OECD GOING DIGITAL TOOLKIT

POLICY NOTE

Trade and cross-border data flows

OECD
BETTER POLICIES FOR BETTER LIVES

going digital

This Toolkit note was written by Javier López-González. It builds on work declassified by the Trade Committee in December 2018, and on the OECD report to the G20 Digital Economy Task Force (DETF) in 2020 entitled "*Mapping approaches to data and data flows*". The note was provided to the Trade Committee on 30 November 2020 and it was subsequently prepared for publication by the OECD Secretariat.

This Toolkit note is a contribution to the OECD Going Digital project, which aims to provide policy makers with the tools they need to help their economies and societies thrive in an increasingly digital and data-driven world.

For more information, visit *www.oecd.org/going-digital*.

#GoingDigital

Please cite this publication as:

López-González, J. (2021), "Trade and cross-border data flows", *OECD Going Digital Toolkit Notes*, No. 11, OECD Publishing, Paris, *https://doi.org/10.1787/7bc12916-en*.

Note to Delegations:

This document is also available on O.N.E. under the reference code:

TAD/TC/WP(2020)19.

Table of Contents

Figures

Boxes

Trade and cross-border data flows

In today's digitalised and globally interconnected world, data – and its flow across borders – has become the lifeblood of our economic and social interactions. However, as more data crosses borders, concerns about its use and misuse have emerged. These concerns have led to a growing number of data regulations conditioning the movement of data across borders, affecting trade in the process. This Going Digital Toolkit note provides an overview of the emerging policy landscape related to cross-border data flows with a view to enabling more informed discussions on solutions that can enable the trade-related opportunities of digital transformation while tackling some of the new challenges it raises.

In today's digitalised and globally interconnected world, data has become the lifeblood of our economic and social interactions. The proliferation of devices and sensors, the exponential growth in computing power, the plummeting costs of data storage, and the growing ability to deliver more data at greater speeds, have altered how we conduct our lives and how businesses operate (OECD, 2020[1]). Today, it is difficult for an international trade transaction to take place without some form of cross-border data flow. At the same time, many domestic transactions are also supported by cross-border data flows.

Whether for international trade (National Board of Trade, 2014[1]), (MGI, 2016[2]), (López González and Jouanjean, 2017[3]), (Casalini and López González, 2019[4])), production (National Board of Trade, 2015[5]), productivity (OECD, 2015[6]), (Brynjolfsson and McElheran, 2016[7]) and in services (Ferracane and Van der Marel, 2018[8]), manufacturing (Brynjolfsson and McElheran, 2019[9]) and agriculture (OECD, 2019[10]), data, and its flow across borders, enables new opportunities to promote growth, well-being and inclusion.

However, as we become increasingly reliant on data for our daily economic and social activities, new challenges arise. The ubiquitous exchange of data is fuelling concerns about the use, and especially the misuse, of data, amplifying concerns about privacy protection, digital security, regulatory reach, competition and industrial policy. This is especially the case when data crosses different jurisdictions. The Internet is global and borderless, but regulations are not.

Against this backdrop, this Going Digital Toolkit note provides an overview of the emerging policy landscape, with a view to enabling more informed discussions on solutions that can enable the trade-related opportunities of digital transformation while tackling some of the new challenges it raises.

What is data and how does data flow?

Global traffic from data centres is estimated to have increased fourfold since 2015 – from 5 zettabytes in 2015 to around 20 zettabytes in 2021 (CISCO, 2020[11]). To put that into perspective, a zettabyte is 1 000 000 000 000 000 000 000 bytes (21 zeros); that is, a thousand exabytes, a billion terabytes, or a trillion gigabytes. There are 20 times more bytes of traffic from data centres than there are stars in the expanding universe (UCSB, 2013[13]). The pace of change shows no signs of slowing down; in fact, the size of global data flows is expected to continue growing at an accelerating pace (CISCO, 2020[11]) .

However, the economic activity that growing data traffic supports is not easy to measure. How bits and bytes translate into dollars and cents is hard to establish. This is because, from an economic perspective, data is different to other resources, factors of production or inputs. First, data is valued at use, not at volume. For instance, a spreadsheet with 100 personal shopping entries may

occupy the same memory space as one with 100 personal health records, but its underlying value is different. A retailer will value the shopping entries more than a health service provider (which will value the personal health records more). The value of data is ultimately derived from its use, not its volume.

Second, the value of data can increase when merged to become greater than the sum of its parts. For instance, the shopping entries linked to the health records can help target advertisements towards the health conscious shopper. Third, data has both inherent and potential value. Information not used today can become valuable tomorrow with changing business dynamics or when combined with different data yet to become available.[1]

Data can also be copied at virtually no cost. This means that its use can serve many different purposes at once.[2] The 100 personal health records may be used by one health service provider to research cures for cancer while it can be used by another to provide remote health services. The use for one purpose does not stop the use for the other.

Although data is often described as the "new oil" (The Economist, 2017[14]), this characterisation is misleading (Mandel, 2017[15]). Like oil, data is an essential input into the economy; however, data is not scarce, and can be copied and transferred at virtually no cost. Data is different.[3] Ultimately, data are vast an unordered or unprocessed points that are collected; they become information when analysed to identify relationships between data points.[4]

Knowledge is generated by analysts, and increasingly by machines or algorithms, that recognise the importance of the information and wisdom is generated by the decisions that make the most of the streams of analysed data. In this data-information-knowledge-wisdom (DIKW) hierarchy (Figure 1), each stage is dependent on those that come before it. There is no wisdom without knowledge, no knowledge without information, and no information without data.

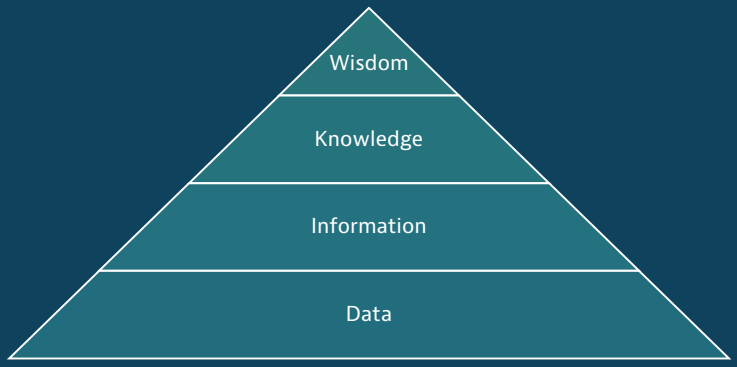
[1] For instance, popular social networking platforms ran strong deficits during early years of operation while thinking about how to best capitalise on the mass of information gathered.

[2] In economic terms, data might be thought of as non-rivalrous which means that its consumption by one user does not prevent the simultaneous consumption by another.

[3] See (Mandel, 2017[15]) for a discussion on differences between data and oil.

[4] Although there is a difference between data and information, the paper uses these terms interchangeably.

Figure 1. There is no wisdom without knowledge, no knowledge without information, and no information without data



Source: Adapted from (Rowley, 2007[16]).

Data also travels through the Internet in irregular ways. When a file is sent from one computer to another, it is first broken down into different "packets". These are like little parcels of information marked with the Internet Protocol addresses of the sender and the recipient, and a code identifying the sequence in which the packets are to be reassembled at destination. Once the packets leave the origin computer, they cross different networks and take different routes to the destination computer. Routers, the traffic wardens of the Internet, guide the packets across networks, ensuring that, at each step, they take the shortest or least congested route. Once the packets arrive at their destination, the computer re-assembles them according to the pre-specified sequence. If a packet is missing, a signal is sent for that packet to be re-sent.

This means that:

- When flowing between two countries, packets take different routes, often crossing a number of third countries.
- The ultimate origin and destination of data flows is often a technical issue. For example, firms use mirror sites, which replicate webpages in different countries, to increase the speed of data transfers.
- In some instances, what might seem to be a domestic transfer, involves a cross-border flow.

Why is data regulation emerging?

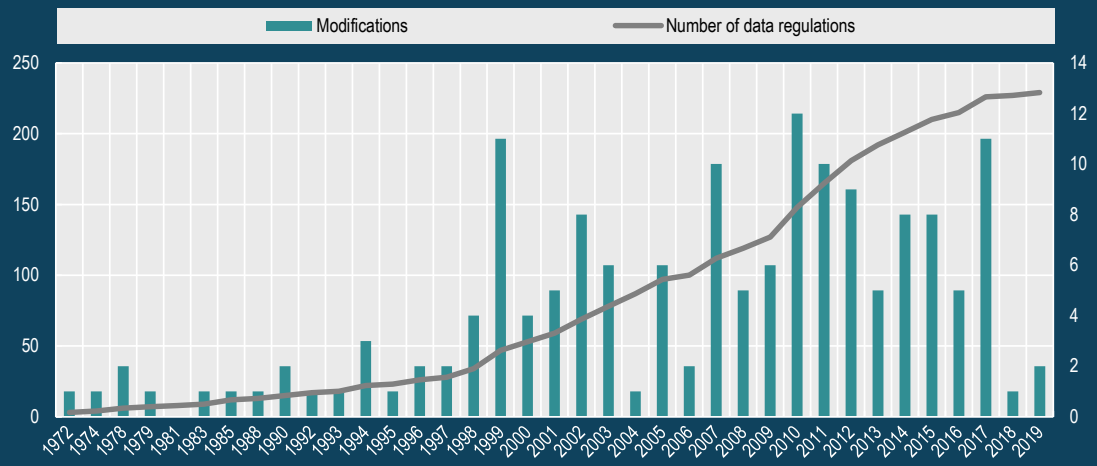
As a result of growing digitalisation, the information trail left in today's economic and social interactions is richer than ever before. Moreover, what data is being gathered and the use that is being made of this information is not always clear. This has fuelled a range of concerns about the use and misuse of data, including in the context of power relations among firms and between

firms and consumers, but in particular with respect to privacy and data protection.[5]

These concerns are compounded when dealing with cross-border data flows, especially when data moves beyond the reach of domestic regulatory bodies or is subject to differing regulations depending on where it is located and the type of information that it contains. Indeed, while data and digital activity are inherently borderless, regulations are not, and ensuring privacy and security, protecting intellectual property, enabling economic development and maintaining the reach of regulatory and audit bodies can become more complex when data crosses jurisdictions.

In light of these emerging regulatory challenges, governments have been updating and adapting their data-related policies. This has resulted in a growing number of countries placing conditions on the transfer of data across borders or requiring that data is stored locally (Figure 2).

Figure 2. A growing number of data regulations



Note: Data regulations include different types of regulation relating to data transfers and local storage requirements. Numbers are affected by the way in which regulations are structured, as this varies by country; some countries may have a single regulation covering a wide range of measures; others will have several different regulations covering, for example, restrictions on data flows for different types of data, and local storage requirements.
Source: (Casalini and López González, 2019[4]).

[5] Privacy itself is difficult to define. It means different things to different people and the value attached to privacy, whether as individuals or in society, can be subjective. There can also be trade-offs between benefitting from highly personalised and often "free" services and the extent to which consumers are able to keep their data private. The optimal choice in that trade-off will also vary according to individual preferences.

The reasons countries are reviewing their data policy are manifold, but can be broadly grouped into five categories (OECD, 2020[13]). Much of the debate about data flows revolves around the movement of personally identifiable information, raising concerns about *privacy and data protection*. For some, the challenge is to ensure that data transferred outside of a specific jurisdiction continues to receive the same protection that it received in the domestic jurisdiction. However, views on privacy and data protection can vary significantly across cultures, which is why regulation also differs.

Some measures that condition data flows aim to secure access to information for *regulatory control or audit purposes*. In this sense, requirements for data to be stored locally can be seen as a means of ensuring that information is readily accessible to regulators, the online equivalent of a longstanding practice in the offline world. Such measures can be sector-specific, reflecting particular regulatory requirements for specific data such as business accounts, telecommunications or banking data.

Measures related to *national security* often mandate that data is stored and processed locally for the purpose of protecting information deemed to be sensitive, or securing the ability of national security services to access and review data. The latter requirement can be very broad in nature, providing wide scope of access to any form of data.

Governments also promote local storage and processing with a view to ensuring *data security*. The rationale for implementing countries is that data security can best be guaranteed when storage and processing is domestic.

Finally, conditioning the flow of data or mandating that it be stored locally can be motivated by the desire to use a pool of data to encourage or help develop domestic capacity in digitally intensive sectors, a kind of *digital industrial policy*, including in the context of economic development. This can reflect a view that data is a resource that needs to be made available first and foremost to national producers or suppliers. These approaches can be sector specific or apply to a range of data types.

How are countries regulating cross-border data flows and data storage domestically?

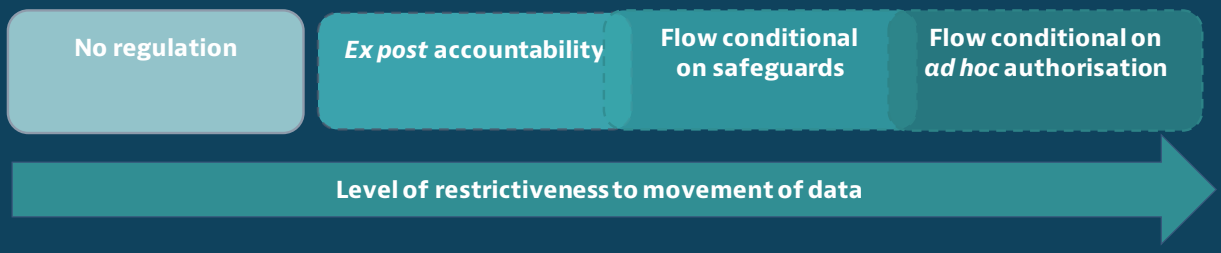
As a result of these concerns, two broad types of data policies have emerged: 1) those that condition the movement of data across borders, and 2) those that mandate that data is stored locally (Casalini and López González, 2019[4]). Each approach addresses different and sometimes overlapping policy objectives. The manner in which countries approach their data-related policies naturally reflects the underlying preferences, including in relation to trade-offs, of their citizens.

Cross-border data flows

Cross-border data flow regulation varies widely, reflecting different cultural preferences and policy objectives. Four broad approaches have emerged (Figure 3). These are not mutually exclusive: different approaches can apply to different types of data even within the same jurisdiction. For example, health data might be subject to more stringent approaches than data related to product maintenance.

- At one extreme, in some jurisdictions (notably less-developed countries), there is *no regulation* of cross-border data flows, usually because there is no data protection legislation at all. While this implies no restrictions on the movement of data, the absence of regulation might affect the willingness of others to send data.
- The second type of approach does not prohibit the cross-border transfer of data nor does it require any specific conditions to be fulfilled, but provides for *ex-post accountability* for the data exporter if data sent abroad is misused (e.g. firms can send data across borders, but they are legally accountable if something goes wrong).
- A third approach, *flows conditional on safeguards*, includes approaches relying on the determination of *adequacy or equivalence* as ex-ante conditions for data transfer (Box 1). These rulings can be made by a public authority or by private companies and can include requirements about how data is to be treated. Where an adequacy determination has not yet been made, firms can move data under options such as *binding corporate rules*, *contractual clauses* and consent (Box 2).
- The last broad type of approach, flow conditional on ad hoc authorisation, relates to systems that only allow data to be transferred on a *case-by-case basis* subject to review and approval by relevant authorities. This approach relates to personal data for privacy reasons but also to the more sweeping category of "important data", including in the context of national security.

Figure 3. Broad approaches to cross-border data flow regulation



Source: Adapted from (Casalini and López González, 2019[4]).

Across the different types of approaches, a number of exceptions are envisaged to permit the transfer of data. These include transfers in relation to "legitimate interest", or for the "public interest", or in relation to legal claims (among others). Data-subject consent is also a frequently used exception for permitting data transfers, but its use remains the subject of debate (Innovation, Science and Economic Development Canada, 2019[14]).

Box 1. Adequacy or equivalence

Adequacy or equivalence can either be evaluated by a data exporter or a public body. For instance, in some approaches, it is the data exporter who decides whether the recipient entity provides adequate levels of protection and conforms to applicable privacy principles. However, and more frequently, a public body (such as the national data protection authority), certifies that the data protection system of another country is adequate or equivalent.

These determination can take the form of a unilateral recognition, when one country certifies the adequacy of another and data can flow unimpeded in one direction. Or it can take the form of a mutual recognition of data protection measures: when two countries choose to recognise each other's systems. In this instance, once established, the free flow of data in both directions is assured (for example the 2019 mutual adequacy findings by the European Union and Japan).

Although adequacy and equivalence are discussed here jointly, these terms do not necessarily mean the same thing. Equivalence implies the assessment of a level of objective similarity between two regulations, both in terms of the tools used and the objectives or outcomes of the regulation. Adequacy, in turn, can be more flexible as it implies agreeing on a common outcome but allowing for different tools to be used to meet this outcome.

With many approaches to cross-border data flows relying on some form of adequacy or equivalence decision, how these decisions are made is important. In line with the OECD Guiding Principles for Regulatory Quality and Performance, it is important that the regulations and related decision-making process remain transparent, non-discriminatory, and efficient, in line with the stated public policy objectives and better integrate consideration of market openness principles (including avoidance of unnecessary trade restrictiveness). Today, only a few countries outline the substantive criteria used to determine adequacy in their data protection regulations.

Source: (Casalini and López González, 2019[4]).

Box 2. Binding corporate rules and standard contractual clauses

Binding corporate rules bind the affiliates of a multinational company located in different countries to apply effective rights and legal remedies for the protection of data. These rules enable data to move between affiliates located in different countries, even when these are in countries that do not recognise each other's data protection systems. Transfers are, however, restricted to affiliates within the group. While binding corporate rules provide flexibility, they are often subject to approval by the data protection authority (DPA) in the respective countries, a procedure that can be long and sometimes unpredictable in terms of outcome.

Standard contractual clauses are ready-made rules that provide for data transfers to third-parties located in other countries. The clauses, which are to be used in contracts, are developed by the DPA and, as such, are automatically considered to provide sufficient safeguards for transferring data, even to countries that do not enjoy an equivalence or adequacy recognition. While these clauses are convenient as they are ready for use, the terms they impose are relatively onerous to meet and can lead to high administrative costs

Source: (Casalini and López González, 2019[4]).

Local storage requirements

Local storage requirements constitute another type of emerging data-related policy. As their name indicates, measures falling under this category require that certain types of data are stored in local servers, and often also include local processing requirements. Although distinct from cross-border data flow restrictions, a complete prohibition on the transfer of data amounts to a de-facto requirement for local storage and processing. In contrast, a local storage requirement does not necessarily correspond to a prohibition of cross-border transfer. That said, local storage requirements could still affect cross border data flows to the extent that companies switch from a foreign supplier to a domestic supplier to store and process data that is collected in a certain country.

As with regulations on cross-border data transfers, local storage requirements can be grouped into four categories, also with blurred boundaries (Figure 4). Different local storage and processing rules can also apply to different types of data even within a country. They can be aimed at personal data, or can be sector-specific, typically targeting regulated sectors such as health,

telecommunications, banking or payment processing, insurance, or satellite mapping.[6]

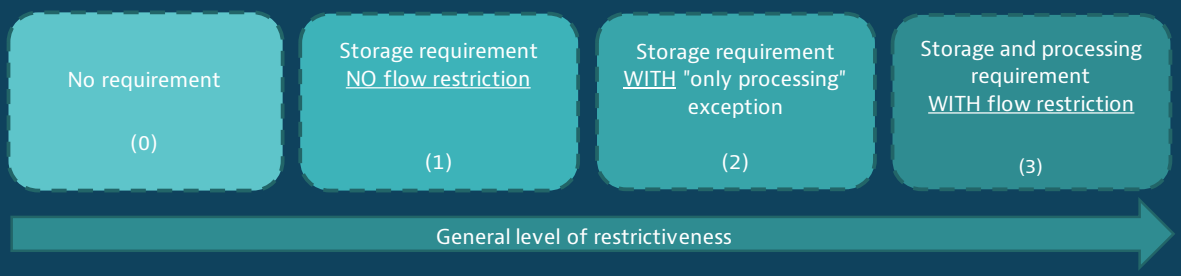
A default position is where there are *no requirements* to store data locally. This is a relatively common category given that the number of local storage requirements remains small and targeted to specific sectors.

Another approach requires that *a copy of the targeted data is stored in domestic computing facilities*. This type of approach has no restrictions in terms of transferring or processing copies of the data abroad and its objective is, more often than not, to ensure that regulators do not encounter issues related to jurisdictional reach. Approaches falling under this category often target telecommunications metadata and financial and fiscal data from businesses, as a continuation of traditional data retention policies. Newer approaches to data retention now establish that data be retained and made accessible to local authorities without prescribing the country where the data has to be stored. Data retention is also generally limited to a specified time period.

A third approach relates to those where there are *no flow restrictions but foreign storage is not allowed*, implying that processing can occur abroad, but that post-processing, data must be returned to the home country for storage.

Finally, there is a category of approaches that require that data be stored locally with conditions attached to transferring and/or processing those data abroad. These last two requirements can be related to a desire to encourage the development of domestic data storage and other data services industries and thus can be related to industrial policy objectives.

Figure 4. Broad approaches to local storage requirements



Source: (Casalini and López González, 2019[4]).

[6] For example, Regulation (EU) 2018/1807 on a framework for the free flow of non-personal data in the European Union (EU) prohibits localisation of non-personal data within the EU and contains provisions to help governments access data stored in other Member States.

Which instruments exist to enable cross-border data flows?

While there are legitimate reasons for diversity in regulations, the regulatory landscape that underpins cross-border data flows and local storage requirements is becoming increasingly complex. Moreover, the emerging patchwork of approaches risks undermining the different policy objectives they were intended to serve in the first place. Uncertainties about which rules apply to which data, resulting from overlapping or sometimes conflicting requirements for entities involved in data processing, can generate new risks. A firm that does not know what level of protection it must afford to its customers or whether or not it can transfer some or most types of information across borders is going to struggle to ensure privacy protection and to engage in trade. At the same time, government enforcement action can also be hindered by a lack of co-ordination on these inherently transboundary issues. This, in turn, can undermine consumer trust.

Alleviating possible tensions between approaches and ensuring that data can flow with trust has been a goal of policy makers for a number of years. Governments and other stakeholders have increasingly been using a range of approaches to provide businesses with legal certainty as to the basis for data transfers while ensuring that, upon crossing a border, data is granted the desired degree of protection or oversight. Many different instruments and mechanisms have been devised and implemented; these can be grouped into 4 broad categories (Figure 5).

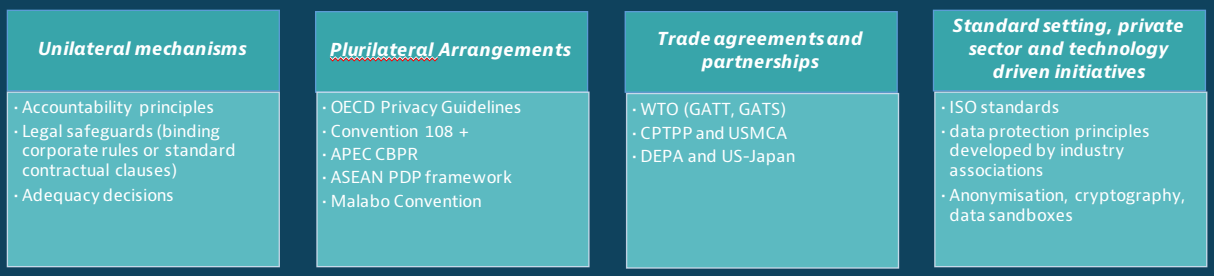
- **Unilateral mechanisms** enable the transfer of data to countries outside the domestic territory under certain conditions. These include the use of *ex-post accountability principles*; ex-ante *legal safeguards* such as contractual clauses or binding corporate rules; and *adequacy decisions*, where countries declare that other jurisdictions provide appropriate safeguards.
- **Plurilateral arrangements** generate consensus around the transfer of specific types of data. The most well-known examples relate to the transfer of personal data and include the OECD Privacy Guidelines, the APEC Cross Border Privacy Regime (CBPR) or the Council of Europe's Convention 108+.[7] There are many different approaches within this category, each with different levels of enforceability.
- **Trade agreements and partnerships** are increasingly addressing issues around data flows. The depth and density of rules varies from one

[7] Other examples of plurilateral arrangements might also include Interpol's Rules on the Processing of Data (RDP). These provide a framework for sharing data between 194 countries through the use of specific information systems.

agreement to another. For example, binding provisions on cross-border transfers and enforcement mechanisms are provided in recent trade agreements – such as the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) and the United States-Mexico-Canada Agreement (USMCA) – and, new types of digital trade arrangements – such as the US-Japan Digital Trade Agreement or the Digital Economic Partnership Agreement between New Zealand, Singapore and Chile. At the same time, discussions on data flows are ongoing in the context of the Joint Statement Initiative on e-commerce at the WTO.

- Increasingly, access to data is being facilitated under **standard setting, private sector or technology driven initiatives**. This includes the use of ISO standards, data protection principles developed by industry associations or privacy enhancing technologies (PET) such as anonymisation and cryptography technologies or data sandboxes that enable access to data within controlled environments.

Figure 5. Instruments for facilitating cross-border data transfers



Source: Author's elaboration.

Each broad instrument type tackles the issue of data transfers from a different perspective. The approaches are also not mutually exclusive: countries can use different approaches with respect to different partners, types of data and in different situations. The scope of data that each approach covers also varies. For instance, rules on cross border data flows in trade agreements often cover all types of data, while existing plurilateral arrangements on cross-border data transfers, as well as some of the unilateral instruments, focus mainly on issues around privacy and data protection, areas where there has been most activity in the context of emerging regulation (see (Casalini, Lopez-Gonzalez and Nemoto, 2021[18])).

Why does it matter?

Understanding how data creates value and how it supports economic activity and identifying the challenges that data raises is key to making the most out of the digital transformation. Data is different, it cannot be depleted and can be shared and re-used by many different users and for many different purposes. This means that data sharing has the potential to give rise to considerable economies of scale and scope.

However, as more and more data crosses borders, new challenges emerge. These are being met with new data regulation that either restricts the movement of data or mandates that it be stored locally. The resulting patchwork of rules and regulations makes it difficult not only to enforce privacy and data protection across different jurisdictions, but also for firms to operate across markets, affecting their ability to internationalise and draw benefits from operating on a global scale. Understanding the evolving regulatory environment is an important first step in helping economies meet the dual goal of ensuring that data can flow across borders with trust.

Annex. A selection of approaches to cross-border data flows

Cross-border elements of Australian privacy laws

Responsible entity: Australia

Description: Australia's data privacy regulation stems from the Privacy Act 1988 (the Act). The Act contains 13 Australian Privacy Principles (APPs), which deal with all stages of the processing of personal information, setting out standards for the collection, use, disclosure, quality and security of personal information. The Act applies to 'APP entities' including Government agencies, private sector organisations with an annual turnover of AUD 3 million or more, and to certain smaller entities that deal more directly with personal information (such as health care services).

- APP 8 imposes strict rules on APP entities governing the cross-border disclosure of personal information held in Australia:
- APP 8 generally requires an APP entity, before disclosing personal information to a foreign recipient, to take reasonable steps (such as a contractual arrangement) to ensure that the foreign recipient will handle the personal information in accordance with the APPs, and

Section 16C of the Privacy Act makes the APP entity responsible for personal information disclosed to a foreign recipient, unless an exception applies.

There are some exceptions to APP 8, such as where a disclosure is required or authorised by law, or where other specified circumstances exist. Most relevantly, APP 8 may not apply where:

- The foreign recipient is subject to a law, or binding scheme, that has the effect of protecting the information in a way that is, overall, at least 'substantially similar' to the way in which the APPs protect the information, and
- There are mechanisms that the individual can access to take action to enforce the protection of that law or binding scheme.

An APP entity may also disclose personal information to an overseas recipient without complying with APP 8 where the entity expressly informs the individual that the principle will not apply and the individual then consents to the disclosure.

Read more: *https://www.ag.gov.au/rights-and-protections/privacy*.

The European Union's General Data Protection Regulation

Responsible Entity: European Union

Description: On 25 May 2018, EU Regulation 2016/679 (GDPR) entered into force in all EU member states, superseding the 1995 Data Protection Directive (95/46/EC) Directive. The GDPR confirms and updates a number of rights for individuals with regard to their personal data. These include: the right to access their own data; the right for rectification and erasure; the right to portability (to move data); and the right not to be subject to automated decision making.

The GDPR applies to all data processing in the European Union, as well as to foreign operators if they specifically target the EU market by offering goods and services to individuals in the European Union (mere accessibility through the internet is not enough). Compared to the 1995 Directive, the GDPR expands the toolbox for sending data from the European Union to third countries, while ensuring that the protection of data is not undermined through international transfers. According to GDPR, the cross-border transfer of data is possible when:

The Commission has made an adequacy decision with regard to the data protection system of the recipient country. These are made on the basis of a series of clear criteria such as the recipient country's rule of law, respect for fundamental rights and the applicable data protection law, among others. These criteria have been further detailed in the "Adequacy Referential" adopted by the European Data Protection Board. A recent example of such adequacy decision is the "two way" adequacy arrangement concluded with Japan.

There are appropriate safeguards in place. These safeguard can be in the form of binding corporate rules, or standard contractual clauses, or public agreements between enforcement authorities through codes of conduct or certification mechanisms. These need to ensure enforceable rights and effective legal remedies for individuals whose personal data is transferred;

Statutory grounds (so-called "derogations") such as consent, performance of a contract, public interest and legitimate interests exist. These derogations should be used for specific situations and cannot be relied on for systematic transfers.

Read more:
https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection.

The OECD Privacy Guidelines (2013)

Responsible Entity: Organisation for Economic Co-operation and Development (OECD)

Description: Data flow governance has been a recurring focus of OECD work for over 40 years. Work in the 1970s led to the OECD's 1980 Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data ("OECD Privacy Guidelines"). The Guidelines are designed to ensure the protection of privacy whilst encouraging transborder flows of personal data with trust. They represent the first internationally agreed set of privacy principles that apply to the protection of personal data whether in the public or private sector. The Guidelines are drafted in technologically neutral language and are non-binding.

The 1980 Guidelines presumed that free transfers of personal data should generally be allowed, but recognised that they could be restricted when the receiving country "does not yet substantially observe the Guidelines or where the re-export of such data would circumvent its domestic privacy legislation" (paragraph 17 of the original Guidelines).

The 2013 revisions to the OECD Privacy Guidelines (OECD, 2013[15])included important updates to the data flow governance provisions. With regard to free flow and legitimate restrictions, key principles are summarised in paragraphs 16 to 18, namely:

> (16). A data controller remains accountable for personal data under its control without regard to the location of the data.
>
> (17). A Member country should refrain from restricting trans-border flows of personal data between itself and another country where (a) the other country substantially observes these Guidelines or (b) sufficient safeguards exist, including effective enforcement mechanisms and appropriate measures put in place by the data controller, to ensure a continuing level of protection consistent with these Guidelines.
>
> (18). Any restrictions to trans-border flows of personal data should be proportionate to the risks presented, taking into account the sensitivity of the data, and the purpose and context of the processing.

The Guidelines also encourage states to co-operate on privacy matters and support the development of international arrangements that promote interoperability among privacy frameworks.

The Guidelines continue to be implemented by countries through legislation, enforcement and policy measures, and have influenced developments in privacy law, principle and practice even beyond OECD countries. For instance, the APEC Privacy Framework, which aims at promoting electronic commerce throughout the Asia Pacific region, is consistent with the core values of the

OECD Guidelines, and reaffirms the value of privacy to individuals and to the information society.

The OECD continues to work with countries and experts to scope developments and provide practical recommendations on the implementation of the Guidelines in today's digital environment.

Read more: *https://www.oecd.org/sti/ieconomy/privacy-guidelines.htm*.

The Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules (CBPR) System

Responsible entity: Asia-Pacific Economic Cooperation

Description: The APEC Cross-Border Privacy Rules (CBPR) System, in place since 2011, is a framework developed by APEC economies to promote the interoperability of privacy regulation through the enforcement of minimum standards. The CBPR System is not mandatory for APEC economies, and even when an economy adheres to it, companies can choose whether to seek certification under the System.

If an economy adheres to the CBPR System, it confirms its participation in the Cross-border Privacy Enforcement Arrangement (CPEA), a regional framework for enforcement cooperation in privacy matters. At the same time, it confirms its intention to use at least one Accountability Agent; that is, a third party oversight entity which has been approved by the Joint Oversight Panel. In practice, adherence does not change the possibility for a member economy to retain its own privacy regulation, but it simply requires the appointment of a data protection authority that is in charge of legally enforcing the privacy policies certified by the Accountability Agent.

Moreover, even if a company is located in an adhering economy, the company does not have to comply with the CBPR privacy framework unless the company itself voluntarily chooses to seek certification under the framework. In order to do this, the company must develop a privacy policy consistent with the framework to be reviewed by a competent Accountability Agent. Once the privacy policy is approved, the company is "white listed" as compliant with APEC's regional privacy standards. It therefore assumes liability for applying the relevant privacy practices to both the domestic relevant authority and an Accountability Agent.

The CBPR System only applies to data controllers, but a Privacy Recognition for Processors has also been recently developed to help processors gain the trust of data controllers.

Read more: *https://cbrps.org*.

Council of Europe's Convention 108

Responsible Entity: Council of Europe

Description: The 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, commonly referred to as Convention 108 of the Council of Europe, is a treaty protecting the right to privacy of individuals with respect to personal data which is automatically processed. To date, fifty-three states have committed to establish, under their own domestic law, sanctions and remedies for violations of the Convention's provisions. While individuals do not have a right of remedy directly under the Convention, claims between states with regard to how the Convention has been transposed could potentially be brought before the International Court of Justice.

A Protocol for the modernisation of the Convention was adopted by the Committee of Ministers on 18 May 2018 and opened for signature on 10 October 2018. When it will enter into force, it will repeal the 2001 Additional Protocol.

The 2001 Additional Protocol established that states that are signatories to the Convention could not restrict the free flow of personal data between themselves, while with respect to third states, they had to restrict the flow of data and allow the transfer only where an adequate level of protection was ensured in the recipient entity, or where safeguards were in place.

The new Protocol of 2018 provides that States which are party to the Convention should not restrict the flow of personal data among themselves, but introduces exceptions to this for cases where there is a risk that the transfer could lead to the circumvention of the provisions of the Convention, or where a party is bound by harmonised rules of protection shared by States belonging to a regional international organisation. This means that when the 2018 Protocol will enter into force, the signatories to the Convention will not be bound to ensure the free flow of data between themselves if one of the exceptions apply. The latter exception, for example, applies to the Member States of the European Union. However, as explicitly stated in the General Data Protection Regulation (EU) 2016/679, a third country's accession to Convention 108 and its implementation "will be an important factor when applying the European Union's international transfer regime, in particular when assessing whether the third country offers an adequate level of protection (which in turn allows the free flow of personal data)."

Read more: *https://www.coe.int/en/web/data-protection/-/modernisation-of-convention-108*.

References

Brynjolfsson, E. and K. McElheran (2019), "Data in Action: Data-Driven Decision Making and Predictive Analytics in U.S. Manufacturing", *Rotman School of Management Working Paper No. 3422397*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3422397. [10]

Brynjolfsson, E. and K. McElheran (2016), "The rapid adoption of data-driven decision-making", *American Economic Review*, Vol. 106, pp. 133-139, http://dx.doi.org/10.1257/aer.p20161016. [8]

Casalini, F. and J. López González (2019), "Trade and Cross-Border Data Flows", *OECD Trade Policy Papers*, No. 220, OECD Publishing, Paris, https://dx.doi.org/10.1787/b2023a47-en. [5]

CISCO (2020), *Cisco Annual Internet Report (2018–2023) White Paper*, https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html. [12]

Ferencz, J. (2019), "The OECD Digital Services Trade Restrictiveness Index", *OECD Trade Policy Papers*, No. 221, OECD Publishing, Paris, https://dx.doi.org/10.1787/16ed2d78-en. [18]

Ferracane, F. and E. Van der Marel (2018), "Do data policy restrictions inhibity trade in services?", *European Centre for International Political Economy, Brussels*, https://ecipe.org/wp-content/uploads/2018/10/Do-Data-Policy-Restrictions-Inhibit-Trade-in-Services-final.pdf. [9]

Freund, C. and D. Weinhold (2002), "The Internet and International Trade in Services", *American Economic Review*, Vol. 92/2, pp. 236-240, http://dx.doi.org/10.1257/000282802320189320. [16]

G20 (2020), "Ministerial Declaration", *G20 Digital Economy Ministers Meeting*, https://g20.org/en/media/Documents/G20SS_Declaration_G20%20Digital%20Economy%20Ministers%20Meeting_EN.pdf. [28]

Innovation, Science and Economic Development Canada (2019), *Canada's Digital Charter in Action: A plan by Canadians, for Canadians*, https://www.ic.gc.ca/eic/site/062.nsf/vwapj/Digitalcharter_Report_EN.pdf/$file/Digitalcharter_Report_EN.pdf. [14]

López González, J. and J. Ferencz (2018), "Digital Trade and Market Openness", *OECD Trade Policy Papers*, No. 217, OECD Publishing, Paris, https://dx.doi.org/10.1787/1bd89c9a-en. [27]

López González, J. and M. Jouanjean (2017), "Digital Trade: Developing a Framework for Analysis", *OECD Trade Policy Papers*, No. 205, OECD Publishing, Paris, https://dx.doi.org/10.1787/524c8c83-en. [4]

MGI (2016), "Digital Globalization: The new era of global flows", *McKinsey & Company*, http://: http://www.mckinsey.com/business-functions/mckinsey-digital/ourinsights/digital-globalization-the-new-era-of-global-flows. [3]

National Board of Trade (2015), "No Transfer, No Production – a Report on Cross-Border Data Transfers, Global Value Chains, and the production of goods", *Kommerskollegium, Stockholm.*, https://ec.europa.eu/futurium/en/system/files/ged/publ-no-transfer-no-production.pdf. [6]

National Board of Trade (2014), "No Transfer, No Trade – the Importance of Cross-Border Data Transfers for Companies Based in Sweden", *Kommerskollegium, Stockholm*, https://unctad.org/system/files/non-official-document/dtl_ict4d2016c01_Kommerskollegium_en.pdf. [2]

Nordås, H. (2016), "Services Trade Restrictiveness Index (STRI): The Trade Effect of Regulatory Differences", *OECD Trade Policy Papers*, No. 189, OECD Publishing, Paris, https://dx.doi.org/10.1787/5jlz9z022plp-en. [19]

OECD (2020), *Mapping Approaches to data and data flows*, OECD Publishing, http://www.oecd.org/trade/documents/mapping-approaches-to-data-and-data-flows.pdf. [1]

OECD (2020), *MAPPING APPROACHES TO DATA AND DATA FLOWS*, http://www.oecd.org/termsandconditions. [30]

OECD (2019), "Digital Opportunities for Trade in the Agriculture and Food Sectors,", *OECD Publishing, Paris*, https://doi.org/10.1787/91c40e07-en. [11]

OECD (2017), *Key Issues for Digital Transformation in the G20*, https://www.oecd.org/g20/key-issues-for-digital-transformation-in-the-g20.pdf (accessed on 20 September 2019). [17]

OECD (2017), *Services Trade Policies and the Global Economy*, OECD Publishing, Paris, https://dx.doi.org/10.1787/9789264275232-en. [26]

OECD (2015), *Data-Driven Innovation: Big Data for Growth and Well-Being*, OECD Publishing, Paris, https://dx.doi.org/10.1787/9789264229358-en. [7]

OECD (2013), *The OECD Privacy Framework 2013*, OECD Publishing, Paris, https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf. [15]

OECD MCM (2020), *2020 Ministerial Council Statement: A strong, resilient, inclusiv and sustainable recovery from COVID019*. [29]

Rowley, J. (2007), "The wisdom hierarchy: Representations of the DIKW hierarchy", *Journal of Information Science*, Vol. 33, No. 2, https://doi.org/10.1177%2F0165551506070706. [16]

UCSB (2013), *About how many stars are in space?*, http://scienceline.ucsb.edu/getkey.php?key=3775#:~:text=The%20number%20of%20stars%20in,stars%20in%20the%20observable%20universe. [13]

WTO (2018), *2018 World Trade Report*, https://www.wto.org/english/res_e/publications_e/world_trade_report18_e.pdf (accessed on 20 September 2019). [20]

WTO (2017), *Joint Statement on electronic commerce*. [24]

WTO (2017), "Provisions on Electronic Commerce in Regional Trade Agreements", *WTO Working Papers*, No. 2017/11, World Trade Organization, Geneva, https://dx.doi.org/10.30875/82592628-en. [25]

WTO (2017), *Work Programme on Electronic Commerce: Draft Ministerial Decision of 13 December 2017*. [23]

WTO (1998), *Work Programme on Electronic Commerce*. [22]

Wu, M. (2017), *Digital Trade-Related Provisions in Regional Trade Agreements: Existing Models and Lessons for the Multilateral Trade System Acknowledgements Acknowledgements*, http://e15initiative.org/wp-content/uploads/2015/09/RTA-Exchange-Digital-Trade-Mark-Wu-Final-2.pdf (accessed on 20 September 2019). [21]