessment is necessary before an outbound transfer can take place:

1) In cases where the transfer concerns "important data", which is broadly defined as data that could endanger national security, economic operation, social stability, public health and safety;
2) In case the transfer concerns personal data by a critical information infrastructure operator or processor of personal information that processed data for 1 million or more individuals;
3) Also in the case of transfers concerning personal data by a personal information processor that has made outbound transfers of personal information of 100,000 individuals or sensitive personal information of 10,000 persons in the preceding year;
4) Lastly, the CAC may also require security assessment in other situations which are not further defined.

In terms of the process, there are three main steps that data processors need to undertake:

- A self -assessment on the risks related to the outbound transfer of the data;
- Submit the application first to the provincial level regulator, which includes several documents such as the self-assessment and other materials demonstrating protection of the data in the receiving end;
- Submit the application to the CAC, the national regulator that will make an assessment within 45 days.

Article 8 of the Measures covers the factors that the CAC will take into account when undertaking a security assessment. The assessment includes a wide range of aspects, for example:

- the risks that the transfer may entail for national security or public interests, among other policy objectives;
- Legitimacy, necessity and method of transfer;
- Whether the level of data protection in the recipient country meets the requirements of laws in China;
- Sensitivity of the data and risks of being tampered with abroad;
- Agreed safeguard measures between the data processor and data recipient;
- Any other matter that the CAC deems necessary.

In case of unfavourable outcomes, the data handler can ask the CAC for a re-assessment with a final decision. In case of a positive decision, the permission to transfer data

abroad is valid for two years but if substantial changes in the risk factors arise, a new assessment might be needed.

Source: Authors' assessment

Outside this typology, a new category of approaches about access rather than location 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. A useful example of this can be found in the context of Denmark's Bookkeeping Act (see also Box 4). From 2006 to 2015, the Act required data to be stored in Denmark with clear conditions for transfer and storage abroad, making this a Category 2 data localisation measure. However, by 2015, the Act drops the local storage requirement in favour of access conditions stipulating that a requirement for access be given to Danish public authorities (when justified). 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.[9] Within the European Union, legislation on the movement of non-personal data forbids data localisation within the European Union, but requires that data be made accessible to the relevant authorities.[10]

This emerging regulation largely covers non-sensitive data such as business records or non-personal data. The conditions for access include notices of where the data might be stored; requirements for an agreement to exchange information to be in place; or requirements that records be kept according to domestic guidelines irrespective of where these are stored.

### Box 4. Examples of no local storage requirements but condition on access (Category 0)

**Danish Bookkeeping Act (2015)**

*Section 12. The accounting material must be stored in such a way that it can be made available in Denmark without difficulty to public authorities and others who, under other legislation, have the right to demand access to the accounting material.*

*Paragraph 2. The accounting material may be stored in electronic form in Denmark or abroad if the person responsible for bookkeeping 1) keep the accounting records in accordance with this law, 2) can at any time obtain the material and provide access to it in this country; 3) store any descriptions of used systems, etc. and any necessary passwords, etc. in this country, and 4) ensure that the accounting records are printed in clear print or made available in a recognised file format.*

**Brazil's Resolution CMN No. 4,893 of 26 April 2021**

*Art. 11. The institutions mentioned in art. 1 must ensure that their policies, strategies and structures for risk management established in regulation in force, specifically regarding to the criteria for decision on the outsourcing of services, include the*

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

[10] 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).

*contracting of relevant data processing, data storage and cloud computing services, in the country or abroad.*

*Art. 16. The contracting of data processing, data storage and cloud computing relevant services provided abroad must fulfil the following requisites:*

*I. the existence of an agreement for exchange of information between the Central Bank of Brazil and the supervisory authorities of the countries where the services may be provided;*

*II. the contracting institution must ensure that the provision of the services mentioned in the heading do not cause damage to its own functioning neither do they deter the action of the Central Bank of Brazil;*

*III. the contracting institution must define, previously to the contracting, the countries and the regions in each country where the services can be provided and the data can be stored, processed and managed; and*

*IV. the contracting institution must anticipate alternatives for business continuity either in the case of impossibility of continuation of the contract or in the case of its termination.*

**New Zealand's Goods and Services Tax Act 1985 updated 2022**

Section 75 (3BA) A registered person required by subsection (3) to keep and retain a record must keep and retain the record—

a) in English or te reo Maori, or in a language in which the Commissioner authorises the person under subsection (6) to keep the record or the type of record; and

b) at a place in New Zealand, or at a place outside New Zealand where—

i. the Commissioner authorises the registered person under subsection (6) to keep the record or the type of record:

ii. the record is kept by a person authorised by the Commissioner under subsection (6) to keep records for persons that include the registered person.

**Mexico's Federal Telecommunications Law article 190 (II)**

*Article 190. The telecommunications concessionaires and, where appropriate, the authorized ones must:*

*II. Maintain a record and control of communications that are made from any type of line that uses its own or leased numbering, under any modality, that allow the following data to be identified with precision:*

*[…]*

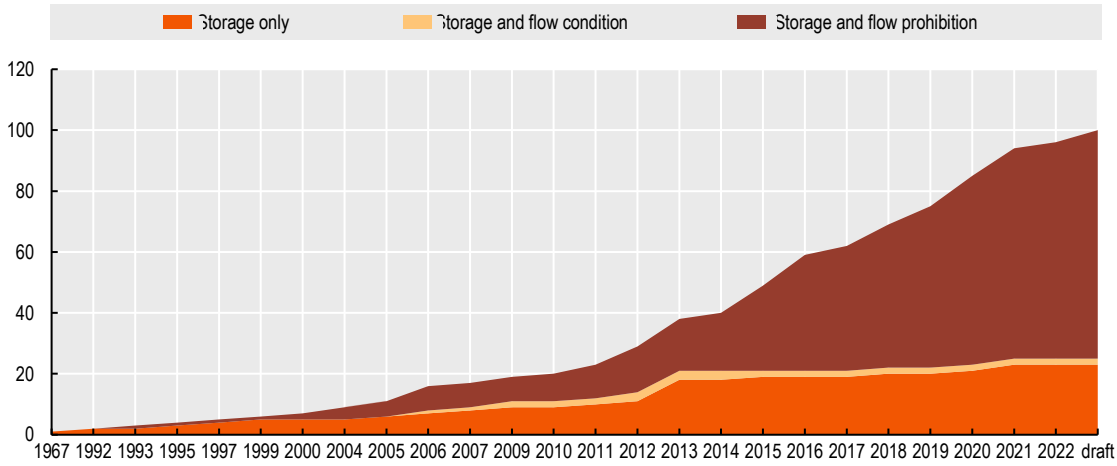
*Data should be retained for 12 months [..] in systems that permit real time access to competent authorities through electronic means.*

*[the regulation provides for clear access conditions without mentioning location]*

## 2.4. How have data localisation policies evolved?

The number of explicit data localisation measures has been increasing (Figure 2). By early 2023, there were 96 measures across 40 countries in place and 4 draft regulations (counting that three measures that were previously in place had been revoked). Nearly half of the identified data localisation measures have emerged after 2015. Importantly, the measures themselves are becoming more restrictive; by early 2023, more than two-thirds of identified measures involved a storage requirement with a flow prohibition (Category 3).

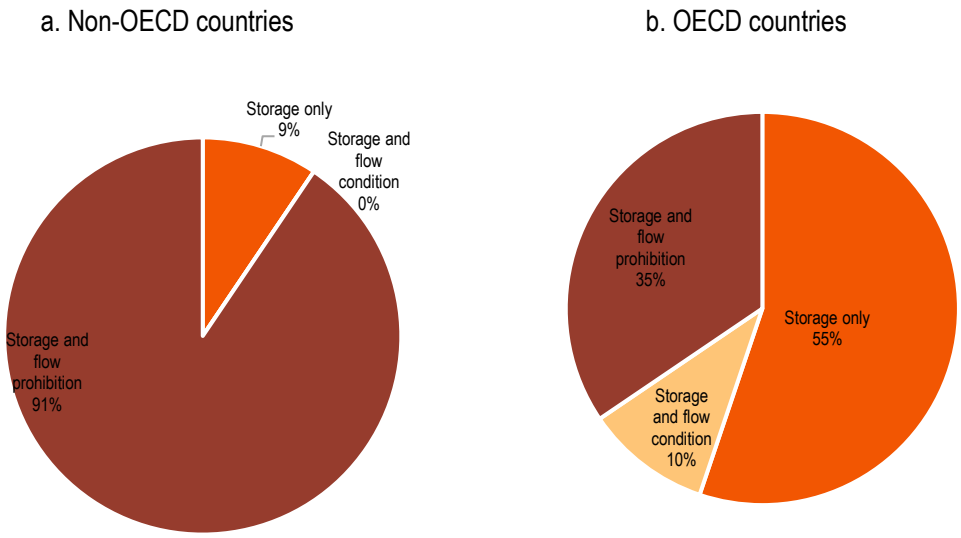
### Figure 2. Data localisation is growing and becoming more restrictive




Note: Data localisation measures are defined as explicit requirements that data be stored or processed domestically.
Source: Author's compilation based on own compilation including through the Digital Trade Alert, the OECD Digital STRI and Cory and Dascoli (2021[2]).

Data localisation measures are more prevalent across non-OECD countries – around 70% of all measures (74 in total). Non-OECD country measures are also more restrictive (Figure 3). Indeed, overall, 55% 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 91% of identified data localisation measures).

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



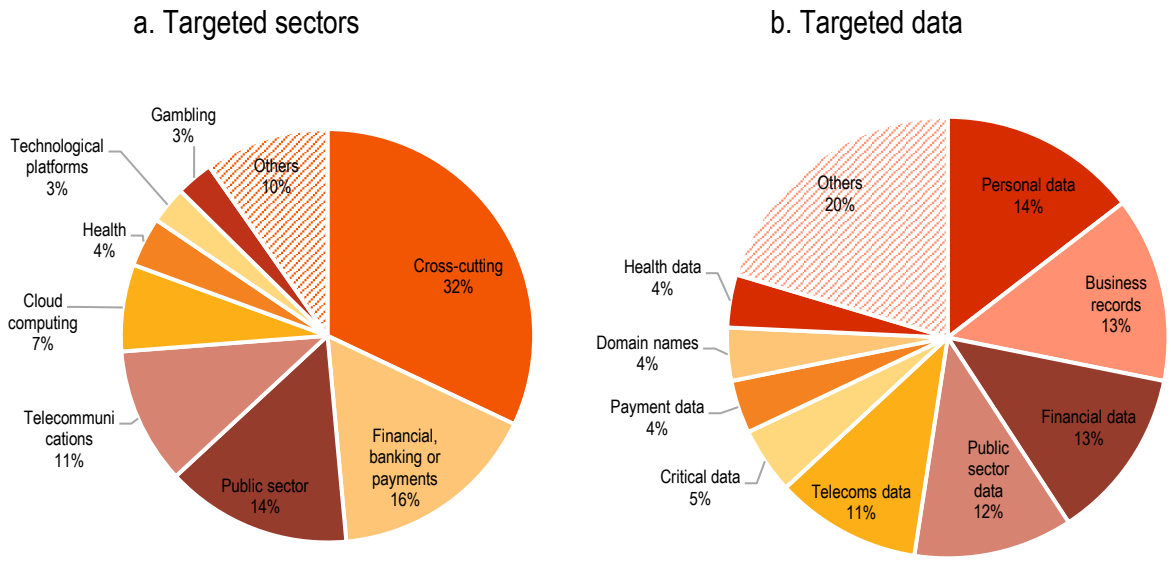

Note: Data localisation measures are defined as explicit requirements that data be stored or processed domestically. In the order of least restrictive to most restrictive: Storage only refers to Category 1 in Figure 1. Storage and flow condition refers to Category 2 in Figure 1 and Storage and flow prohibition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

Data localisation also affects a diverse range of data (personal and non-personal) and sectors.[11] In terms of sectors (Figure 4a), 32% of data localisation measures identified are cross-cutting, meaning that they have implications across all sectors of the economy. Around 16% of measures identified apply to financial, banking or payments sectors, a further 14% of to the public sector and 11% to telecommunications sectors. The remaining 27% of measures apply to cloud computing, health, gambling, tech platforms and other sectors (overall, not counting cross-cutting measures, 13 sectors are identified as being affected).

Where data types are concerned (Figure 4b), the five largest categories are: personal data (14% of measures), business records (13%), financial data (13%), public sector data (12%), and telecoms data (11%). The remaining 37% of measures apply to 17 different types of health data to critical data, scientific data or data from judicial investigations.

[11] 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[14])).

## Figure 4. Data localisation measures by sector and data type




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.

There are also stark differences in how OECD and non-OECD countries approach regulation (Table 1). For instance, cross-cutting data localisation measures, which largely relate to non-sensitive data such as business records, is approached, in OECD countries, through local storage requirements with no flow restriction. By contrast, in non-OECD countries, these measures are largely approaches using the most restrictive forms of data localisation regulation (Category 3). This is also the case for telecommunications, health and gambling data.

## Table 1. Approaches to data localisation vary significantly across sectors and regions

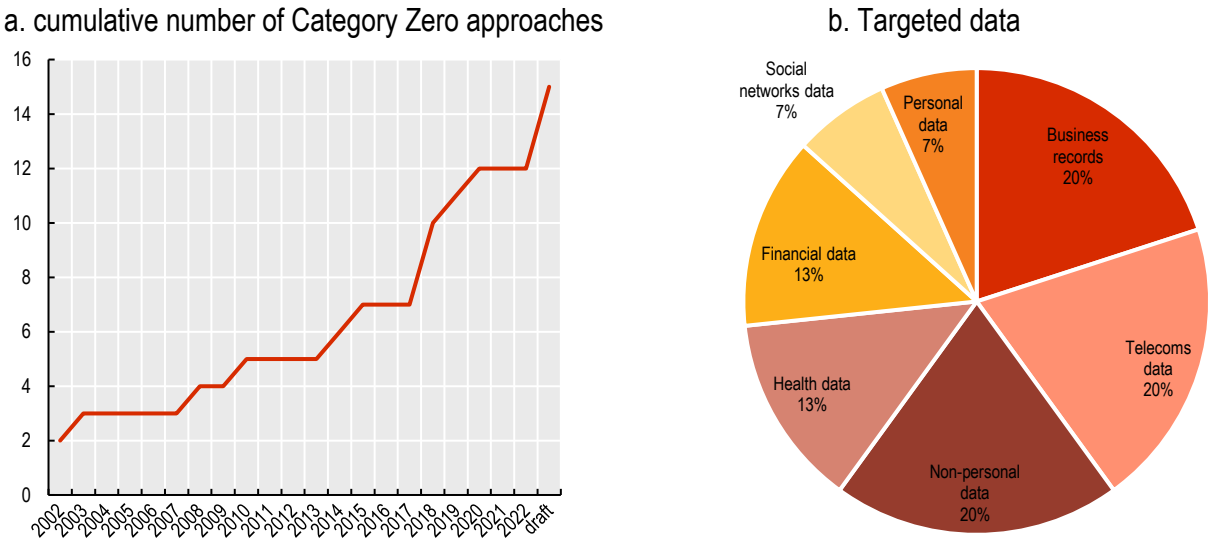
Approaches to data localisation by sector and category across OECD and non-OECD countries

| | non-OECD | | | | OECD | | | |
|---|---|---|---|---|---|---|---|---|
| | Cat. 1 | Cat. 2 | Cat. 3 | Tot | Cat. 1 | Cat. 2 | Cat. 3 | Tot |
| Cross-cutting | 25% | 0% | 75% | 24 | 100% | 0% | 0% | 9 |
| Financial, banking or payments | 0% | 0% | 100% | 12 | 40% | 20% | 40% | 5 |
| Public sector | 0% | 0% | 100% | 9 | 33% | 0% | 67% | 6 |
| Telecommunications | 0% | 0% | 100% | 9 | 100% | 0% | 0% | 2 |
| Cloud computing | 0% | 0% | 100% | 5 | 0% | 0% | 100% | 2 |
| Health | 0% | 0% | 100% | 2 | 0% | 100% | 0% | 2 |
| Gambling | 0% | 0% | 100% | 2 | 100% | 0% | 0% | 1 |
| Other | 9% | 0% | 91% | 11 | 0% | 0% | 100% | 2 |
| TOTALs | 9% | 0% | 91% | 74 | 55% | 10% | 35% | 29 |

Note: values show share of measures approached using specific categories from the taxonomy. For instance, first entry shows that 25% of the data localisation measures that are cross-cutting in place across non-OECD countries can be classified as Category 1 data localisation measures (that is local storage conditions without flow restrictions). Tot indicates the number of measures identified across all categories by sector.
Source: Author's compilation.

Increasingly, countries are relying on approaches which require access to data rather than imposing localisation requirements (Category zero in Figure 1). Approaches under this category have been growing, by 2022, 12 were in place with 3 additional in draft form applying, among other, to business records, telecoms data and non-personal data (Figure 5). These are largely applied by OECD countries (73% of Category zero measures).

**Figure 5. Measures that mandate access rather than imposing location requirements are on the rise**



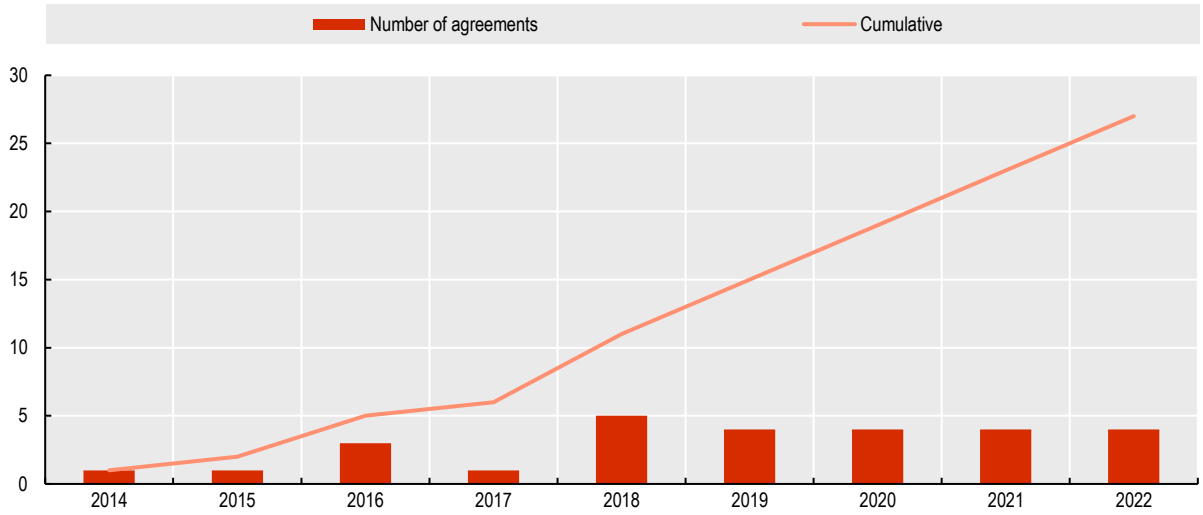

Note: Category zero measures are those that do not impose local storage requirements but condition on access or protection /security.
Source: Author's compilation.

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

Discussions on data localisation often arise in the context of regional trade agreements. Indeed, as of November 2022, 27 agreements involving 32 countries had provisions prohibiting data localisation as a condition for conducting business (Figure 6).[12] The countries with most provisions are Singapore (9), Australia (9), Chile (6), and Japan (5). These either ban or limit data localisation, often under headings entitled 'location of computing facilities' subject to different exceptions (Lopez-Gonzalez, Casalini and Porras, 2022[4]). These provisions have only started emerging since 2014, perhaps in reaction to the rise in data localisation measures, as noted in Figure 2.

[12] See Annex A for a list of agreements (based on the TAPED database (Burri and Polanco, 2020[8])).

## Figure 6. Data localisation provisions in RTAs




Note: See Annex Table A1 for a list of agreements.
Source: Author's compilation based on TAPED database (Burri and Polanco, 2020[8]).

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).[13] 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 (Lopez-Gonzalez, Casalini and Porras, 2022[4]).

## 3. Identifying some of the implications of data localisation for businesses

Three key messages emerge from the analysis. The first is that data localisation is on the rise, the second that this data localisation is becoming increasingly restrictive, especially across non-OECD countries, and the third that trade agreements provide language curtailing some forms of data localisation (albeit with different exceptions).

Having mapped the regulatory environment, this section turns to identifying some of the issues that this landscape raises for businesses. It does so, first, by drawing on insights from an OECD-WTO business questionnaire that was administered in the summer of 2022. And second, via targeted consultations with enterprises operating in the three focus sectors: cloud computing; e-payments and air transport.

This section discusses findings from business consultations. This is without prejudice to the approaches taken by individual countries in the context of their sovereign decisions to adopt data localisation approaches that might best reflect their regulatory objectives.

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

## 3.1. Insights from a business questionnaire

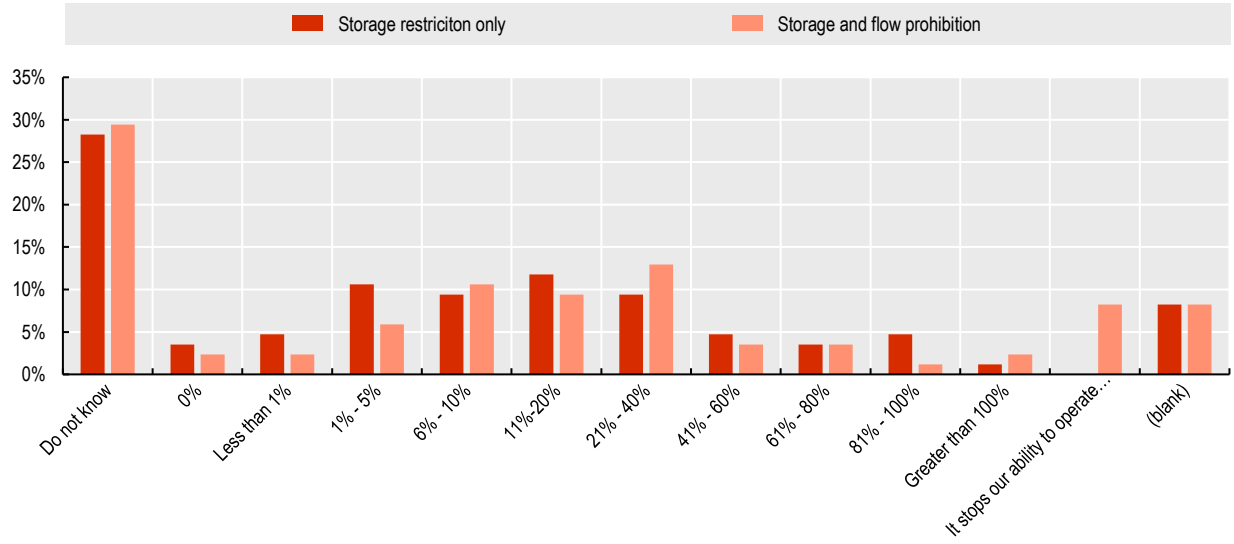
The OECD-WTO Business Survey was administered online during the period 9th of May – 14th of June 2022. It garnered over 400 views with 85 full responses across 32 countries covering most sectors of economic activity. The questionnaire was developed to better understand how data policies, including measures affecting the movement of data and measures requiring data to be stored domestically, affect business activities. Although not developed for this particular paper, insights from this questionnaire can be useful to identify business perceptions of data localisation measures.

The OECD-WTO questionnaire asked businesses to provide insights into the potential costs associated with data localisation measures distinguishing between simple storage requirements (Category 1 approaches) and more prohibitive data localisation measures which combined storage requirements with flow prohibitions (Category 3 approaches)

Overall, the results suggest that, on average, businesses perceive that local storage measures with no flow restrictions can lead to increases in data management costs of around 16%. If local storage is combined with flow restrictions, the impacts can be considerably higher, at around 55% (see Figure 7).[14] Importantly, 8% of respondents said that more prohibitive data localisation measures would *stop* their ability to operate internationally.

The OECD-WTO questionnaire also asked about the extent to which data localisation measures also helped deliver other legitimate public policy objectives (Figure 8). The results clearly show that most businesses (around 70% of respondents) did not think, or were uncertain about, links between data localisation and domestic innovation, privacy protection or data security.

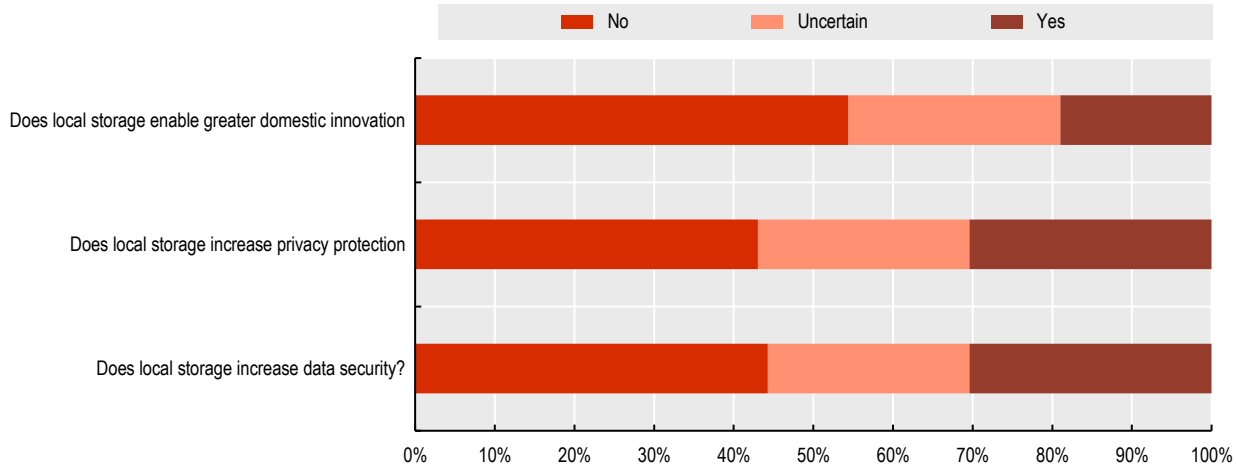
### Figure 7. Perceived impact of data localisation on data management costs




Note: Businesses were asked the extent to which different measures would affect their total data management costs (including ICT equipment and legal costs).
Source: OECD-WTO Business Questionnaire

[14] To get to this number, the average cost increase in the given bracket was taken and multiplied by the share of responses that chose that bracket. For cost increases that led business to claim that they would stop their activities costs of 500% are assumed.

**Figure 8. Other public policy objectives and data localisation**




Source: OECD-WTO Business Questionnaire

## 3.2. Insights from targeted consultations with businesses

Business consultations can help provide illustrative examples of how companies perceive and respond to emerging data localisation measures. To better grasp the direct, but also the more indirect, or unintended, consequences of data localisation regulation, structured business consultations were held during the period spanning February to April 2023. Firms were asked a set of 6 questions (see Annex B) about perceptions towards different approaches to data localisation, including in their consequences. Three sectors were targeted, cross-border e-payments, cloud computing and air travel.[15]

### *3.2.1. Cross-border e-payments*

*How does it work?*

Payments conducted electronically, through digital or online modes, are a key element of the evolving digital landscape, underpinning both domestic and international transactions. They include credit or debit card payments, internet banking, e-wallets, mobile money, gift cards, etc.. When they involve merchants (recipients of the payments) and consumers (issuers of the payments) located in different countries, they are known as cross-border e-payments.[16]

Since domestic payment systems are not directly connected internationally, and cross-border transfers can be costly and take time, e-payments do not generally imply direct transfers of currency across borders. Instead, a complex system of interbank credits and debits is set in motion. When a consumer in country A places an order for a good in country B, data, from the consumer to the merchant bank flows either directly or via a payment network. Approval of this payment is generally done after an artificial intelligence, or machine learning, driven fraud detection analysis. Once approved, the consumers bank

[15] The selection of firms was organised through direct contact with businesses, business associations and Business at OECD. Overall, 11 companies were interviewed, largely headquartered in G7 countries but with global operations.

[16] However, even domestic transactions can involve cross-border payments when undertaken with global vendors that operate international transaction networks.

agrees to credit the merchant bank the sum of the transaction, often through the consumers' bank account with the merchant bank, or, in its absence, via one or various correspondent banks or payment networks.[17]

The entire process, which can take seconds, relies on the movement of different types of data across international borders. As e-payments proliferate, whether through growing use of contactless payments, digital platforms or other e-commerce transactions, the volume of transactions has also been growing, as have consumer expectations for faster and more reliable payment systems.

### *What does the regulatory landscape look like for e-payments?*

After *cross-cutting measures*, which include, among others, regulations on business records and privacy, *financial, banking or payment sectors* face the highest number of data localisation measures (16% of the measures identified). These include, among others, strict data localisation requirements (Category 3 approaches) in India that mandate all payment data to be stored locally, as well as requirements to keep local copies of payment data in domestic servers for access by regulators in Chile (Category 1)[18].

There are clear divides in approaches to regulating these sectors across OECD and non-OECD countries. Out of the 17 data localisation measures identified, 12 arise in non-OECD countries (as shown also in Table 1). These take the most restrictive form of data localisation regulation (Category 3). By contrast, measures in OECD countries, of which five are identified, only two require local copies to be kept domestically, without restricting the transfer of data for processing or storage abroad (Category 1). One non-OECD country, Brazil, has recently, in 2021, started approaching data regulation in this sector by requiring access of data to regulators instead of mandating local storage (Category 0).

### *How does data localisation affect businesses in this sector?*

Interviews with stakeholders from the business community highlighted that the proliferation of data localisation measures in the e-payment sector has led to an overall increase in the cost of operating domestically and across geographical borders. This is especially the case for operations outside OECD countries, with explicit references made to the particularly onerous data localisation measures in India and in China.

However, businesses stressed that any form of local storage can be costly, even simple storage requirements with no flow restrictions (Category 1). This is because, despite server space being relatively cheap, keeping local copies of data also requires duplicating measures to maintain high levels of data security across connected payment networks. This implies significant additional capital and personnel costs. Indeed, businesses operating in this sector tend to prefer centralisation of servers, helping facilitate processing and data security. Having to setup additional servers to meet data localisation measures entails ensuring that the overall integrity and security of the payment network system is maintained, which can be costly and adds complexity.

[17] E.g. if the consumers bank does not hold an account in the merchants bank it will rely on a correspondent bank were both holds accounts. If that is not the case, they can use different banking networks.

[18] The modification in 2019 of Chapter 20-7 of the Bank Circular 2409, Financial Circular 798 still provides that institutions that carry out activities abroad considered significant or strategic must have a contingency data processing center located in Chile, but it has also introduced the possibility to obtain an exemption from this, subject to the conditions laid out in the law.

In some countries, which have large enough markets and there is a strong business case for continuing to operate, these costs are faced, however, businesses might: i) reduce the amount of services offered; ii) pass on the cost increases to consumers. In smaller markets where it can be more difficult to make a business case, companies may even decide to pull out of business operations or not make further investment there.

In addition to these more direct impacts on businesses, a range of indirect impacts or unintended consequences were also highlighted:

- **Reduced efficiency of e-payment systems**. Wider fragmentation and increases in complexity of the global payment systems reduce efficiencies, including via less capacity to take advantage of economies of scale. This can mean longer waiting times and higher transaction costs for users.
- **Less secure and reliable e-payment systems subject to increased risk of cyberattacks**. Growing data localisation measures lead to less secure and reliable payment systems by hindering the ability of firms to identify and avert cybersecurity incidents and risks.[19] Timely access to relevant information is key to effectively respond to cyberattacks, limiting their impact, as well as preventing future threats.
- **Decreases in competition in e-payment markets**. Data localisation requirements have the potential to distort the playing field in favour of national suppliers of e-payment services. Often, local companies, which do not have access to global technologies and networks can provide lower quality and more expensive services.
- **Increased risk of data loss from natural disasters and reduced resilience**. Natural disasters might impact particular geographic locations generating irreversible data losses if companies store all their data in that location. Data localisation, for example, may prohibit backups to a geographically remote facility: having data geographically distributed is a crucial element to increase resilience.
- **Reduced ability to detect and prevent fraud**. Data localisation requirements hinder effective fraud detection and prevention which relies on careful analysis of data through machine learning and AI techniques to detect fraud attempts. The more available data, the more effective the model is at detecting fraud. Data localisation measures create data fragmentation that limit the effectiveness of fraud detection systems. Indeed, IIF (2023) found that the adoption of measures requiring local storage combined with prohibitions to share this data could lead to a 50% loss in fraud modelling.[20]
- **Negative "downstream effects", particularly on small businesses**. Data localisation requirements may have negative impacts on small businesses which rely on online payment processors to scale-up and expand into foreign markets through digital trade.[21]
- **Uncertainty about regulation, including in terms of scope and how it applies**. Data localisation regulation is not always straightforward in terms of scope and application. This leads to uncertainties which can reduce efficiencies and add to

[19] See https://www3.weforum.org/docs/WEF_Addressing_E-Payment_Challenges_in_Global_E-Commerce_clean.pdf

[20] See IIF (2023), Data policy impacts – Fraud prevention, January 2023

[21] See https://www.govinfo.gov/content/pkg/CHRG-114hhrg97419/pdf/CHRG-114hhrg97419.pdf

existing costs. this is especially the case for foreign businesses (although also for domestic firms).

### *3.2.2. Cloud computing*

*How does it work?*

Cloud computing is defined by the US National Institute of Standards and Technology (NIST) as "a model for enabling ubiquitous, convenient, on demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction".[22] In other words, cloud computing allows users to rent IT resources (computing power, storage and database management) on a "pay-as-you-go pricing" basis.[23] One key advantage it offers users is the ability to scale up or down activities without needing to undertake important capital investments. This can be especially important for smaller firms, enabling them to better face changes in demand.

The use of cloud computing has been growing and is expected to continue to grow. Gartner (2022[9]) forecasts a 20.7% growth in global end-user spending on public cloud services, reaching a total $591.8 billion in 2023. Cloud computing providers offer different models of use to companies, governments and individuals:

- *Infrastructure-as-a-service (IaaS)*, where users have access to a common infrastructure, as in the case of storage of data on the cloud;
- *Software-as-a-service (SaaS)*, where users can host and manage software applications through licences;
- *Platform-as-a-service (PaaS)*, where users have access to a platform environment to create software applications.

Moreover, end-users can also choose among different types of deployment of cloud services: whether public, private or hybrid cloud. Another key element of the services provided relates to strong cybersecurity.

Cross-border data flows are integral to cloud computing. Indeed, the cloud is a vast network of remote but interconnected servers located around the world that allow access to files and data from any Internet-capable device, irrespective of the geographical location from where data are accessed. Files and data stored in the cloud can potentially be stored in servers located in different jurisdictions or can potentially be transferred from one jurisdiction to another (OECD, 2014[10]). Cloud services providers offer detailed information about the countries in which datacentres are located.[24] They also offer tailor-made solutions to comply with different localisation requirements, including with respect to public data through government contracts.

---

[22] See The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology, available at https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

[23] 'Pay-as-you-go pricing' entails that users of cloud computing do not need to invest in hardware or pay for capacity that it is not used; nor they need to invest in the infrastructure or datacentres and take care of their maintenance. Users only pay for the resources consumed. They access the resources on the internet, using the infrastructure systems of the cloud providers.

[24] See as examples Google Cloud, IBM Cloud, AWS, Azure

*What does the regulatory landscape look like for cloud computing?*

The alleged motivations behind the introduction of data localisation requirements are largely in the context of ensuring data safety, national security, and the respect of human rights, as well as ensuring that governments can access data in the event of judicial proceedings. However, some businesses have argued that there are also increasing objectives to use data localisation measures to favour domestic industries, such as cloud computing companies over foreign competitors.

Seven data localisation requirements in the cloud computing sector have been identified, two of which are in draft form. These mostly concern public sector data and occupy, across both OECD and non-OECD countries, Category 3 approaches, that is, measures that mandate local storage and prohibit cross-border data flows.

In non-OECD countries, notable approaches include India's adoption of guidelines that state that government departments must introduce specific contractual terms with cloud services providers to ensure that all public sector data residing in cloud storage networks must be located on servers in India.[25] Saudi Arabia introduced a cloud computing regulatory framework that contains an obligation for cloud providers to store and process public sector data inside the country.[26] In addition, Saudi Arabia introduced a cybersecurity framework that requires that financial institutions use only cloud services located in the country.[27] South Africa introduced a draft policy mandating that critical information must be processed and stored in South Africa, irrespective of the location where the cloud provider is domiciled[28]; Vietnam discussed a draft telecommunication law that mandates that cloud computing services providers are responsible of storing data in the country.[29] In the Ukraine, data localisation measures were introduced in 2022 but later revoked in the context of the Russian war of aggression (see Box 5)

In OECD countries, the U.S. adopted a strict localisation policy for defence-related data, requiring that cloud service providers that store government data must store them within

[25] See Ministry of Electronics and Information Technology (MeitY), 2017 Guidelines for Government Departments On Contractual Terms Related to Cloud Services, available at https://www.meity.gov.in/writereaddata/files/Guidelines-Contractual_Terms.pdf

[26] See Communication, Space, and Technology Commission, 2020 Cloud Computing Regulatory Framework, available at https://www.cst.gov.sa/en/RulesandSystems/RegulatoryDocuments/Documents/CCRF_En.pdf

[27] See Saudi Arabia Monetary Authority, 2017, Cyber Security Framework, available at https://www.sama.gov.sa/en-US/RulesInstructions/CyberSecurity/Cyber%20Security%20Framework.pdf

[28] See Communication and Digital Technologies, 2021 Draft National Policy on Data and Cloud, available at https://www.gov.za/sites/default/files/gcis_document/202104/44389gon206.pdf

[29] See Ministry of Information and Communications, 2022 Amended Telecommunication Law, available at https://chinhphu.vn/du-thao-vbqppl/du-thao-luat-vien-thong-sua-doi-5329

the U.S.[30] Furthermore, Türkiye adopted a circular requiring that public sector data stored in the cloud must be located in the country.[31]

### Box 5. Data localisation and the Ukraine

In March 2022, the Ukraine introduced the Cloud Services Law prohibiting government authorities from processing and storing data in the public cloud and requiring servers to be physically located within the country's border.[1] However, in recognition to the vulnerabilities this created in the context of the ongoing war, Ukraine's Parliament took action, amending this data localisation requirement to allow government data to be stored abroad and in the cloud through specific war-time regulation.[2]

Ukraine's Minister of Digital Transformation solicited tech companies to help Ukraine perform a data migration from existing servers to the cloud and towards servers located abroad.[3] A few months after Russia's invasion of Ukraine, Amazon Web Services reported to have effectively assisted Ukraine by "providing the Ukrainian government with access and resources for migrating to the cloud and securing critical information".[4] Other cloud services providers, such as Microsoft[5] and Google[6], granted technology support to allow Ukraine to run their digital infrastructure and services into the cloud.

Source: Authors' assessment

---

[1] Article 11 of the Ukrainian Cloud Services Law stated that:

> "it is prohibited to process information constituting a state secret, official information, state and unified registers, the creation and maintenance of which is established by law, using cloud resources and/or data processing centers located abroad or in the temporarily occupied territory of Ukraine, or belonging to the state recognized by the Verkhovna Rada of Ukraine as an aggressor state or an occupying state, or belonging to entities whose activities are subject to the Law of Ukraine "On sanctions" and on which a decision was made to apply sanctions in Ukraine."

[2] Resolution No. 263 of the Cabinet of Ministers of Ukraine, dated 12 March 2022, determines that in a warlike situation, additional measures apply, including to locate public information resources and public e-registers as well as their encrypted reserve copies **on the cloud resources or data centers outside Ukraine**

> Draft Law 7152 "On Amending Some Laws of Ukraine Concerning Maintenance of Functioning of Information and Communication Systems, Electronic Communication Systems, Public Electronic Registers" dated 13 March 2022 **allows locating public e-registers abroad during the martial law and up to six (6) months after cancellation of the martial law**

[3] See https://www.nytimes.com/2022/03/12/technology/ukraine-minister-war-digital.html

[4] See https://www.aboutamazon.eu/news/community-engagement/supporting-humanitarian-efforts-in-ukraine

[5] See https://blogs.microsoft.com/on-the-issues/2022/11/03/our-tech-support-ukraine/

[6] See https://cloud.google.com/blog/products/identity-security/how-google-cloud-is-helping-those-affected-by-war-in-ukraine

---

[30] See Defense Acquisition Regulations System, Department of Defense (DoD), 2015 Defense Federal Acquisition Regulation Supplement: Network Penetration Reporting and Contracting for Cloud Services (DFARS Case 2013-D018), available at https://www.federalregister.gov/documents/2015/08/26/2015-20870/defense-federal-acquisition-regulation-supplement-network-penetration-reporting-and-contracting-for#sectno-reference-239.7602-2

[31] See 2019 Presidential Information and Communication Security Measures Circular No. 2019/12, available at https://cbddo.gov.tr/mevzuat/2019-12-sayili-bilgi-guvenligi-tedbirleri-cumhurbaskanligi-genelgesi/

*How does data localisation affect businesses in this sector?*

Data localisation requirements can be problematic for cloud providers given that "location independence" is a core aspect of the cloud delivery model. However, regulatory requirements, as well as users' concerns over the storage location of data, push cloud service providers to increase their transparency over the locations in which their servers are located.

Interviews with companies revealed that data localisation requirements can lead to:

- **Increased costs of providing cloud computing services**. Reducing the ability of operators to take advantage of economies of scale in the location of servers (both in terms of physical infrastructure and engineering labour force) leads to growing operational costs. In the presence of restrictive data localisation requirements (Category 3), cloud service providers would only operate in countries where they have datacentres or in countries where it would be profitable to build new infrastructures.
- **Negative impacts on downstream users**. Small businesses face higher costs to access critical digital tools which can have positive trade-enhancing effects helping scale-up activities and "go global". This is especially the case for small businesses located in countries without sufficient local infrastructure for cloud computing.
- **Reductions in the amount of services provided**. Reduced ability to move data can lead to cloud computing companies not being able to provide in every country all the services they could potentially provide. This too can have important consequences downstream and limit users' choice.
- **Increased compliance costs with potential difficulties in understanding what requirements apply to which type of data**. Cloud computing is at the intersection of different types of data. Cloud providers store personal information or information that might be needed for regulatory purposes. Businesses claimed that it can be difficult to track what requirements apply to what data, and that sometimes, requirements can overlap. This complexity creates uncertainty with negative effects on operations. International regulatory fragmentation on these issues exacerbates this problem.
- **Increased cybersecurity risks**. To ensure the integrity and security of cloud computing systems, data transfers about potential cybersecurity threats (henceforth 'threat data') are needed. Any reduction in the mobility of this 'threat data' can lead to increased vulnerabilities and lowered resilience. The ability to detect a threat in one part of the globe and to update all security systems simultaneously is key to ensuring data security. Companies overwhelmingly agree that data localisation requirements do not lead to greater data security. Indeed, data security does not depend on the geographical location of the servers storing cloud data, cyber-criminals can attack from anywhere. Data security rather depends on investment in technical assets, such as end-to-end encryption or anonymising technologies. Concentrating cloud data in servers located within a specific territory increases the level of vulnerability to cyberattacks or disruptions caused by natural disasters.
- **Increased risk of data loss from natural disasters and reduced resilience**. As was the case in the e-payment sector, businesses claimed that natural or man-made disasters are a strong argument against data localisation which affects the ability to store different copies of data in different geographical areas to increase resilience.

### *3.2.3. Air travel data*

*How does it work?*

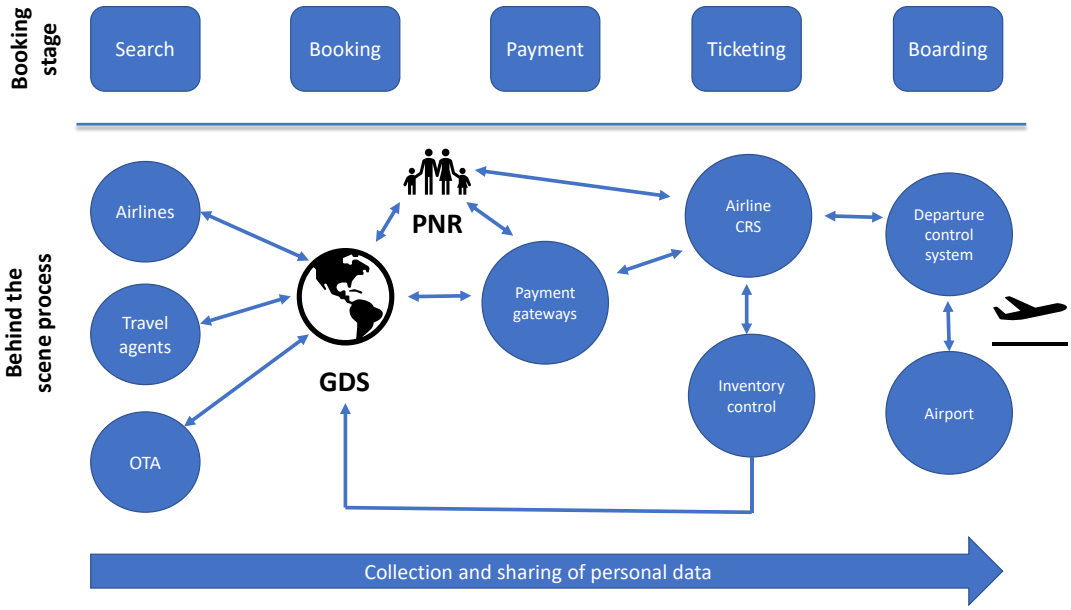
Air transport plays an important role in facilitating economic development, supporting tourism, and stimulating foreign investment and trade. Since 1995, world passenger air traffic (in revenue passenger-km) increased at an average annual growth rate of 5% (ICAO, 2023[11]). However, the COVID-19 pandemic substantially affected air travel with scheduled passenger traffic dropping by 60% in 2020 compared to 2019, and by 49% in 2021 compared to 2019 before gradually re-bouncing in 2022 (ICAO, 2023[12]).

Aviation is a data intensive sector. The seamless flow of information across different actors and borders is essential for the safe and timely travel of millions of passengers. At the same time, digitalisation has fundamentally changed how passengers search, book and pay for airline tickets enabling greater visibility on available routes and tickets, incentivising more price competition among airlines, and fostering higher quality services.

The ticketing process involves different stages involving the collection, transfer and processing of data across different countries (Figure 9). Airline tickets are increasingly booked online, including on the airlines websites or through online travel agents (OTA), in addition to more traditional travel agencies. Global Distribution Systems (GDS), such as Amadeus, Sabre or Travelport, frequently act as virtual middlemen between travel agents and airlines ensuring real-time monitoring and communication on available seats and passenger information. Bookings may be made with one airline (the marketing carrier) but then individual flight sectors may be flown with that airline and/or another airline (the operating carrier) all of whom will need the relevant booking details

Once passengers book a specific flight, a Passenger Name Record (PNR) is created. This is a digital file that contains key travel information (e.g., passenger name, departure and arrival location, contact information, etc.) and which can be progressively updated with additional travel information (e.g., payment information, frequent flier number, travel preferences, baggage information, car rental and hotel reservation etc.). The PNR is primarily collected by the airlines and usually stored on the marketing airlines computer reservation system (CRS) with copies on the operating carriers (CRS) and GDS servers where involved in a booking to ensure smoother coordination and avoid duplication of flight reservations. The CRS systems used by airlines, also known as Passenger Service Systems (PSS) are often provided by third parties with specialized expertise developing and maintaining PSS applications, who provide these services to multiple airlines.

## Figure 9. Use of data in ticket booking and processing




Source: Authors' elaboration

For processing payments, third party payment providers or payment gateways (e.g., Paypal) are used, many of which are themselves dependent on processing data across international borders as illustrated above. Upon confirmation of payment, passengers receive flight itineraries, PNR number (a six-character code) and tickets (which are stored on the airlines CRS(s) with copies also in the GDS).

To ensure smooth boarding and departure, the airline CRS is integrated with the airlines Departure Control System (DCS) and airport information systems. The DCS controls check-ins, creates boarding passes and baggage tags. Data is shared with ground handlers who support check in and other airport processes on behalf of airlines. Data is shared with the airport to ensure that those who are entitled to reach airside areas can do so and inn many countries to ensure that the airport can provide passengers with reduced mobility with support required to transit through the airport. The airport baggage control use barcodes generated through the DCS to sort and track baggage. The bar codes are also shared with international baggage tracking platforms, e.g., in WorldTracer Distribution Network, where passengers can track their baggage. Once passengers scan their boarding passes at gates, the DCS will update the PNR to show that the passenger has boarded and flown as scheduled.

Following the booking or prior to a passenger traveling the airline may be required to provide the APIS or PNR data to the border authorities and potentially other government agencies in the countries passengers will be travelling to (including in some occasions where they will be transiting or overflying).

*What does the regulatory landscape look like for air travel data?*

International air transport is underpinned by the Convention on International Civil Aviation (the Chicago Convention) through the International Civil Aviation Organisation (ICAO).[32] In addition, Air transport operates through a comprehensive network of bilateral air services agreements which stipulate traffic rights and routes for airlines as well as other aspects such as tariffs, ownership requirements, ground handling, safety and security measures, among others.[33]

Passenger information coded in the PNR and advance passenger information (API) which is primarily sourced from machine readable documents such as passports and ID cards, can be a valuable source of information to enhance border control, combat terrorism and criminal activities and strengthen law enforcement efforts across borders. This is governed by a process under Annex 9 of the Chicago Convention which many ICAO members accept, but individual member states increasingly have imposed their own requirements on the provision of such data or prohibitions on the provision of such data which can create conflicting obligations and frustrate the benefit of a multi-lateral process.[34] In addition to Annex 9 of the Chicago Convention, ICAO issued Guidelines 9944 that cover best practices related to the transfer, processing and storage of PNR data (ICAO, 2010[13]). Several countries mandate the retention of PNR data for a specific period of time in the context of law enforcement.[35]

Airlines, travel agencies, GDS providers, payment gateways, and other key players in aviation are also subject to more cross-cutting requirements on business operations, including requirements on data transfer and data localisation. As such, corporate information such as accounting and financial data can be subject to local storage requirements and generate added costs for businesses which can have substantial implications in an industry that is inherently global and relies on commercial operations across many countries. As noted earlier in this paper, data storage requirements for cross-cutting business data and financial data tends to take the most restrictive form (local storage with prohibition on flow or based on ad-hoc exception), and this is true particularly for non-OECD countries (see Table 1 above). In addition, as the sector handles large volumes of personal data, localisation requirements related to such data would also have substantial implications on the effective cross-border sharing of passenger information needed for international air travel.

[32] Next to ICAO, the International Air Transport Association (IATA), a trade association for the world's airlines, supports different areas of civil aviation, including developing common frameworks and approaches (e.g., on airport landing and take-off slot allocation), facilitating financial settlement in booking processes, and providing a forum for co-operation among actors in the sector.

[33] Air travel is largely carved out of GATS schedules. Nonetheless, the WTO GATS applies to three subsectors, namely: computer reservation systems, selling and marketing of air transport services and aircraft repair and maintenance. See WTO GATS Annex on Air Transport Services, paragraph 3.

[34] Amendment 28 to Annex 9 of the Chicago Convention.

[35] Article 12(2) of EU Directive 2016/681 and Judgment of the Court of Justice of the European union in Case C-817/19 (21 June 2022), para. 255. Note that the requirement to store PNR data applies to local agencies that collect such data and not to airlines that transmit these.

*How does data localisation affect businesses in this sector?*

Any rules which prohibit or unduly restrict the ability to transfer data internationally about passengers inevitably restrict the ability of those passengers to travel internationally.

The data held by airlines are being constantly updated in real time based on new and changed bookings, changes to inventory and other passenger and airline activity. As a result, it is essential that there is a single source of that information which in practice means a single geographic location at which that data is held globally.

As a result, data localisation requirements, whether or not combined with restrictions on cross-border data transfers, will have very significant impacts on airlines' operations to countries requiring data localisation. At best, it would result in very significant additional operational complexity and costs for the issues raised to be overcome. At worst, it might negatively impact decisions of airlines to fly to those locations adversely impacting international trade, tourism and other activities.

Consultations with businesses and business associations in this sector provided useful insights on different implications on data localisation measures including the following:

- **Well-defined rules, protocols and standards are already in place for passenger data**. The aviation industry is subject to comprehensive international and domestic regulations, and as such, the flow of essential aviation data is already subject to established rules, protocols and standards, especially around the storing, processing and transferring of PNR data.
- **Cross-cutting data localisation measures can affect business operations**. The growing volume of regulations, including those affecting business operations more generally and widening regulatory fragmentation across countries is creating uncertainties with negative impacts to the supply of air transport services.
- **There are growing uncertainties on the linkages with data protection and privacy rules in aviation**. Obligations to provide PNR, APIS and increasingly other personal data (such as Covid vaccination status) to government agencies potentially conflicts with privacy and data protection laws and other international data transfer and data localisation rules. Moving data together with passengers is inherent in this industry as well as sharing, when necessary, that information among airlines, and across different ancillary service providers and government agencies. This also raises concerns for data localisation. The increased complexity of the above mentioned issues has led to the convening of an expert panel to explore these issues at ICAO.
- **Regulatory uncertainty can raise compliance costs and undermine efficient air transport services.** Reducing regulatory uncertainty and lack of predictability are instrumental in formulating policies for a global industry such as aviation and should be undertaken in cooperation with industry actors as much as possible.

## 4. Identifying discussions points

The findings from the work undertaken demonstrate that data localisation is on the rise and that it is becoming increasingly restrictive. Businesses claim that this is affecting their ability to operate globally, while, at the same time, also having unintended consequences such as increased exposure to cybersecurity and fraud.

While it remains the prerogative of governments to establish the mix of instruments or mechanisms that best serve their policy interests and objectives, greater understanding, discussion and agreement on issues related to data localisation can be conducive to greater overall confidence and "trust" in the environment that underpins the global flow of data and that supports a growing part of our economies and societies.

International discussions can serve the purpose of ensuring that approaches to data localisation continue to deliver on justified public policy objectives in a way that is least trade restrictive. This could include:

- **Continued monitoring of the evolving regulatory environment** to stay on top of evolving trends and wider engagement in transparency exercises.
- **Continued discussions around moving, in principle, towards less restrictive forms of data localisation where possible**. For example, where possible, the use of access conditions rather than local storage requirements should be explored to reduce some of the unintended consequences of data localisation. Or moving from more restrictive data localisation measures with flow prohibitions towards data localisation measures with transparent conditions for transfers.
- **Continued cooperation on these issues, in dialogue** with regulators, trade policy makers and other relevant stakeholders, including from the private sector. This would contribute to reducing fragmentation and enhancing interoperability across regulatory regimes with a view to ensuring more transparent and predictable approaches.
- Continued efforts to realise **global rules that address data localisation** and take into account justified public policy objectives while avoiding excessive fragmentation, especially through discussion at the WTO under the Joint Statement Initiative on e-commerce.

# *References*


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. [8]

Casalini, F. and J. López González (2019), "Trade and Cross-Border Data Flows", *OECD Trade Policy Papers*, No. 220, OECD Publishing, Paris, https://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://doi.org/10.1787/ca9f974e-en. [14]

Chander, A. and U. Le (2014), "Breaking the Web: Data Localization vs. the Global Internet", *School of Law University of California, Davis*, Vol. Research Paper No. 378, https://ssrn.com/abstract=2407858. [15]

Chander, A. and U. Lê (2015), "Data nationalism", *Emory Law Journal*, Vol. 64/677, https://ssrn.com/abstract=2577947. [6]

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. 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. [2]

Gartner (2022), , https://www.gartner.com/en/newsroom/press-releases/2022-10-31-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-reach-nearly-600-billion-in-2023. [9]

ICAO (2023), *Effects of Novel Coronavirus (COVID-19) on Civil Aviation: Economic Impact Analysis*, https://www.icao.int/sustainability/Documents/COVID-19/ICAO_Coronavirus_Econ_Impact.pdf. [12]

ICAO (2023), *World Aviation and the World Economy*, https://www.icao.int/sustainability/pages/facts-figures_worldeconomydata.aspx. [11]

ICAO (2010), *Guidelines on Passenger Name Record (PNR) Data*, https://www.icao.int/Security/FAL/ANNEX9/Documents/9944_cons_en.pdf. [13]

Lopez-Gonzalez, J., F. Casalini and J. Porras (2022), "A preliminary mapping of data localisation measures", *OECD Trade Policy Papers N. 262, OECD Publishing, Paris*. [4]

OECD (2014), "Cloud Computing: The Concept, Impacts and the Role of Government Policy", *OECD Digital Economy Papers*, No. 240, OECD Publishing, Paris, https://doi.org/10.1787/5jxzf4lcc7f5-en. [10]

Selby, J. (2017), "Data localization laws: trade barriers or legitimate responses to cybersecurity risks, or both?", *International Journal of Law and Information Technology*, Vol. 25, pp. 213–232, https://doi.org/doi: 10.1093/ijlit/eax010. [7]

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. [3]

# Annex A. List of Trade Agreements with ban on local storage requirements

| Long title | Short title | Parties | Year signed |
|---|---|---|---|
| Protocolo Adicional al Acuerdo Marco de la Alianza del Pacífico | Pacific Alliance Additional Protocol (PAAP) | CHL, COL, PER, MEX | 2014 |
| Agreement between Japan and Mongolia for an Economic Partnership | Japan Mongolia FTA | JPN, MNG | 2015 |
| Trans-Pacific Partnership Agreement | Transpacific Partnership (TPP) | AUS, BRN, CAN, CHL, JPN, MYS, MEX, NZL, PER, SGP, USA, VNM | 2016 |
| Acuerdo de Libre Comercio entre la República de Chile y la República Oriental del Uruguay | Chile Uruguay FTA | CHL, URY | 2016 |
| Updated Singapore-Australia Free Trade Agreement (SAFTA) | Australia Singapore | AUS, SGP | 2016 |
| Trade Agreement between the Argentine Republic and the Republic of Chile | Argentina Chile FTA | ARG, CHL | 2017 |
| Free Trade Agreement between the Democratic Socialist Republic of Sri Lanka and the Republic of Singapore | Singapore Sri Lanka FTA | LKA, SGP | 2018 |
| Australia-Peru Free Trade Agreement | Australia Peru FTA | AUS, PER | 2018 |
| Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) | CPTPP | AUS, BRN, CAN, CHL, JPN, MYS, MEX, NZL, PER, SGP, VNM | 2018 |
| United States - Mexico - Canada Agreement | USMCA | USA, MEX, CAN | 2018 |
| Chile - Brazil Bilateral Trade Agreement | Brazil Chile FTA | BRA, CHL | 2018 |
| ASEAN Agreement on Electronic Commerce | ASEAN E-commerce Agreement | ASEAN | 2019 |
| Indonesia - Australia Comprehensive Economic Partnership Agreement | Australia-Indonesia CEPA | AUS, IDN | 2019 |
| Australia-Hong Kong Free Trade Agreement and associated Investment Agreement | Australia-Hong Kong FTA | AUS, HKG | 2019 |
| Agreement Between The United States Of America And Japan Concerning Digital Trade | Japan US Digital Trade Agreement (DTA) | JPN, USA | 2019 |
| Australia - Singapore Digital Economy Agreement | Australia Singapore Digital Economy Agreement (ASDEA) | AUS, SGP | 2020 |
| Digital Economy Partnership Agreement ("DEPA") Between Singapre, Chile & New Zealand | Digital Economy Partnership Agreement (DEPA) | CHL, NZL, SGP | 2020 |
| Regional Comprehensive Economic Partnership ("RCEP") | RCEP | 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 United Kingdom of Great Britain and Northern Ireland | EU UK TCA | EU, GBR | 2020 |
| Mercosur Agreement on Electronic Commerce | Mercosur E-commerce Agreement | ARG, BRA. PRY, URY | 2021 |
| Chile - Paraguay Free Trade Agreement | Chile-Paraguay FTA | CHL, PRY | 2021 |
| Australia-United Kingdom Free Trade Agreement | Australia - UK FTA | AUS, GBR | 2021 |
| Free Trade Agreement between Iceland, the Principality of Liechtenstein and the Kingdom of Norway and the United Kingdom of Great Britain and Northern Ireland | UK, Iceland, Liechtenstein and Norway FTA | GBR, ISL, LIE, NOR | 2021 |
| Digital Economy Agreement between the United Kingdom of Great Britain and Northern Ireland and the Republic of Singapore | Singapore-UK DEA | GBR, SGP | 2022 |
| Free Trade Agreement between the United Kingdom of Great Britain and Northern Ireland and New Zealand | New Zealand-UK FTA | NZL, GBR | 2022 |
| Digital Partnership Agreement Between The Government Of The Republic Of Korea And The Government Of The Republic Of Singapore | Korea-Singapore DEA | KOR, SGP | 2022 |
| EU-New Zealand Free Trade Agreement | EU-New Zealand FTA | EU, NZL | 2022 |

Source: Own using TAPED database (Burri and Polanco, 2020[8]). Note: In December 2022, negotiations between the EU and Chile reached their political conclusion on the EU-Chile Advanced Framework Agreement (includes art.19.4, on prohibition of data localisation) and in early 2023 the UK-Ukraine Digital Trade Agreement was signed (includes art. 132-L, on location of computing facilities).

# Annex B. Template for interviews with businesses

## Introduction

Data, and its flow across borders, underpins modern day economic and social interactions. However, governments are adopting new regulation that either conditions the movement of data across borders or that mandates that data is stored domestically. The OECD has been working on mapping these measures and analysing their implication for international trade.

At the request of the Japanese government under their G7 Presidency, we are collecting and analysing information about how measures that explicitly require data to be stored domestically affect business activities. This includes:

- Measures that require domestic data storage with no conditions on transfer. An example is where accounting records are to be stored domestically so that regulators can access but a copy can also be sent and stored abroad.
- Measures that require domestic data storage and have clearly defined transfer or access conditions. An example is where health data is asked to be stored domestically but there are clear provisions for its transfer should it be needed.
- Measures that require domestic storage and which prohibit data to flow. An example of this where strategic or important data must be stored within the country at all times.

This work aims to illustrate the implications of different approaches for business activities so as to help governments better understand the issues businesses face and identify unforeseen consequences arising from existing regulation.

Against this backdrop, we would be keen to hear responses to the following questions. All discussions will be strictly confidential, and results will only be presented in an aggregate format. No enterprise-specific or personal or sensitive information will be disclosed.

### *Questions*

- Q1. Can you tell us a bit about your core business functions and in particular about how cross-border data flows support these activities?
- Q2. Have you encountered data localisation or storage requirements in the course of your business operations? How do such requirements affect your ability to conduct business? Please specify with respect to cost of compliance but also ability to deliver services efficiently.
- Q3. How have you reacted to this regulation? (e.g. installing a data centres in a specific location, relocating activities, outsourcing, changing the nature of the services you deliver?...)
- Q4. Do you think that the storage requirements you face meet the governments policy objectives?
- Q5. What are the unforeseen consequences of these measures?
- Q6. Are there any other issues that should be brought to governments' attention?