OECD publishing

MAPPING COMMONALITIES IN REGULATORY APPROACHES TO CROSS-BORDER DATA TRANSFERS

OECD TRADE
POLICY PAPER
May 2021 **n°248**

OECD
BETTER POLICIES FOR BETTER LIVES

OECD TRADE AND AGRICULTURE DIRECTORATE

Mapping Commonalities in Regulatory Approaches to Cross-Border Data Transfers

Francesca Casalini, Javier López-González, and Taku Nemoto

Data flows across borders underpin today's digitalised and globally interconnected world, but have also given rise to a range of concerns, including about privacy protection, intellectual property protection, regulatory reach, competition, and industrial policy. This has led to the emergence of a patchwork of rules governing cross-border data flows, complicating both the enforcement of public policy goals and increasing the costs for firms of all sizes of operating on a global scale. In practice, countries are using a range of mechanisms and instruments to enable cross-border data transfers with "trust", including unilateral mechanisms, plurilateral arrangements, and trade agreements. This paper identifies the commonalities, complementarities and elements of convergence in these different instruments for moving data across borders, with the aim of supporting international dialogue and co-operation on more predictable and transparent combinations of data flows and "trust".

Key words: Digital economy, trade policy, data-flows, privacy, interoperability, data free flows with trust

JEL codes: O3, F13

Acknowledgements

The authors would like to thank Nasya Desiria for excellent research assistance as well as Janos Ferencz, Julia Nielson, Irene Olivan-Garcia, Susan Stone, and the Working Party on Data Governance and Privacy in the Digital Economy for comments. They also would like to thank the members of the OECD Working Party of the Trade Committee for their valuable feedback and direction in developing and finalising this report. Finally, the authors thank Jaqueline Maher and Michèle Patterson for preparing this document for publication.

This document replaces a previous version. Figures 1 and 7, and Table A A.1 have been updated.

Table of contents

FIGURES

TABLES

Key messages

The growing patchwork of rules and regulations on cross-border data flows is making it difficult not only to effectively enforce public policy goals such as privacy and data protection across different jurisdictions, but also for firms to operate across markets, affecting their ability to internationalise and benefit from operating on a global scale. While much work in this area has focused on highlighting the differences in approaches to cross border data flows, less attention has been given to identifying common elements that may serve as building blocks in bridging different approaches.

By mapping commonalities in regulatory approaches to cross-border data transfers, this paper highlights the ways that countries create "trusted" environments enabling cross-border data flows. The main insights from this work are:

- There is no single mechanism to enable what has come to be called "data free flows with trust". Governments pursue different, or even multiple and complementary, approaches.
- A range of *unilateral mechanisms* for safeguarding cross-border transfers exist. These vary according to whether safeguards require public sector approval before transfer (pre-authorised safeguards), or if they leave discretion as to how to safeguard transfers to the private sector (open safeguards). The analysis reveals that pre-authorised safeguards, such as public adequacy decisions and *ex ante* legal safeguards are more common (65%). However open safeguards, which include accountability principles, private sector adequacy evaluations and contracts, are also widely used (54%). Most countries incorporate some form of safeguard into their data transfers, but they go about it in different ways.
- *Plurilateral arrangements* that aim to generate consensus around privacy and personal data protection, including in relation to international transfers, have also been widely adopted (including by 97 economies). As both a consequence, and a driver, of these arrangements, 68% of the elements covered in existing domestic privacy and data protection regulation across a sample of OECD and emerging economies overlap. This suggests that there is a high degree of commonality in existing frameworks and therefore some common ground to build on to enable data transfers.
- Since 2008, 29 *trade agreements* between 72 economies have included provisions on data flows. Not all provisions have the same depth – 45% of agreements include binding commitments on data flows (for all types of data). Of those with binding provisions, almost all include exceptions allowing parties to restrict data flows to meet "legitimate public policy objectives" and all couple data flow provisions with provisions on privacy or consumer protection frameworks (including through references to plurilateral arrangements).
- *Standards and technology-driven initiatives* such as ISO standards and privacy-enhancing technologies (PETs), including cryptography and sandboxes, are increasingly being used by organisations to protect and control access to data.

Commonalities are found between and within instruments. For instance, whether through unilateral mechanisms, trade agreements or plurilateral arrangements, there appears to be consensus on the dual goals of safeguarding data and enabling its flow across borders. There is also growing evidence of *convergence*, whether in the trade agreements which combine binding data flow provisions with provisions on privacy and consumer protection frameworks, or in the principles that underpin domestic privacy and personal data protection frameworks. Finally, there exists a high degree of *complementarity* between instruments. Unilateral mechanisms draw from, and contribute to, plurilateral arrangements and trade agreements increasingly reference plurilateral data protection arrangements along with their binding data flow provisions. Together, these can be seen as indicating the emergence of an international architecture, or architectures, aimed at reaping the benefits of data flows while enabling governments to meet other legitimate public policy objectives.

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 these instruments can be conducive to greater overall confidence and "trust" in the environment that underpins the global flow of data and that supports a growing share of our economies and societies.

Executive summary

In today's digitised and globally interconnected world, data has become the lifeblood of economic and social interactions. However, the pervasive exchange of data, including across borders, has fuelled concerns about the use and, especially the misuse, of data, amplifying concerns about privacy protection, digital security, intellectual property protection, regulatory reach, competition policy and industrial policy. This is especially the case in the context of data crossing different jurisdictions.

As a result, countries have been adopting and adapting regulations addressing the movement of data, often introducing measures that condition the movement of data across borders or, in some cases, measures that mandate that data is stored or processed in specific locations. The resulting patchwork of rules and regulations is making it difficult not only to effectively enforce public policy goals such as privacy and data protection across different jurisdictions, but also for firms to operate across markets, affecting their ability to internationalise and benefit from operating on a global scale.

It is increasingly clear that the benefits of digital trade for both businesses and consumers depend strongly on the degree of "trust" (recognising that this can be understood differently) in the digital environment. Individuals will not engage with businesses they do not "trust" and businesses will struggle to reap the benefits of scale unless they can operate with "trust" globally. Although there is no clear consensus on the meaning of "trust" in this context, the concept of *data free flow with trust*, championed by Japan under the G20 'Osaka Track', encapsulates the policy impetus to find a balanced solution to these challenges.

Building on the Osaka Track efforts, G20 Leaders recognised, at the Riyadh Summit in November 2020, the need to continue addressing challenges to "further facilitate data free flow and strengthen consumer and business trust" (G20, 2020[1]). The importance of harnessing "the transformative potential of the digital economy by data free flow with trust" and addressing its challenges was also highlighted in the recent OECD 2020 Ministerial Council Statement (OECD MCM, 2020[2]). At the same time, G20 Digital Economy Ministers underlined the value of "identifying commonalities between existing approaches and instruments used to enable data to flow across borders with trust". Longstanding work at the OECD, and particularly in the Trade Committee, has also been geared towards better understanding the policy environment around trade and cross-border data flows and has underscored the need to promote dialogue on instruments that can help bridge different domestic approaches to data flow regulation.

Against this backdrop, the aim of this paper is to map different approaches and mechanisms available for countries to enable the movement of data across borders with "trust" (recognising that different countries have different understanding of what consumer and business "trust" means and of the mechanisms that might enable "trust" in cross-border data flows). This mapping exercise shows that there is no one, single mechanism to enable the free flow of data with "trust". Governments pursue different, or even multiple and complementary approaches:

- A wide range of *unilateral mechanisms* for safeguarding cross-border transfers exist. These are domestic approaches that vary according to whether safeguards require some form of public sector approval before transfer (pre-authorised safeguards), or if more discretion is left to the private sector as to the nature of safeguards (open safeguards). Analysis across OECD countries and selected economies (76 economies in total) suggests that 'pre-authorised safeguards', which include the use of public adequacy determinations and standard contractual clauses, feature in 65% of economies. By contrast, "open safeguards", which include *ex ante* accountability principles, contracts and private adequacy determinations, feature in 54% of economies (79% and 33% respectively when countries subject to the General Data Protection Regulation (GDPR) are counted individually). Most countries incorporate some form of safeguard in their data transfer mechanisms, but they differ in the way they go about it, with more or less involvement by the government.
- *Plurilateral arrangements* that generate consensus around privacy and personal data protection, including in the context of international transfers, have also been widely adopted. They include, among others, the OECD Privacy Guidelines, the APEC Cross-Border Privacy Rules (CBPR) System and the Council of Europe Convention 108 and related instruments. To date, these plurilateral arrangements involve at least 97 economies, some of which are party to several arrangements. As both a consequence, and a driver, of these, 68% of the elements covered in

existing domestic privacy and data protection regulations across a sample of OECD countries and emerging economies overlap. This suggests that there is a high degree of commonality in existing frameworks and therefore common ground to build on to enable data transfers.

- *Trade agreements* are increasingly including provisions on data flows. Since 2008, 29 agreements involving 72 economies have some form of data flow provisions. However, not all provisions have the same depth – only 45% have binding commitments on data flows (of all types of data). Of those that have binding provisions, almost all include exceptions allowing parties to restrict data flows to meet "legitimate public policy objectives" and include provisions on the need for domestic privacy legislation (including references to plurilateral arrangements).
- *Standards and technology-driven initiatives* such as ISO standards and privacy-enhancing technologies (PETs), such as cryptography and sandboxes, are increasingly being used, at the organisational level, to protect and control access to data, including in the context of international transfers.

The analysis suggests that the specific instruments that countries adopt to enable "trusted" data flows are diverse. However, *commonalities* between and within instruments exist. For instance, whether through unilateral mechanisms, trade agreements or plurilateral arrangements, there appears to be consensus on the dual goals of safeguarding data and enabling its flow across borders. There is also growing evidence of *convergence*, whether in the trade agreements which combine binding data flow provisions with provisions on privacy and consumer protection frameworks, or in the principles that underpin domestic privacy and personal data protection frameworks. Finally, there exists a high degree of *complementarity* between instruments. Unilateral mechanisms draw from, and contribute to, plurilateral arrangements and trade agreements increasingly reference plurilateral data protection arrangements along with their binding data flow provisions. Together, these can be seen as indicating the emergence of an international architecture, or architectures, aimed at reaping the benefits of data flows while enabling governments to meet legitimate public policy objectives.

It is the prerogative of governments to establish the mix of instruments or mechanisms that best serve their policy interests and objectives. However, greater understanding, discussion and agreement on these instruments can be conducive to greater overall "trust" in the environment that underpins the global flow of data and that supports a growing share of our economies and societies.

1. Introduction

In today's digitised and globally interconnected world, data has become the lifeblood of economic and social interactions. It is changing how businesses operate; altering the configuration of global value chains (GVCs); giving rise to new information industries; and changing how services are produced and delivered and even how we trade and grow food (OECD, 2020[3]). Today, firms of all sizes and across all sectors use data, and it is increasingly difficult for an international trade transaction to take place without a cross-border data transfer of some sort.

However, the pervasive exchange of data, including across borders, has fuelled concerns about the use and, especially the misuse, of data, amplifying concerns about privacy and data protection, digital security, regulatory reach and industrial policy, among others. This has resulted in countries updating and adapting their data regulation, often introducing measures that condition the movement of data across borders or that mandate that data is stored or processed in specific locations (Casalini and López González, 2019[4]).

The emerging approaches to data regulation vary significantly across countries and types of data, reflecting differences in preferences for privacy and data protection and governments' pursuit of a range of other policy objectives. However, the resulting patchwork of regulations is creating uncertainty for governments and individuals, including with respect to the applicable rules in a given situation (OECD, 2020[3]). It is also making it difficult for firms, especially smaller ones, to operate across different markets, affecting their ability to internationalise and benefit from trade.

In this evolving environment, it is increasingly clear that the benefits of digitalisation for both businesses and consumers depend strongly on the degree of "trust" in the digital environment. Individuals will not engage with businesses they do not trust and businesses will struggle to reap the benefits of scale unless they can operate globally. The concept of *data free flows with trust*, championed by Japan under the G20 'Osaka Track', encapsulates the policy impetus to find a balanced solution to these challenges.[1]

In 2020, building on these efforts, G20 Leaders recognised, at the Riyadh Summit in November 2020, the need to address current challenges which can "further facilitate data free flow and strengthen consumer and business trust" (G20, 2020[1]). G20 Digital Economy Ministers also recognised the importance of "sharing experiences and good practices for data policy, in particular interoperability and transfer mechanisms, and identifying commonalities between existing approaches and instruments used to enable data to flow across borders with trust" (G20, 2020[5]). Longstanding work at the OECD and in particular in the Trade Committee has also aimed to better understand existing systems and underscored the need to promote further dialogue with a view to identifying instruments to bridge different approaches.

Against this backdrop, and without prejudice to the different approaches taken by countries, this report maps existing commonalities in mechanisms used to enable data to move across borders with "trust". It is hoped that this will help governments in their ongoing discussions across different fora. This includes discussions on e-commerce at the WTO, which touch upon cross-border data flows, privacy protection and data localisation; discussions within the context of trade agreements, which are increasingly including provisions addressing cross-border data flows; and deliberations undertaken across different international arrangements (often) outside the scope of trade.

The paper begins by providing an overview of the evolving regulatory landscape, looking at domestic approaches to cross-border data transfers. Section 3 then identifies different mechanisms for transferring data across borders, categorising these into four broad areas and mapping their use and the common elements within them. Section 5 concludes with observations on the emerging landscape.

The paper builds on existing work (Casalini and López González, 2019[4]) (Casalini, López González and Moïsé, 2019[6]), providing a more focused mapping of existing instruments and mechanisms that relate to cross-border data transfers. Although the focus is on the movement of all types of data across international borders, much of the discussion involves regulations that condition the movement of personal data across jurisdictions, reflecting the fact that privacy and personal data protection are the most common measures.

[1] See also discussion in (WEF, 2020[26]).

2. The existing regulatory landscape[2]

Data has become a critical resource for modern day economic and social activities. Its use and re-use has been shown to generate a number of benefits across societies, often in ways that cannot easily be anticipated (OECD, 2019[7]). Whether for international trade ((National Board of Trade, 2014[8]), (MGI, 2016[9]), (López González and Jouanjean, 2017[10]), (Casalini and López González, 2019[4]), (Aaronson, 2019[11])), production ((National Board of Trade, 2015[12]), (Cory, 2017[13])), and productivity ((OECD, 2015[14]), (Brynjolfsson and McElheran, 2016[15])) in services (Ferracane and Van der Marel, 2018[16]), manufacturing (Brynjolfsson and McElheran, 2019[17]) and agriculture (OECD, 2019[18]), data, and its flow across borders, is powering a digital revolution offering a range of new opportunities to promote growth, wellbeing and inclusion.

Although data-use is often associated with firms operating in services sectors, firms across all sectors rely on data to support their business activities. For instance, in manufacturing, data helps to coordinate research and design outputs; exercise overarching control and coordination of geographically dispersed processes of production; and track and trace products as they travel to the border and beyond (Casalini and López González, 2019[4]). In agriculture, data is supporting a move towards precision agriculture techniques, that rely on data analytics to optimise resources and enable savings on seed, fertiliser and irrigation, as well as enabling new traceability and connections to markets (OECD, 2019[18]).

However, 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 being made of this information is not always clear. This has fuelled a range of concerns about use and misuse of data, including in the context of power relations among firms and between firms and consumers, and in particular with respect to privacy and data protection.[3] 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 protecting privacy, digital and national security; protecting and enforcing intellectual property rights;[4] enabling economic development; and maintaining the reach of regulatory and audit bodies can all become more complex when data crosses jurisdictions.

Moreover, different data are subject to different governance frameworks (OECD, 2020[3]).[5] And data types can overlap, raising issues that touch on different policy domains. In addition, different definitions often exist for different types of data. That is, what one country might consider as personal data might not be considered as such in another (Casalini and López González, 2019[4]). This means that what data is subject to what data governance framework is a complex issue, with challenges compounded when data crosses international borders where definitions, policy domains and data governance frameworks may differ.

---

[2] This section draws heavily on the work undertaken in (Casalini and López González, 2019[4]) and on a recent report for the G20 written with the Science Technology and Innovation Directorate of the OECD (OECD, 2020[3]).

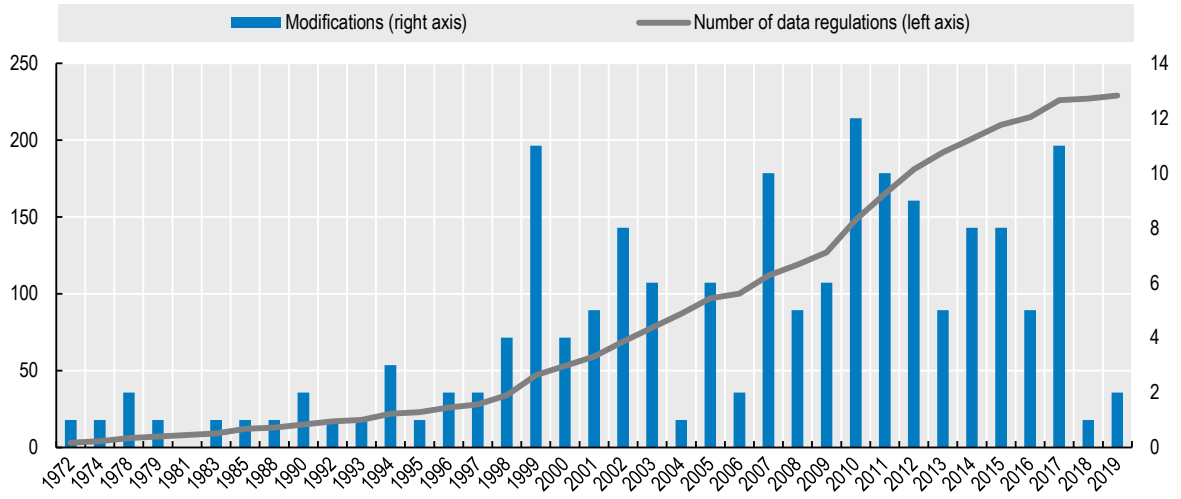
[3] Privacy itself is difficult to define. It means different things to different people and the value attached to privacy, whether as individuals or by society, can be subjective. There can also be trade-offs between benefitting from highly personalised and often 'free' services and the extent to which consumers are able to keep their data private. The optimal choice in that trade-off will also vary according to individual preferences. Having said this, national and international privacy and personal data protection frameworks, including the OECD Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data [OECD/LEGAL/0188] (OECD Privacy Guidelines), provide agreed sets of principles and rules applicable to the protection of privacy and personal data.

[4] The challenges that intellectual property rights raise in the context of cross-border data flows are noted in the Osaka and the Riyadh Declarations. Intellectual property, however, is not addressed in this paper. For an overview of the complexities of different regulatory frameworks, including IPR, see OECD (forthcoming[23]) and OECD (2019[7]).

[5] For example, while personal data might be subject to privacy and personal data protection, data from the private sector may be subject to intellectual property rights (IPR).

In light of these emerging regulatory challenges, governments have been updating and adapting their data-related policies, resulting in a growing number of countries placing conditions on the transfer of data across borders or requiring that data is stored locally (Figure 1).

Figure 1. Data regulation is increasing



Note: "Data regulation" includes 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 Lopez-Gonzalez (2019).

The reasons countries are reviewing their data policy are manifold, but can be broadly grouped into five categories (OECD, 2020[3]). Much of the debate about data flows revolves around the transfer of personally identifiable information, raising concerns about *privacy and data protection*. For some, the challenge is to ensure that, when data is transferred outside a specific jurisdiction, this data continues to receive the same protection that it received in the domestic jurisdiction.[6] 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 the online equivalent of a longstanding practice in the offline world of ensuring that information is readily accessible to regulators. Such measures can be sector-specific, reflecting particular regulatory requirements and targeting specific data, such as business accounts, telecoms or banking data.

Measures related to *national security* often mandate that data be 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 in particular can be very broad in nature, providing wide scope of access to any form of data.

[6] In this context, the issue of government access to personal data held by the private sector is also relevant and is currently being discussed in the OECD Committee on Digital Economy Policy (CDEP). A statement on this issue and its links with cross-border data flows was issued by CDEP in December 2020. It highlights "unconstrained and disproportionate government access to personal data held by the private sector as a crucial issue for data governance and the protection of individual rights and as a potential barrier to enabling the free flow of data with trust" (see https://www.oecd.org/digital/trusted-government-access-personal-data-private-sector.htm). The OECD Committee on Digital Economy Policy is currently discussing the development of high-level principles or guidance in this area.

Governments also promote local storage and processing with a view to ensuring *digital security*. The rationale for implementing countries is that digital 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.

2.1. How are countries regulating cross border data flows?

Two broad types of data policies have emerged relating to cross-border data transfers (Casalini and López González, 2019[4]). Those that condition the movement of data across borders, on which this paper mainly focuses, and those that mandate that data is stored locally (Box 1). Each addresses different and sometimes overlapping policy objectives. The manner in which countries approach their policies relating to the cross-border flow of data tends to reflect the underlying preferences, including in relation to trade-offs. Countries also take different approaches depending on the nature of the data involved. For instance, some might condition the transfer of personal data, but not of private sector manufacturing data, while others might deem industrial data as 'important' (for different reasons) and apply local storage requirements.

Cross-border data flow regulation varies widely, reflecting different cultural preferences and policy objectives.[7] In particular, four broad approaches have emerged (Figure 2). 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 LDCs), 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 other countries to send data to these locations.

The second type of approach does not prohibit the cross-border transfer of data, nor does it require prior public authorisation or specific conditions to be fulfilled, but provides for *ex post accountability* for the data exporter if data sent abroad is misused (e.g. firms send data but if something goes wrong they are legally accountable).

A third approach, *flows conditional on safeguards*, includes approaches relying on a range of pre-authorised and transparent conditions for data transfer. In the context of privacy and personal data protection, these relate to determinations of adequacy or equivalence by a public authority. Where an adequacy determination has not yet been made, firms can move data under options such as binding corporate rules, or model or approved contractual clauses, among others.

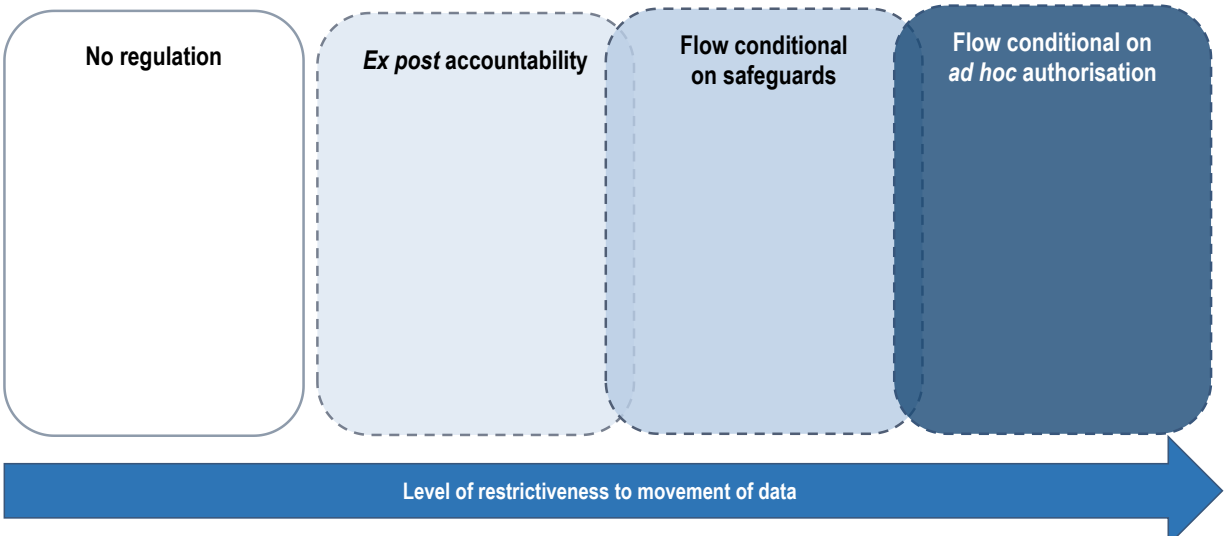
The last broad type of approach, flow conditional on *ad hoc authorisation*, relates to systems that only allow data to be transferred on a case-by-case basis, subject to review and approval by relevant authorities. This approach relates to personal data for privacy reasons, but also to the more sweeping category of "important data", including in the context of national security.

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 "public interest", or in relation to legal

[7] Cross-border data flow regulation has largely, although not exclusively, been developed in the context of international transfers of personal or personally identifiable data; however, countries also condition the flow of other types of data. For instance, the China's Cybersecurity Law conditions the movement of "important" information. Moreover, while some types of data may be able to move abroad, there might be a requirement that firms guarantee access to governments for audit purposes.

claims. Data-subject consent is also a frequently used, albeit limited, concession for permitting data transfers.

Figure 2. Broad approaches to cross-border data flow regulation



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

Box 1. Local storage requirements

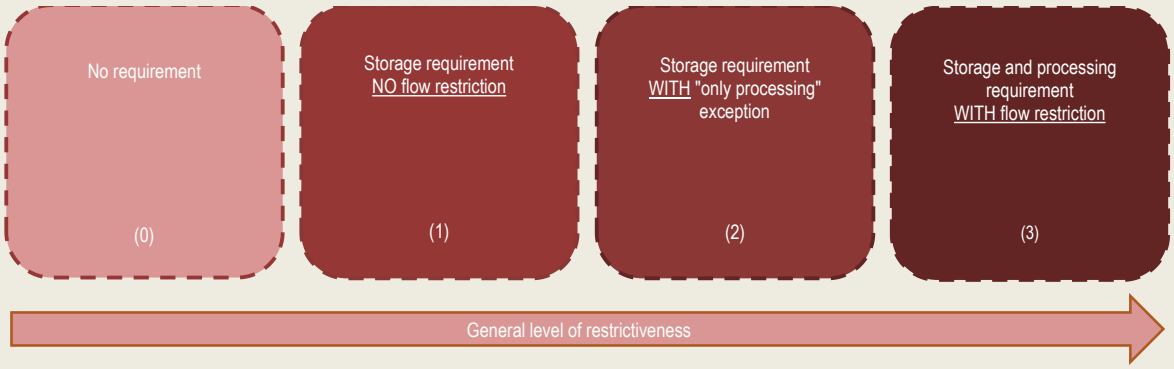
Local storage requirements constitute another type of emerging data-related policy. As their name indicates, measures falling under this category require that certain types of data be stored in local servers, and often also include local processing requirements. Although distinct from cross-border data flow restrictions, a complete prohibition on the transfer of data amounts to a *de facto* requirement for local storage and processing. However, 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 3). 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, telecoms, banking or payment processing, insurance, or satellite mapping.

- 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.
- Next are approaches that require 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.

- Another type of approach is 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 data be stored locally with conditions attached to transferring and/or processing those data abroad.

These last two requirements can be related to national security interests, but also a desire to encourage the development of domestic data storage and other data services industries and thus can be related to industrial policy objectives



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

2.2. What issues does the emerging regulatory landscape raise?

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. For example, 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, effective government enforcement action can also be hindered by a lack of coordination on these inherently transboundary issues. This, in turn, can undermine consumer "trust".

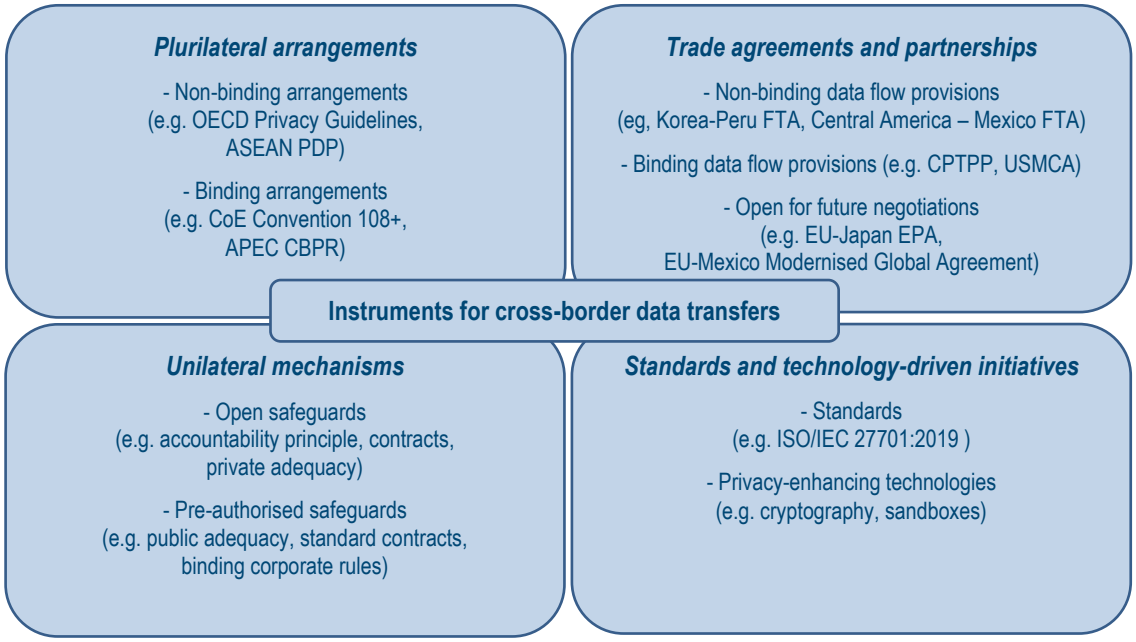
Against this backdrop, and building on discussions under the 'Osaka Track' championed by the Japanese presidency of the G20, G20 Leaders recognised, at the Riyadh Summit in November 2020, the need to continue addressing challenges to "further facilitate data free flow and strengthen consumer and business trust" (G20, 2020[1]). The G20 Digital Economy Ministers' further highlighted the need to share "experiences and good practices for data policy, in particular interoperability and transfer mechanisms, and identifying commonalities between existing approaches and instruments used to enable data to flow across borders with trust" (G20, 2020[5]). The importance of harnessing "the transformative potential of the digital economy by data free flow with trust" and addressing its challenges was also highlighting in the recent OECD 2020 Ministerial Council Statement (OECD MCM, 2020[2])[8] and has been a priority of OECD Committees, including the Trade Committee. To support these efforts and enable continued discussions in this area, the present exercise provides a mapping of the commonalities between approaches currently used to enable data to flow across countries.

[8] On this issue the statement says: "We commit to working together to harness the transformative potential of the digital economy by data free flow with trust and to address its challenges, including data protection and privacy, digital security, disinformation and the digital divides" (OECD MCM, 2020[2]).

3. Identifying commonalities in approaches facilitating cross-border data transfers

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 instruments 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. It is the prerogative of governments to establish what instruments or mechanisms best serve their policy interests and objectives, including in the context of enabling "trust" in data flows. In this context, many different instruments and mechanisms have been devised and implemented, a number of which have been developed for the transfer of personal data. Approaches can be grouped into four broad categories (Figure 3).

Figure 3. Instruments for facilitating cross-border data transfers



Source: Authors' elaboration.

Unilateral mechanisms enable the transfer of certain types of data to countries outside the domestic territory under certain conditions. They include the use of 'open safeguards' referring to ex-post accountability principles, contracts and private sector adequacy, as well as 'pre-authorised safeguards' such as public adequacy decisions, standard contractual clauses or binding corporate rules. These transfer mechanisms are largely developed in the context of transfers of personal data.

Plurilateral arrangements generate consensus around the transfer of specific types of data, again largely in the context of personal data. The most well-known examples are the OECD Privacy Guidelines, the APEC Cross-Border Privacy Rules (CBPR) System or the Council of Europe's Convention 108+.[9] There are many different approaches within this category, with different levels of enforceability.

Trade agreements and partnerships are increasingly addressing issues around data flows in the context of both personal and non-personal data. The depth of rules varies from one agreement to another, with

[9] 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.

varying degrees of binding and exemptions. Trade agreements combine rules on cross-border data flows with provisions on issues such as personal information and/or consumer protection.

Increasingly, data-flows are being discussed in the context of *standards and technology-driven initiatives*. This comprises initiatives by non-governmental actors and includes the use of ISO standards or privacy enhancing technologies (PET), such as cryptography technologies or data sandboxes, which enable access to data within controlled environments.

Each broad instrument tackles the issue of data transfers from a different perspective. The approaches are also not mutually exclusive: countries can use different approaches at the same time with respect to different purposes, partners, types of data and situations. This means that the approaches can often be complementary. 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 mechanisms, focus mainly on issues around privacy and data protection, where there has been most activity in the context of emerging regulation.[10]

3.1. Unilateral mechanisms

What are they?

Unilateral mechanisms are domestic approaches that enable the transfer of certain types of data to countries outside the domestic territory under certain conditions. They are some of the tools through which some of the data policies in the typology shown in Figure 2 are implemented.[11] These can be grouped in terms of two broad mechanisms, largely developed in the context of transfers of personal data: i) 'open safeguards'; and ii) 'pre-authorised safeguards'. The difference between these two mechanisms is that pre-authorised safeguards generally require some form of public sector approval before transfer, while open safeguards leave more discretion to the private sector as to how to safeguard the data being transferred (even if in the context of principles and guidance provided by domestic regulation). The mechanisms are not mutually exclusive: transfers might foresee either a private sector assessment of adequacy, or the use of publicly-authorised safeguards. The use of one mechanism over another may also reflect differing legal cultures.[12]

A number of general exceptions to cross-border transfers may apply across approaches. These include transfers for necessity, legitimate interest, public interest, or through data-subject consent. These are, however, limited concessions for transfers that do not directly seek to safeguard the transfer of data across borders.

Open safeguards include *ex post* accountability principles, contracts or private sector-led adequacy decisions. *Ex post* accountability refers to frameworks that allow cross-border transfers to take place without specific upfront requirements such as additional legal steps. In these cases, "trust" is placed on the data holder on the understanding that, if data is mishandled or misused in the foreign country, the data holder in the regulating country will be accountable. For instance, the US Privacy Act will remain relevant for US citizens if data is misused abroad. Another approach within this category is where transferring entities are encouraged or required to develop their own legal instruments to protect the data when it crosses borders, such as through the use of *contracts*. Finally, "*private sector adequacy*" occurs when the data holder is accountable for having taken reasonable steps to assure the adequacy of protection in the

[10] The analysis herein does not address general exceptions for the transfer of data such as legitimate interest, public interest or data-subject consent. These remain limited concessions that do not directly seek to build trusted environments for the transfer of data across borders.

[11] Another mechanism for transfer is "*ad hoc* authorisation" where transfers are subject to review and approval by relevant authorities. This type of "mechanism" is not discussed in this section owing to its *ad hoc* nature.

[12] Based on the analysis in this report, countries that have a *common law* system tend not to condition cross-border transfers ex-ante, on the understanding that entities transferring data continue to be accountable for the protection of the data under existing principles that prevail in the case of domestic transfers. However, countries that have a *civil law* system tend to see conditioning data flows *ex ante* as necessary to guarantee a degree of equivalence in levels of protection across borders.

transfer, often on the basis of principles set out by the public sector. For instance, in Australia, transfers are permitted provided that the transferring entity "take such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the Australian Privacy Principles". These approaches have in common that they are not subject to *ex ante* approval by a public body. Although these types of rules are most often explicitly found in the context of privacy protection for personal data, they potentially apply to all data for which there are domestic rules, and no additional specific rule relating to cross-border transfers (e.g. in relation to protection of IPRs, or confidentiality).

Pre-authorised safeguards include *public adequacy decisions* and *public sector-led ex-ante safeguards*. Public adequacy decisions are a unilateral recognition by a public body certifying that the personal data protection regime of another jurisdiction meets a certain level of privacy requirements and thus permitting the transfer of personal data to that jurisdiction. A designated public body is in charge of determining adequacy or equivalence on the basis that the protection afforded to individuals in the receiving country is similar to that afforded domestically. This is the case, for example, of the European Commission's (EC) determination that Israel provides an adequate degree of privacy protection or the designation by the Colombian Superintendence of Industry and Commerce ("SIC") that the United States provides adequate protection. The recently invalidated Privacy Shield Framework between the United States and the European Union was another example of an adequacy decision (Box 1).

Box 1. Schrems II: The EU Court of Justice Decision on personal data flows

On 16 July 2020, the European Court of Justice pronounced itself on two mechanisms used by companies to transfer personal data from Europe to third countries. First, it invalidated the "Privacy Shield" framework, an adequacy decision by the European Commission allowing transfers of personal data from the European Union to US-based companies participating in the program. The judgement invalidated the adequacy decision on grounds that surveillance laws in the United States were deemed to go beyond what is strictly necessary by EU standards. The Court also held that the Privacy Shield Ombudsperson mechanism did not provide European data subjects with effective legal remedy.

Second, the Court confirmed that "standard contractual clauses" (SCCs) – model contracts approved by the European Commission that contain data protection safeguards – are a valid instrument for the transfer of personal data outside the European Union. However, it clarified that transfers to any third country, using mechanisms such as contractual clauses, should be suspended or prohibited when the clauses are breached or it becomes impossible to honour them, and this cannot be remedied/addressed through additional safeguards. The decision requires companies to assess, on a case by case basis, whether their counterparts in third countries will be able to comply with the SCCs, in light of possible conflicting obligations under the laws of the third country, e.g. in the context of surveillance. This scrutiny extends beyond transfers to the United States and applies to data transfers to any third country. Further guidance by the European Data Protection Board has been provided on whether and how transfers on the basis of legal safeguards can ensure adequate protection.[1]

1. https://edpb.europa.eu/news/news/2020/european-data-protection-board-41st-plenary-session-edpb-adopts-recommendations_fr.
Source: *Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems* (Case C-311/18, "*Schrems II*"), European Court of Justice.

Ex ante legal safeguards are instruments, sometimes used as an alternative where a public adequacy decision has not been made, that create ex-ante, legal guarantees with regard to the transferred data, aiming to ensure uniform levels of protection and enforcement in the jurisdiction of destination. These unilateral instruments range from standardised contractual safeguards to binding corporate rules (BCR) or other approved legal instruments or schemes. In some instances, they can require the transferring entity to take a number of additional internal steps, as determined by the relevant authorities.[13]

Standard contractual clauses (SCCs) refer to ready-made rules that provide for personal data transfers to third-parties located in other countries. These clauses, designed to be incorporated into contracts, are developed by public authorities in cooperation with Data Protection Authorities (DPAs) and are generally considered to provide sufficient safeguards for the transfer of data, even to countries that do not enjoy an equivalence or adequacy recognition.[14] BCRs bind the affiliates of a multinational company located in different countries to apply effective rights and legal remedies for the protection of personal data according to the regulatory framework where approval for BCRs is sought. These rules, once approved by the designated public body, 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, and might be subject to risk assessment.[15] Finally, other approved legal instruments refers to mechanisms such as codes of conduct, or certification schemes that are either prescribed by the government or that need to be reviewed and approved by a public body in advance of their implementation (to be deemed to provide sufficient safeguards when data crosses borders).

Gauging adoption of different unilateral mechanisms

Use of unilateral mechanisms for enabling data flows across borders varies widely by country, largely reflecting domestic approaches to cross-border data flows (Figure 2). Countries also use different instruments for different purposes, and sometimes they use a range of options for transfer. Analysis of the frequency of availability of different mechanisms across 46 economies (including all OECD countries and selected economies as listed in Annex B) reveals that pre-authorised safeguards are most commonly recognised (Figure 4). Indeed, 65% of economies reviewed (79% when countries in the European Economic Area subject to GDPR are counted individually) rely on this category of instruments versus 54% of economies (33% when GDPR is counted as one) relying on open safeguards.[16]

Notwithstanding the differences between these two categories of approaches, some commonalities emerge (Figure 5). Both types of safeguards include approaches that rely on some form of adequacy (48% of economies using open safeguards and 77% of economies using pre-authorised safeguards), or the use of contracts (48% of economies using open safeguards and 37% of economies using pre-authorised safeguards). The key difference relates to who designs these. In the case of open safeguards, adequacy is assessed by the firm, provided they meet objectives set by the government. In the case of pre-authorised safeguards, the governments make the adequacy determination. Similarly, in the case of open safeguards, it is the firm which decides what provisions the contracts will include, whereas in the case of pre-authorised safeguards, the government drafts the model contracts that must be used by firms.

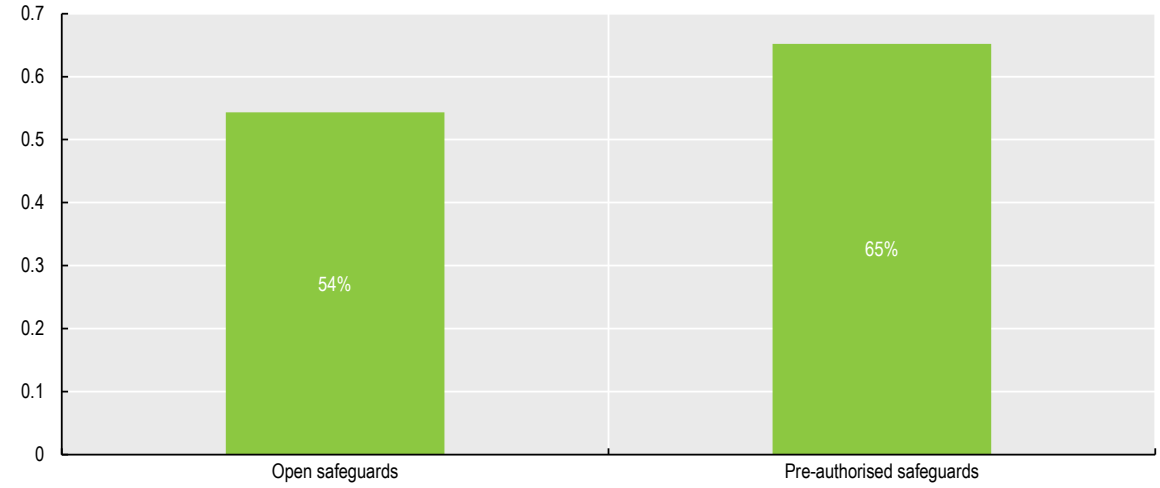
[13] For instance, to ensure that legal instruments for transfers are created (i.e. developing company-wide BCRs).

[14] Although, in some cases, the entities operating the transfer will still need to conduct a contextual risk assessment and adopt supplementary measures necessary to ensure that the level of protection established in the country of origin can be respected in the destination country (that includes, for example, ensuring that there are no conflicts with the law of that country).

[15] The DPA validating a set of BCRs may also need to conduct a risk assessment about the context of the operations.

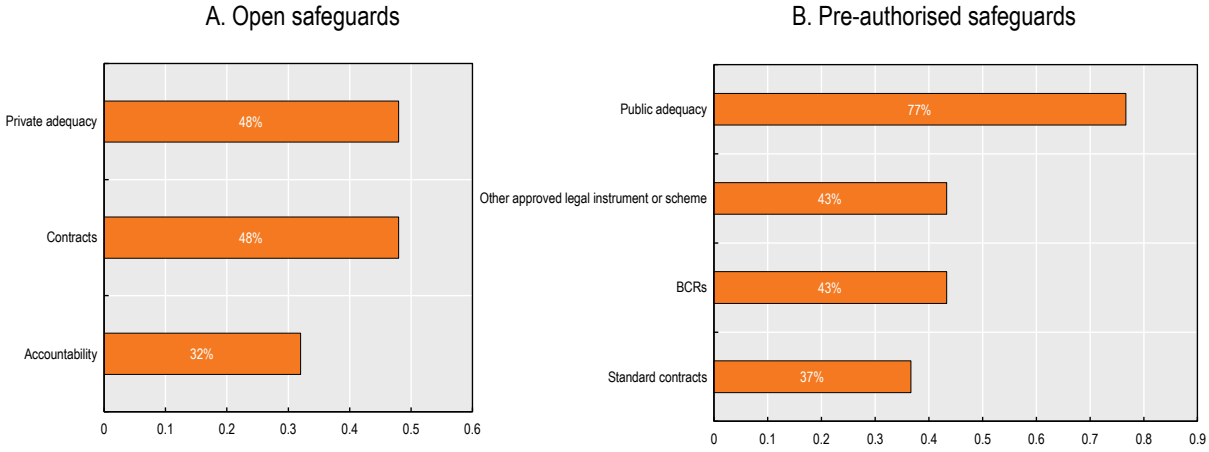
[16] See Annex B for a list of economies covered in this exercise.

Figure 4. Unilateral mechanisms for enabling cross-border data flows



Note: Percentages are calculated with respect to the number of economies that rely on unilateral mechanisms in the existing sample. This is comprised of 46 economies (76 when counting the economies implementing GDPR separately). Last updated October 2020.
Source: Authors' calculation, see Annex B for a discussion of the method used.

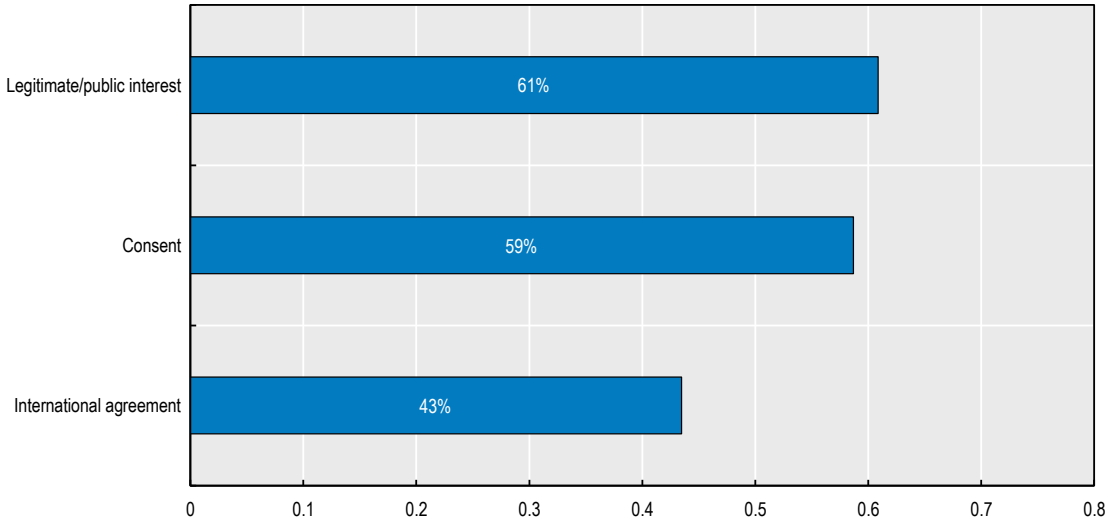
Figure 5. Instruments across broad unilateral approaches



Note: Percentages are calculated with respect to the number of economies within respective categories, see Figure 4 for distribution between open and pre-authorised safeguard categories. The sample includes 46 economies (76 when economies implementing GDPR are counted separately). In Figure 5.b, 'other approved legal instrument or scheme' includes countries recognising either the use of an approved (vs standard) contract, or of an approved code of conduct or certification scheme. Last updated October 2020.
Source: Authors' calculation, see Annex B for a discussion of the method used.

In terms of exceptions, a large majority of the sampled economies (61%) maintain exceptions that allow cross-border transfers that fulfil conditions related to necessity and public interest, with few discernible differences across the two types of unilateral approaches. Consent by the data-subject is also a widely used exception (59%) and many countries also explicitly recognise data transfers based on international agreements, underscoring a degree of complementarity between unilateral mechanisms and plurilateral arrangements (Figure 6).

Figure 6. General exceptions for transfers



Note: Percentages are calculated with respect to the number of economies that foresee these exceptions in the existing sample that comprises 46 economies (76 when economies implementing GDPR are counted separately). Last updated October 2020.
Source: Authors' calculations. See Annex B for a discussion of the method used.

The figures and discussion in this section should not be viewed as guidance on what is or is not best practice. Rather, they represent a count of the different mechanisms available for enabling transfers across countries, without prejudice to countries choice of the instruments that are best suited to their specific situation and social and political contexts.

3.2. Plurilateral arrangements

What are they?

Plurilateral arrangements are international instruments that create rules, or aim to generate consensus, around cross-border transfers of specific types of data, often on the basis of alignment on underlying principles. The most widely discussed are those developed in the context of privacy and data protection.[17] These arrangements have often emerged under the auspices of regional organisations, but may also be open to participation by other countries as well (Table A A.1). Since they provide principles on privacy and data protection and cross-border transfers, they often both reflect and shape the unilateral mechanisms discussed in the previous section.

There are many different approaches to plurilateral arrangements in the context of privacy and data protection, with different levels of enforceability. On one side, there are *non-binding plurilateral arrangements* that rely on "soft law" to encourage parties to adopt data protection principles and promote interoperability between privacy protection regimes in order for data to be transferred abroad. An example of this is the 1980 OECD Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data ("OECD Privacy Guidelines"), which were revised in 2013, and which set out guiding principles to ensure the protection of privacy while avoiding restrictions on data flows that are disproportionate to the risks presented (Box 3). The OECD Privacy Guidelines were the first internationally agreed upon set of privacy principles on the protection of personal data, whether in the public or private sector. They continue to be implemented by countries through legislation, enforcement and policy

[17] However, other plurilateral arrangements, in particular for the sharing of a specific type of data among government agencies, exist across different fields. For instance, Interpol has developed specific *Rules on the Processing of Data* which include legal instruments with a global scope for regulating international exchange of criminal data. Similar agreements can be found in the context of passenger data exchange under the auspices of IATA.

measures, and have influenced developments in privacy law, principle and practice in OECD countries and beyond.

Box 2. The OECD Privacy Guidelines (2013)

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, 2013b) 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 reproduced below:

> (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 is continuing to work with countries and experts to scope developments and provide practical recommendations on the implementation of the Guidelines in today's digital environment (see https://www.oecd.org/sti/ieconomy/privacy-guidelines.htm).

Source: OECD (2020[3]).

A regional example of a non-binding plurilateral approach is the ASEAN Framework on Personal Data Protection (ASEAN PDP Framework), which sets out principles of personal data protection for ASEAN Member States to implement in their domestic laws. In 2018, building on the ASEAN PDP Framework, the ASEAN Framework on Digital Data Governance was endorsed. [18] This framework sets out strategic priorities, principles and initiatives to guide ASEAN Member States in their policy and regulatory approaches towards digital data governance, including for cross border flows of all types of data (see Table A A.1 for participating economies). Principles include facilitating cross-border data flows within ASEAN by developing unambiguous requirements that data can be transferred from one ASEAN Member State to another. In 2019, ASEAN commenced work on the ASEAN Cross Border Data Flows Mechanism and in 2020, ASEAN adopted a set of model contractual clauses (MCCs) to facilitate cross-border data flows in ASEAN Member States. ECOWAS and the Organization of Ibero-American States (in the context of the Ibero-American Data Protection Network) have also developed standards in this field, with the Supplementary Act A/SA. 1/01/10 on Personal Data Protection[19] of 2010, and the Standards for Personal Data Protection for Ibero-American States[20] of 2017, respectively.

There are also *binding plurilateral approaches* with stronger enforcement mechanisms. For instance, 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 binding treaty protecting the right to privacy of individuals with respect to personal data which is automatically processed. To date, 55 states have committed to establish, under their own domestic law, sanctions and remedies for violations of the Convention's provisions (see Table A A.1 for participating economies). The 2018 Amending Protocol, when it enters into force, will update the provisions on the flow of personal data between signatories (creating what is commonly known as Convention 108+).

The APEC Cross-Border Privacy Rules (CBPR) System, in place since 2011, also has a binding element, although it operates very differently.[21] The CBPR System is a government-backed data privacy certification framework that companies can join to demonstrate compliance with agreed privacy protection principles and enforcement mechanisms, allowing them to transfer data between CBPR participating economies with greater trust.[22] 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. However, once a company acquires the CBPR certification, it assumes liability under the CBPR framework *vis-á-vis* participating economies.[23] To date, nine economies participate in the APEC CBPR system, four of which have accredited certification bodies, and around 30 companies have acquired the CBPR certifications – see Table A A.1 for participating economies.[24]

Another example of such an instrument is the 2014 African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention).[25] The Convention includes principles on personal data

---

[18] https://asean.org/storage/2012/05/6B-ASEAN-Framework-on-Digital-Data-Governance_Endorsed.pdf.

[19] https://www.statewatch.org/media/documents/news/2013/mar/ecowas-dp-act.pdf.

[20] https://iapp.org/media/pdf/resource_center/Ibero-Am_standards.pdf.

[21] Indeed (APEC, 2019[24]) stipulates that "*Once an organization has been certified for participation in the CBPR System, these privacy policies and practices will become binding as to that participant and will be enforceable by an appropriate authority, such as a regulator to ensure compliance with the CBPR program requirements*."

[22] The APEC CBPR System requires participating businesses to implement data privacy policies consistent with the APEC Privacy Framework, a principles-based model for national privacy laws that encourages the development of appropriate information privacy protections and ensuring the free flow of information in the Asia Pacific region. The APEC Privacy Framework was first endorsed in 2005 and updated in 2015.

[23] Non-compliance may result in loss of CBPR certification, referral to the relevant government enforcement authority and penalties.

[24] See www.cbprs.com, accessed June 2020.

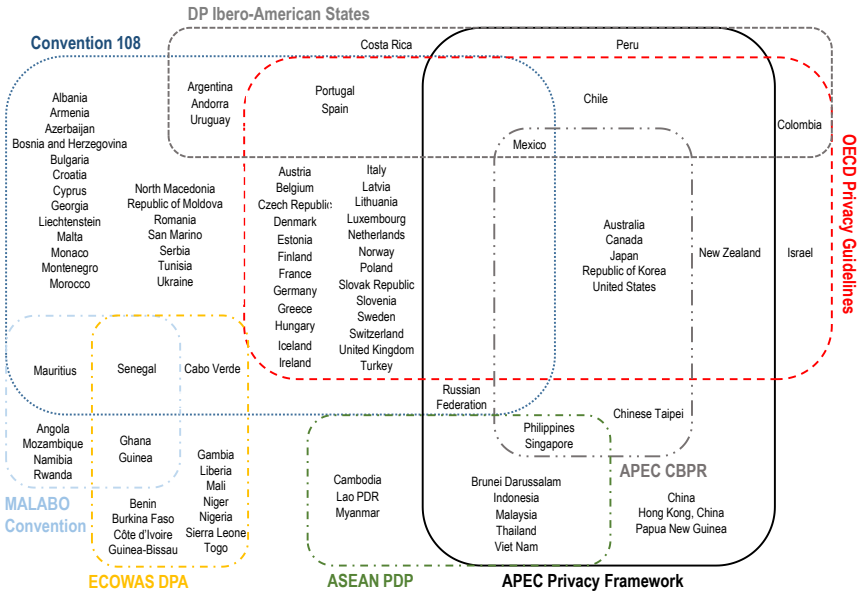
[25] https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf

protection, and targets the protection of privacy without prejudice to the principle of free flow of personal data. To date, 14 countries have signed the Convention and 8 countries have ratified it (ratification of 15 countries is required for the Convention to enter into force; see Table A A.1 for participating economies).[26]

Gauging overlap in privacy and personal data protection frameworks to identify convergence

Plurilateral arrangements are wide and varied. To date, in the context of privacy and personal data protection, they involve at least 97 economies participating in a range of arrangements, often with overlapping membership (Figure 7).[27] Although the picture is complex, there are also commonalities in the principles that underpin these arrangements, and looking at these commonalities in the underlying privacy and personal data protection principles can be helpful in better understanding the evolving international environment.

Figure 7. The overlapping memberships of plurilateral arrangements



Note: For illustrative purposes. Last updated 2 November 2020.
Source: Authors' elaboration.

[26] https://au.int/sites/default/files/treaties/29560-sl-AFRICAN%20UNION%20CONVENTION%20ON%20CYBER%20SECURITY%20AND%20PERSONAL%20DATA%20PROTECTION.pdf

[27] It can be difficult to count the number of countries relying on the OECD Privacy Guidelines. Here, only OECD countries are counted, despite there being wide evidence that adoption of OECD Privacy Guidelines is more widespread.

The common processes or principles seen in these arrangements are generally translated into domestic legislation. In this sense, plurilateral arrangements can promote the adoption of common privacy and data protection principles and reduce uncertainties related to the degree of protection afforded to individuals when data is moved across different jurisdictions. That said, causation can also run in the other direction, with likeminded economies self-selecting into different arrangements.

Identifying similarities in privacy and data protection regulation across economies can provide useful insights into the existing degree of convergence on issues that might matter to enable cross-border data flows, including in the context of the wide overlap in membership across the different arrangements. This can be done by codifying the broad elements contained in the privacy and data protection regulation of different economies involved in these arrangements – see Annex B for information on the methodology.

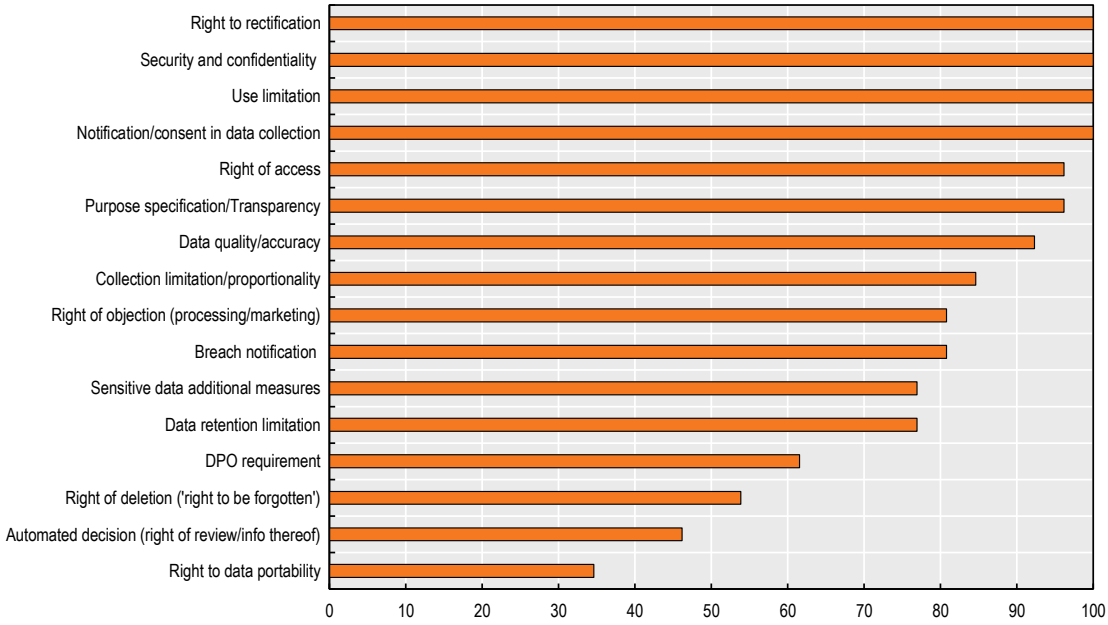
This codification is based on a stylised representation of terms used in privacy and personal data protection regulation, and as such, it provides a rudimentary method for assessing overlap or convergence. For example, two countries may both include in their domestic privacy and data protection regulation the principle of purpose limitation, but they may define or implement it differently. There might also be important differences in terms of the mechanisms and institutional structures used to enforce the privacy and data protection regulation. Nevertheless, and notwithstanding these caveats, it can be useful to undertake this exercise to gain an initial insight into the extent to which countries' existing frameworks currently overlap. Even the existence of common categories in this way can provide indications of areas where further work could be undertaken to understand and perhaps narrow differences between approaches. This analysis should thus be seen as an initial step in assessing convergence upon which such efforts could be built.

Examination of the issues covered in privacy and data protection regulation reveals a high degree of overlap across the elements covered in these regulations (Figure 8). In particular, there seems to be universal adoption, at the level of principle, of issues such as notification and consent, lawful basis for processing, purpose limitation, transparency and openness, security and confidentiality, and right to rectification. These are also issues which are reflected in the OECD Privacy Guidelines. While not universal, there is also strong overlap in terms of references to proportionality, data retention and right to withdraw consent. However, at present, there seems to be less overlap on issues such as the right to be forgotten or the right to data portability.

In terms of aggregate overlap in approaches across countries (Figure 9), the analysis also reveals strong similarities in the set of provisions covered in existing privacy and personal data protection regulations across countries (notwithstanding, as mentioned earlier, issues related to definitions and enforcement). This is partly driven by the finding that there seems to be wide, general agreement on a number of privacy and data protection principles (Figure 8). On average, across the economies sampled, there is an overlap of 68% in the regulations as measured by this method. The degree of overlap between parties to a same plurilateral arrangement is also high. On average, the economies covered in this exercise that participate in Convention 108 have a 76% overlap in their regulatory provisions. For the economies covered in this exercise participating in the OECD Privacy Guidelines, the degree of overlap with each other is 71%. However, the APEC system covers a more diverse group and therefore the economies participating in that arrangement have a slightly lower overlap in terms of their sets of domestic regulatory provisions of 68%.

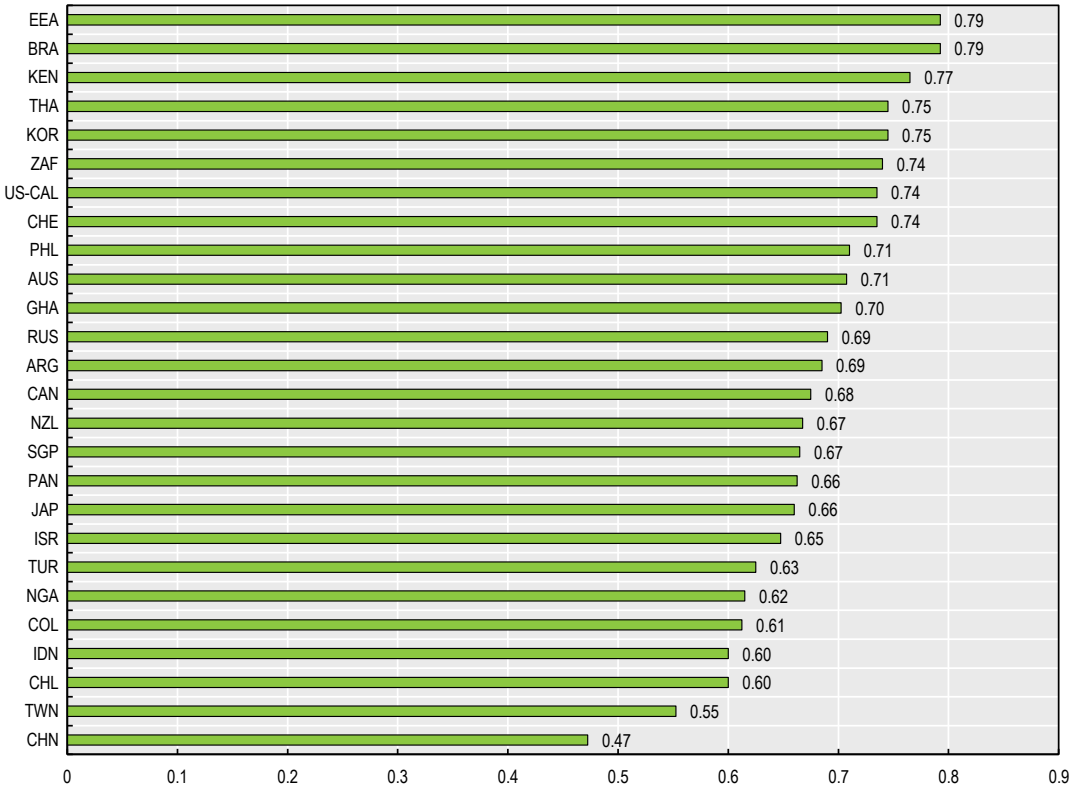
In terms of aggregate overlap in approaches across countries (Figure 9), the analysis also reveals strong similarities in the set of provisions covered in existing privacy and personal data protection regulations across countries (notwithstanding, as mentioned earlier, issues related to definitions and enforcement). This is partly driven by the finding that there seems to be wide, general agreement on a number of privacy and data protection principles (Figure 8). On average, across the economies sampled, there is an overlap of 68% in the regulations as measured by this method. The degree of overlap between parties to a same plurilateral arrangement is also high. On average, the economies covered in this exercise that participate in Convention 108 have a 76% overlap in their regulatory provisions. For the economies covered in this exercise participating in the OECD Privacy Guidelines, the degree of overlap with each other is 71%. However, the APEC system covers a more diverse group and therefore the economies participating in that arrangement have a slightly lower overlap in terms of their sets of domestic regulatory provisions of 68%.

Figure 8. Overlap on issues covered in privacy and personal data protection regulation



Note: Values identify the overlap in stated principles across the privacy and data protection regulation of 26 economies (56 when counting the economies implementing GDPR (31) separately). It is important to note that this analysis identifies the overlap in the presence of different elements of regulation and not the overlap in how these are defined, implemented, or enforced. It is therefore a stylised representation of emerging overlaps. Table up to date until December 2020. New rules on personal data protection are under discussion in many countries, including in Chile, China, etc.
Source: Authors' compilation. See Annex B for a discussion of the method used.

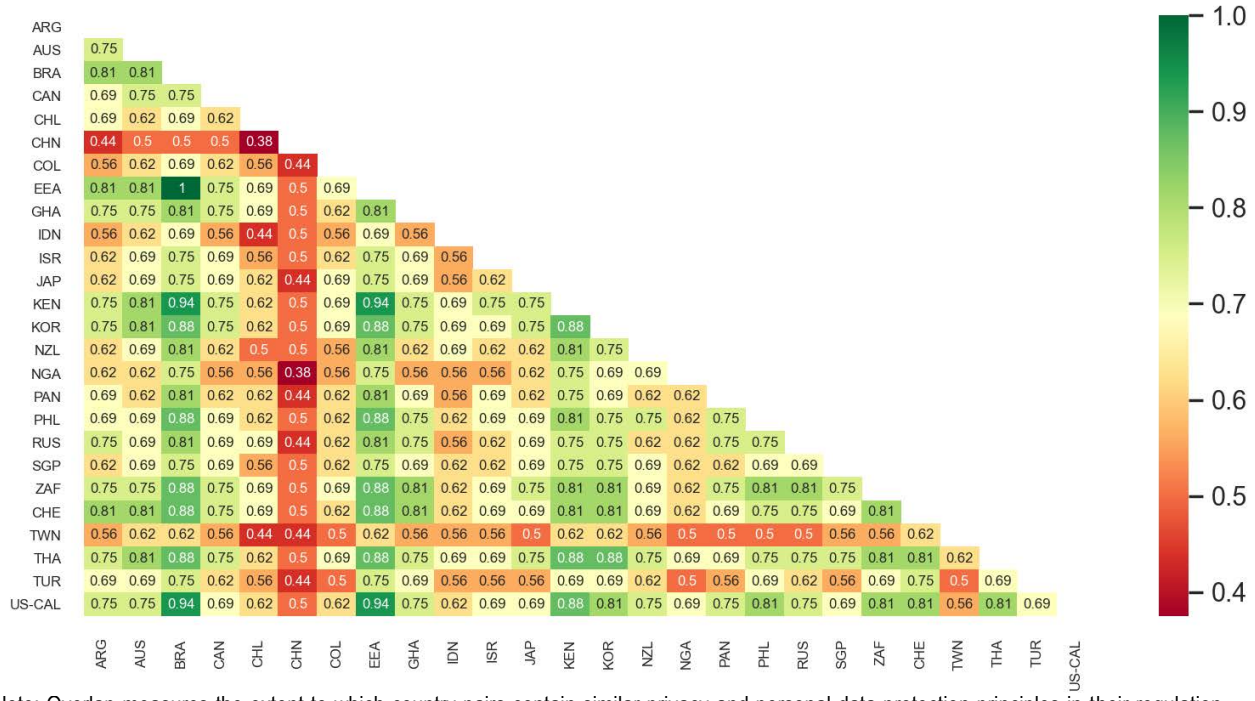
Figure 9. Average overlap in privacy and personal data protection regulation



Notes: Values identify the average overlap in privacy and personal data protection regulation across a sample of 26 economies (56 when counting the economies implementing GDPR (31) separately). It is important to note that this analysis identifies the overlap in the presence of elements of regulation and not the overlap in how these are defined of implemented. It is therefore a stylised representation of emerging overlaps. Table up to date until December 2020. New rules on personal data protection are under discussion in many countries, including in Chile, China, etc.
Source: Authors' own compilation. See Annex B for a discussion of the methodology.

Looking in more detail at the data at the bilateral level (Figure 10) confirms the high degree of overlap, but also provides more granularity as to where the overlap is higher or lower across economy pairs. For instance, the overlap between the EEA approach as captured under GDPR and that of Switzerland is high, but relative to China there is a rather low overlap. Indeed, China, Indonesia and, to a lesser extent, Turkey, seem to have the lowest degree of overlap with others. Nevertheless, at the bilateral level, 85% of the bilateral combinations in Figure 10 have an overlap in provisions above 60%.

Figure 10. Bilateral overlap in privacy and personal data protection regulation



Note: Overlap measures the extent to which country pairs contain similar privacy and personal data protection principles in their regulation (without prejudice to different approaches to, and degrees of, enforcement). Colours capture range of overlap with red showing low overlap and green showing higher overlap. Table up to date until December 2020. New rules on personal data protection are under discussion in many countries, including in Chile and China.
Source: Own calculations.

Overall, these results suggest that there might be elements of convergence in the principles enshrined in different privacy and data protection regulations. This may have come as a result of the plurilateral agreements themselves, or may have driven the formation of plurilateral arrangements as likeminded countries form coalitions. Regardless, this may indicate that plurilateral arrangements might be an avenue to, or important building block in, finding greater agreement on privacy and personal data protection issues, and, in turn, facilitate the movement of personal data across borders with "trust".

3.3. Trade agreements and digital trade partnerships

What are they?

WTO agreements such as the General Agreement on Trade in Services (GATS) and the General Agreement on Tariffs and Trade (GATT) have a bearing on data flows, as data measures may impact trade in goods, goods with embodied or embedded services, and digitally enabled services. However, assessing the legality of measures on data can be complex (see (Casalini and López González, 2019[4])). While there are ongoing discussions in the context of the Joint Statement Initiative on e-commerce at the

WTO that cover "trade-related aspects of electronic commerce", [28] including data flows and privacy protection, the issue of cross border data flows is increasingly being addressed in regional trade agreements (RTAs).

The depth of rules varies among agreements. One category of agreements includes *non-binding guidance on data flows*, with broad provisions affirming the importance of working to maintain cross-border data flows (e.g. Korea-Peru FTA and Central America-Mexico FTA). [29] Another category of agreements includes language that foresees a reassessment of the need for data flow provisions in *future revisions* (e.g. EU-Japan and EU-Mexico).[30] The last category of trade agreements is those that provide *binding rules on data flows*, relating to transfers of all types of data, often with enforcement mechanisms (e.g. CPTPP and USMCA)[31]. Although the detailed approaches in the agreements in this category differ, the following common principles can be identified:

Unrestricted movement of data: Cross-border transfers of information, including personal information, by electronic means *shall not be restricted* or *shall be allowed* if this activity is for the conduct of business;

Exceptions for legitimate public policy objectives: Parties are allowed to maintain measures that restrict the movement of data to achieve legitimate public policy objectives, some agreements stipulate:

- *Non-discrimination:* Measures to achieve legitimate public policy objectives shall not be applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and
- *Not-unnecessarily trade restrictive:* Measures to achieve legitimate public policy objectives shall not impose restrictions on transfers of information greater than are necessary to achieve the stated objectives.

New agreements also include either additional variations on these principles or new types of provisions. For instance, the recently signed Regional Comprehensive Economic Partnership (RCEP) includes a specific exception to *protect essential security interests*.[32] In turn, the recent EU-UK TCA contains binding provisions on cross-border data flows and disciplines on data localisation.[33] It also states that parties may adopt or maintain measures on the protection of personal data, "*including with respect to cross-border*

---

[28] World Trade Organization, *Joint Statement on Electronic Commerce,* WT/L/1056, 25 January 2019, https://trade.ec.europa.eu/doclib/docs/2019/january/tradoc_157643.pdf.

[29] For instance, Nicaragua-Chinese Taipei FTA Art. 14.05 and Colombia-Costa Rica FTA Art. 16.7 (original text in Spanish; translation authors' own) stipulate "Recognizing the global nature of electronic commerce, the Parties affirm the importance of: […] (c) working to maintain cross-border flows of information as an essential element in fostering a vibrant environment for electronic commerce;"

[30] For instance, the EU-Mexico Modernised Global Agreement Art XX and the EU-Japan EPA stipulate "The Parties shall reassess within three years of the date of entry into force of this Agreement the need for inclusion of provisions on the free flow of data into this Agreement."

[31] CPTPP, Art. 14.11, USMCA, Art. 19.11.

[32] RCEP Art. 12.15.3 stipulates "Nothing in this Article shall prevent a Party from adopting or maintaining: […] (b) any measure that it considers necessary for the protection of its essential security interests. Such measures shall not be disputed by other Parties."

[33] EU-UK TCA Art. DIGIT.6 "[t]he 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".

data transfers, provided that the law of the Party provides for instruments enabling transfers under conditions of general application[34] for the protection of the data transferred."[35]

Trade agreements, whether with binding or non-binding rules on data flows, increasingly also include provisions on protection of personal information and online consumer protection.[36] While they do not usually provide detailed privacy principles,[37] they increasingly encourage or require parties to adopt or maintain legal frameworks that provide for the protection of personal information.[38]

In requiring the development of legal frameworks for the protection of personal information, trade agreements may also request parties to take into account principles and guidelines set by relevant international bodies, including the abovementioned plurilateral arrangements. For example, the USMCA references the APEC Privacy Framework and the OECD Privacy Guidelines as relevant international principles and guidelines for privacy protection. Agreements can also encourage the development of mechanisms to promote compatibility between different privacy and data protection regimes. For instance, the USMCA makes reference to the APEC CBPR system. RTAs might also require parties to publish information on the privacy and data protection that they provide to participants in digital trade (e.g. how businesses can comply with any legal requirements and/or how individuals can pursue remedies). In this way, trade agreements can contribute to promoting regulatory convergence and also provide incentives for further regulatory cooperation.[39]

Gauging use of data flow provisions in trade agreements

Use of trade agreements as instruments to enable data flows with "trust" is growing (Figure 11). The Trade Agreements Provisions on Electronic-commerce and Data (TAPED) database (Burri and Polanco Lazo, 2019[19]) shows that, since 2008, 72 economies have signed provisions on data flows across 29 agreements – See Table A A.2 for a list of these agreements.[40] All of these agreements also contain provisions related to privacy protection.

However, as noted above, not all trade agreements have the same depth in their provisions. Around 45% of agreements provide *non-binding* guidance on data flows, including broad provisions promoting cooperation in maintaining cross-border information flows. A further 45% of agreements provide *binding* commitments to enable cross-border data flows. Finally, around 10% of agreements leave decisions on whether parties include provisions on data flows to future negotiations (Figure 12).[41]

---

[34] Its footnote 34 stipulates "*"conditions of general application" refer to conditions formulated in objective terms that apply horizontally to an unidentified number of economic operators and thus cover a range of situations and cases.*"

[35] EU-UK TCA Art. DIGIT.7.

[36] Broader principles on domestic regulation as enshrined in other provisions in trade agreements can also be relevant to the issue of cross-border data flows. In particular, the Japan-UK EPA concluded in October 2020 introduced a provision stipulating that "each Party shall ensure that all its measures of general application affecting electronic commerce, including measures related to its collection of information, are administered in a reasonable, objective and impartial manner" (Art. 8.74).

[37] That said, agreements such as DEPA and USMCA specify certain principles that should be included in a "robust personal information protection framework" (Art. 4.2.3).

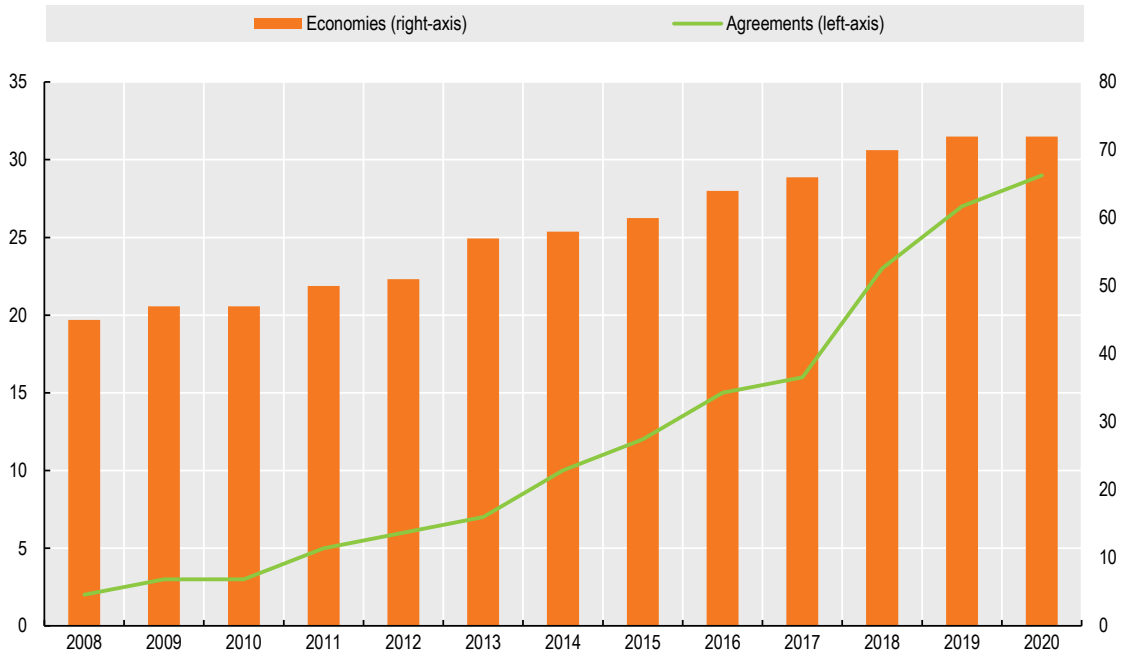
[38] For instance, see CPTPP, Art. 14.8, USMCA, Art. 19.8.

[39] For instance, the CPTPP and the USMCA both encourage parties to exchange information and share experiences on regulations, policies, enforcement and compliance, including on personal information protection (CPTPP, Art. 14.15, USMCA, Art. 19.14.). More broadly, trade can provide the economic incentives for regulatory cooperation.

[40] This exercise relies on the TAPED dataset and Codebook updated on 8 June 2020. The data was accessed on the 12th of October 2020 at the following link https://www.unilu.ch/en/faculties/faculty-of-law/professorships/managing-director-internationalisation/research/taped/.

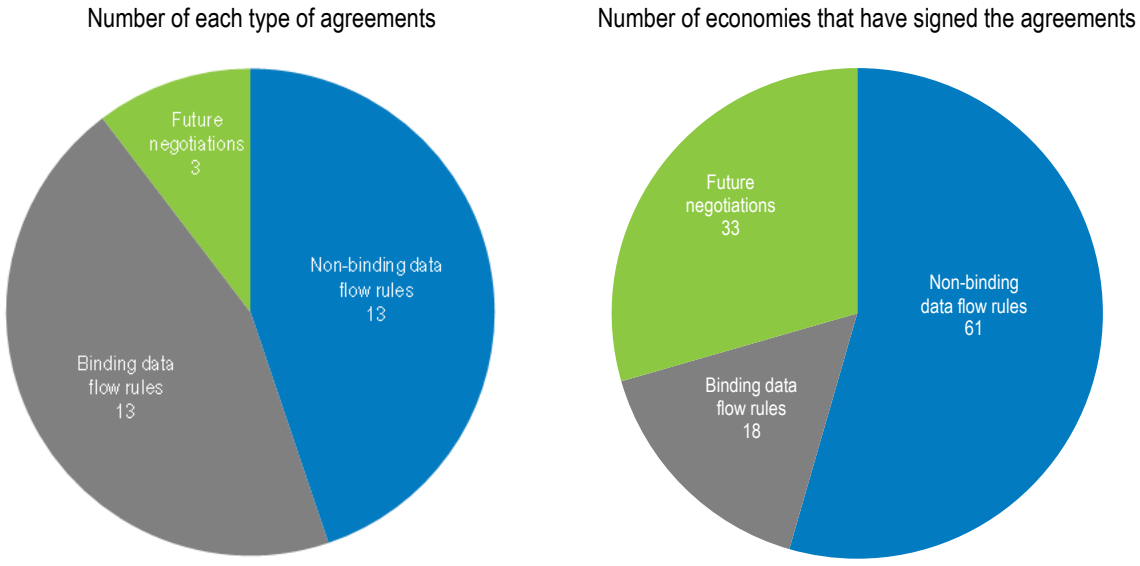
[41] At the same time, some trade agreements that contain non-binding data flow rules or leave the rule making to future negotiations include a general rule on domestic regulation, which, for instance, requires that all measures of general application affecting electronic commerce are administered in a reasonable, objective and impartial manner (e.g. EU-Japan EPA, Japan-Mongolia FTA).

Figure 11. The number of trade agreements with data provisions is growing



Note: See Table A A.2 for a list of agreements. Each EU Member country is counted as one economy.
Source: Own calculations from TAPED database (Burri and Polanco Lazo, 2019[19]).

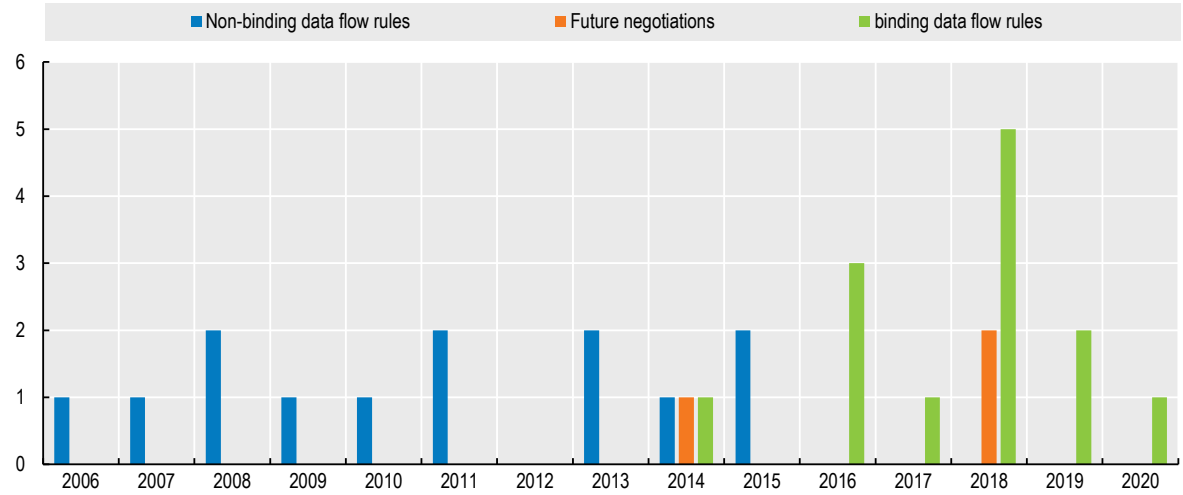
Figure 12. Data flow provisions vary across trade agreements



Note: The agreements covered are listed in Annex A. Most recent agreements that have yet to be covered by the latest TAPED database, for instance, RCEP and the Japan-UK CEPA, are not reflected in the table.
Source: Authors' elaboration based on the TAPED database (Burri and Polanco Lazo, 2019[19]).

Although the number of agreements that include binding data flow rules is the same as the number with non-binding data flow rules, almost all recent trade agreements include the former type of rules (Figure 13). This is also the case in more recent agreements such as the RCEP signed in November 2020, and the Japan-United Kingdom Comprehensive Economic Partnership Agreement (Japan-UK CEPA) which entered into force on January 2021.

Figure 13. Binding data flow rules have been increasing



Note: The agreements covered are listed in Annex A. Most recent agreements that have yet to be covered by the latest TAPED database, for instance, RCEP and the Japan-UK CEPA, are not reflected in the table.
Source: Authors' elaboration based on the TAPED database (Burri and Polanco Lazo, 2019[19]).

The agreements that provide binding rules on data flows and include provisions that foresee *unrestricted movement of data*, also tend to have exceptions allowing parties to restrict the movement of data for legitimate public policy objectives, (although they do not usually provide further definition of what would be regarded as "legitimate"). Each agreement also includes exceptions. About half, including CPTPP, USMCA and the Japan-UK CEPA, subject exceptions to requirements related to both *non-discrimination* and *not unnecessarily trade restrictive* principles. Others, including the Argentina - Chile FTA, only reference *non-discrimination*. Furthermore, more recent agreements, such as RCEP, include a new type of specific exception that allows parties to adopt measures to protect "essential security interests" which "shall not be disputed by other Parties". Moreover, while most of the binding data flow provisions in trade agreements are subject to dispute settlement mechanisms, those in the Japan-US digital trade agreement and RCEP are not. [42]

Increasingly trade agreements also tackle elements related to the concept of "trust". Indeed, all 29 trade agreements with data flow provisions also include provisions related to the protection of personal information and consumer protection. While some simply recognise the importance of such provisions, all agreements that include binding data flow rules also require or promote the adoption of domestic privacy and personal data protection frameworks. This includes encouraging parties to take into account international standards and guidelines on protection of personal information (including some of those mentioned in the plurilateral arrangements section).[43] Indeed, many economies with binding data flow provisions are also party to at least one of the plurilateral arrangements listed in previous section. Out of 18 economies that have signed agreements with binding data flow provisions, 15 have joined at least one of the plurilateral arrangements listed in the previous section.[44] Other provisions in such agreements include requiring parties to publish information on the personal information protection provided;

[42] For instance, RCEP stipulates that in in the event of any differences between parties regarding the interpretation and application of its e-commerce chapter, parties shall first engage in consultations, followed by referring the matter to the RCEP Joint Committee.

[43] Some agreements, such as USMCA and Australia-Singapore, specify what is included in these international standards and guidelines.

[44] 33 economies out of the 61 that have signed agreements with non-binding data flow provisions are party to one plurilateral arrangement.

Table 1. Binding data flow rules have different exceptions

Type of exceptions	Number of agreements	Number of economies that have signed the agreements	Number of agreements that subject data flow rules to dispute settlement
LPPO - Non-discrimination - Not-unnecessarily trade restrictive	6	12	5
LPPO - Non-discrimination	5	8	5
LPPO - Non-discrimination Essential security interests	1	2	1
GATT exceptions[1]	1	2	1
Total	13 agreements	18 economies[2]	12 agreements

Note: LPPO stands for legitimate public policy objectives. The agreements covered are listed in Annex A. Most recent agreements that have yet to be covered by the latest TAPED database, for instance, RCEP, UK-EU TCA and the Japan-UK CEPA, are not reflected in the table.
1. While an article on cross-border flow of information in Mexico-Panama FTA (Art. 14.10) does not include a provision on exceptions, the agreement stipulates that Article XX of the GATT 1994 is incorporated into Chapter on Electronic Commerce and form an integral part of it, mutatis mutandis (Art. 19.2).
2. Some economies have signed more than one agreement.
Source: Authors' elaboration based on the TAPED database (Burri and Polanco Lazo, 2019[19]).

Overall, the analysis suggests that binding data flow provisions go hand in hand with exceptions for legitimate public policy objectives and/or provisions on privacy (and consumer protection). Governments are increasingly using trade agreements to underpin both the need to enable data flows as essential to trade in the digital era, and the recognition that data flows need to be accompanied by safeguards for personal data protection, including via reference to plurilateral arrangements.

Table 2. Binding data flow provisions are closely associated with provisions on the protection of personal information

	Include personal information protection provisions	Require or promote adoption of domestic privacy and personal data protection frameworks	Reference international standards	Encourage the development of mechanisms to promote compatibility between different personal information protection regimes	Require or encourage publishing information on the personal information protection that is provided
Binding data flow rules (13 agreements)	13	13	10	9	12
Non-binding data flow rules (13 agreements)	13	7	5	0	0
Leave discussions to future negotiations (3 agreements)	3	1	1	0	0
Total (29 agreements)	29	21	16	9	12

Note: The agreements covered are listed in Annex A. Most recent agreements that have yet to be covered by the latest TAPED database, for instance, RCEP and the Japan-UK CEPA, are not reflected in the table.
Source: Author's elaboration based on the TAPED database (Burri and Polanco Lazo, 2019[19]).

3.4. Standards and technology-driven initiatives

What are they?

The instruments that fall within this category are different from those discussed in the previous sections. Rather than regulatory instruments by governments, these are tools developed by non-governmental and private sector organisations with a view to better handling issues around cross-border data flows in the context of privacy and security protection.

Two broad categories emerge in this area:

- *Standards,* referring to standards and principles providing guidance on how organisations might manage cross-border transfers in the context of privacy and security risks; and
- *Technology-driven initiatives,* referring to the use of privacy enhancing technologies (PETs) that enable organisations to meet privacy and digital security objectives when transferring data abroad.

This is a fast developing area, and, as for the other instruments, the two approaches are not mutually exclusive: firms can both apply an ISO standard and use privacy enhancing technologies to secure data (indeed, sometimes the latter is a means of implementing the former). These instruments represent organisational tools that attempt to tackle trusted data flows from a different perspective.

Examples of approaches in this areas

Identifying adoption of these instruments is complicated by the fact that, as they are adopted at the organisational level, they are difficult to track. However, examples of different approaches taken in this area can nonetheless help provide insights into the existing options available to organisations when pursuing organisational or technological solutions to build greater "trust" in cross-border data flows.

In terms of *standards*, the International Organization for Standardization (ISO), an independent, non-governmental international standard-setting body composed of representatives from national standards organizations, has developed standards related to privacy and personal data protection. For example, ISO/IEC 27701:2019 specifies requirements and provides guidance for establishing, implementing, maintaining and improving Privacy Information Management Systems (PIMS) (ISO, 2019[20]).[45] More specifically, the standard provides guidance for Personally Identifiable Information (PII) controllers and processors and is aimed at helping organisations comply with domestic data regulations, including GDPR. In terms of the collection and processing of PII across borders, the standards require organisations to specify and record the countries and international organisations to which data is transferred.[46] Organisations are also called upon to "reject any requests for PII disclosures that are not legally binding"[47] and to notify customers of any legally binding requests for disclosure to third parties, such as law enforcement agencies.[48] These standards could help companies comply with domestic data governance legislation.

Technology-driven initiatives may also enable greater "trust" in cross border data flows. Privacy-enhancing technologies (PETs), such as cryptography, are designed to prevent and mitigate the risk of privacy and confidentiality breaches and to enable organisations to better manage data responsibly (OECD, 2017[21]; OECD, 2019[7]; OECD, 2020[3]). In addition, data sandboxes (see below) offering strong levels of control

[45] Privacy Information Management Systems refers to information security management systems which address the protection of privacy as potentially affected by the processing of personally identifiable information (ISO/IEC 27701:2019, 3.2).

[46] ISO/IEC 27701, 7.5.2.

[47] ISO/IEC 27701, 8.5.5.

[48] ISO/IEC 27701, 8.5.4.

and protection of data could also be leveraged towards enabling cross-border access in the case of specific types of data (OECD, 2019[7]).

Homomorphic encryption is "a form of encryption that allows certain computations on encrypted data, generating an encrypted result which, when decrypted, matches the result of the same operations performed on the data before encryption". It can be used "to analyse data in circumstances where all or part of the computational environment is not trusted, and sensitive data should not be accessible" (The Royal Society, 2019[22]). For instance, homomorphic encryption enables a user to encrypt data, send it to the cloud for processing, have the output of the computation sent back to him or her to be decrypted to obtain the result the user wanted, while maintaining the privacy of the individual and confidentiality of the data. The United Kingdom's NHS Digital is using such homomorphic encryption to enable safer sharing and linkage of patient-level data between authorised parties, aiming to improve health and care service through research and planning (The Royal Society, 2019[22]).[49]

Data sandboxes are isolated environments through which data can be accessed and analysed and where analytic results are only exported, if at all, when they are non-sensitive. These sandboxes can be isolated virtual machines that cannot be connected to an external network and/or machines which are required to have physical on-site presence within the facilities of the data holder (where the data are located) (OECD, 2019[7]). The Center for Medicare and Medicaid's (CMS) Virtual Research Data Center (VRDC) is a virtual research environment that provides timely access to Medicare and Medicaid programme data, such as beneficiary-level protected-health information. Researchers working in the CMS VRDC have direct access to approved data files, can conduct their analysis within the CMS secure environment and can download aggregated reports and results to their own personal workstation (OECD, 2019[7]).

4. Observations from the mapping exercise

Concerns related to the growing exchange of data across borders have led to a rising number of measures that condition the movement of data across borders. These vary significantly across countries and types of data, reflecting differences in preferences in relation to privacy and personal data protection and governments' pursuit of a range of other policy objectives. However, the resulting patchwork of regulations is creating uncertainties for governments, firms and individuals with respect to the applicable rules in a given situation. This is not only making it more difficult for firms to know what level of protection they must afford to customers located in different countries, but also increasing the costs of engaging in international trade. This is, in turn, undermining consumer and business "trust" and hampering economic growth and the opportunities for more inclusive trade from the digital economy.

In an effort to enable continued discussions in this area, the present exercise maps the existing instruments that countries use to enable the movement of data across borders with "trust". It categorises these across four broad areas: i) unilateral mechanisms; ii) plurilateral arrangements; iii) trade agreements; and iv) standards and technology-driven initiatives and maps the similarities within and across these different approaches. The exercise aims to contribute to discussions by focusing on identifying areas of similarity or convergence, rather than of difference. The observations gained should be seen as initial building blocks, and a modest but important first step in efforts to make iterative progress on an issue where there are significant international divisions.

The analysis shows that there is no one, single mechanism to enable the free flow of data with "trust". Governments pursue different, or even multiple and complementary, approaches. "Trust" might be achieved by empowering the private sector to provide different degrees of protection, making them liable for data misuse. "Trust" might also come through finding common ground or equivalence on regulatory

[49] *Pseudonomysation*, defined as the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, is also recognised by GDPR (Art. 4 (5)) as an appropriate measure to ensure the privacy of personal data, subject to certain conditions. However, since its inclusion in GDPR, research has shown that pseudonomysed data may be easily de-anonymised. Questions are therefore emerging on the efficacy of this type of measure to withstand progress in re-identification methods (OECD, 2020[3]).

approaches and enforcement mechanisms related to data protection when data cross borders. “Trusted” data flows might also be enabled by trade agreements that provide for unrestricted data flows in the context of data protection frameworks and which provide exceptions for meeting legitimate public policy objectives. Lastly, “trust” might also be generated through the use of technology that enables greater control on access and protection of data.

Despite wide differences across instruments, a range of *commonalities* emerge within and between instruments. For instance, whether through unilateral mechanisms, plurilateral arrangements or trade agreements, there tends to be consensus on the dual goals of safeguarding data and enabling its flow across borders, although differences arise in how these goals may best be achieved. Indeed, enabling protected cross-border data flows has been a key objective of many domestic privacy frameworks and has also been pursued in a range of international discussions from as early as the 1980s with the adoption of the OECD Privacy Guidelines. At the same time, all trade agreements that contain binding provisions on cross-border data flows include exceptions for legitimate public policy objectives and also have provisions on maintaining privacy or consumer protection frameworks. Similarly, many unilateral mechanisms include safeguards for transferring data and those safeguards also share commonalities. For example, many unilateral mechanisms recognise contracts or adequacy decisions as safeguard mechanisms (with differences related to how and by whom the safeguarding is done).

There is also growing evidence of *convergence* within and between instruments, often on the basis of the aforementioned commonalities. For instance, there are signs of growing overlaps in the principles that underscore privacy and personal data protection frameworks, including in the context of plurilateral arrangements. Trade agreements are also showing signs of convergence in increasingly including provisions on unrestricted data flows coupled with exceptions to achieve public policy objective and/or provisions on privacy and consumer protection frameworks.

Finally, there is a high degree of *complementarity* between instruments. Unilateral instruments draw from, and contribute to, plurilateral arrangements, and trade agreements are increasingly referencing plurilateral arrangements on data protection as part of their binding data flow provisions. Together, this indicates the emergence of a kind of international architecture, or a web of architectures, seeking to find ways to combine the benefits of data flows and achievement of legitimate public policy objectives.

The internet is global and borderless but regulations are not. Ensuring the free flow of data with “trust” has been a challenge for policy makers for many years. Different solutions to this complex challenge have emerged, albeit mostly in the context of domestic approaches. International cooperation on these issues, while difficult, can help reconcile differences. By focusing on areas where commonalities exist and highlighting complementarities and elements of convergence between existing approaches, this paper aims to support continued dialogue in this area to help identify where efforts might be most fruitful. It is hoped that this will facilitate international cooperation and dialogue on more predictable and transparent combinations of flows and “trust” that enable governments, firms and consumers to benefit from continued growth, wellbeing and inclusion.

References

Aaronson, S. (2019), "What Are We Talking about When We Talk about Digital Protectionism?", *World Trade Review*, Vol. 18/4, pp. 541-577, http://dx.doi.org/doi:10.1017/S1474745618000198. [11]

APEC (2019), *APEC CROSS-BORDER PRIVACY RULES SYSTEM: Policies, Rules and Guidelines*, http://cbprs.org/wp-content/uploads/2019/11/4.-CBPR-Policies-Rules-and-Guidelines-Revised-For-Posting-3-16-updated-1709-2019.pdf. [24]

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. [17]

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. [15]

Burri, M. and R. Polanco Lazo (2019), "Digital Trade Provisions in Preferential Trade Agreements: Introducing a New Dataset", *SSRN Electronic Journal*, http://dx.doi.org/10.2139/ssrn.3482470. [19]

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. [4]

Casalini, F., J. López González and E. Moïsé (2019), "Approaches to market openness in the digital age"*, OECD Trade Policy Papers*, No. 219, OECD Publishing, Paris, https://dx.doi.org/10.1787/818a7498-en. [6]

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

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. [16]

G20 (2020), *G20 Riyadh Learder's Declaration*, https://www.oecd.org/g20/g20-riyadh-summit.pdf. [1]

G20 (2020), "Ministerial Declaration", *G20 Digital Economy Ministers Meeting*, https://g20.org/en/media/Documents/G20SS_Declaration_G20%20Digital%20Economy%20Ministers%20Meeting_EN.pdf. [5]

ISO (2019), *ISO/IEC 27701:2019*, https://www.iso.org/standard/71670.html (accessed on 22 January 2021). [20]

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. [10]

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. [9]

Mitchell, A. and N. Mishra (2019), "Regulating Cross-Border Data Flows in a Data-Driven World: How WTO Law Can Contribute", *Journal of International Economic Law,*, Vol. 22(3). [25]

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. [12]

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. [8]

OECD (2020), "Mapping Approaches to data and data flows", *Report for the G20 Digital Economy Task Force*, http://www.oecd.org/trade/documents/mapping-approaches-to-data-and-data-flows.pdf. [3]

OECD (2019), "Digital Opportunities for Trade in the Agriculture and Food Sectors,", *OECD Publishing, Paris*, https://doi.org/10.1787/91c40e07-en. [18]

OECD (2019), *Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies*, OECD Publishing, Paris, https://dx.doi.org/10.1787/276aaca8-en. [7]

OECD (2017), *Digital risk and trust*, OECD Publishing, Paris, http://dx.doi.org/10.1787/9789264276284-9-en. [21]

OECD (2015), *Data-Driven Innovation: Big Data for Growth and Well-Being*, OECD Publishing, Paris, https://dx.doi.org/10.1787/9789264229358-en. [14]

OECD (forthcoming), "Digital Trade Inventory: Rules, standards and principles", *OECD Trade Policy Papers*. [23]

OECD MCM (2020), *2020 Ministerial Council Statement: A strong, resilient, inclusiv and sustainable recovery from COVID019*. [2]

The Royal Society (2019), *Protecting privacy in practice : the current use, development and limits of privacy enhancing technologies in data analysis.*, https://royalsociety.org/-/media/policy/projects/privacy-enhancing-technologies/privacy-enhancing-technologies-report.pdf. [22]

WEF (2020), "Data Free Flow with Trust (DFFT): Paths towards Free and Trusted Data Flows", *World Economic Forum White Paper*, http://www3.weforum.org/docs/WEF_Paths_Towards_Free_and_Trusted_Data%20_Flows_2020.pdf. [26]

Annex A. Supporting tables

Table A A.1. Examples of Plurilateral Arrangements

Non-binding plurilateral arrangements	
OECD Privacy Guidelines	**ASEAN PDP Framework**
Australia; **Austria; Belgium; Canada; Chile; Colombia; Czech Republic; Denmark; Estonia; Finland**; **France; Germany**; **Greece; Hungary; Iceland; Ireland; Israel; Italy**; **Japan**; **Korea; Latvia; Lithuania; Luxembourg**; **Mexico**; **Netherlands; New Zealand; Norway; Poland; Portugal; Slovak Republic; Slovenia; Spain; Sweden; Switzerland; Turkey**; the **United Kingdom**; the **United States**.	Brunei; Cambodia; Indonesia; Lao; Malaysia; Myanmar; Philippines; Singapore; Thailand; Viet Nam
APEC Privacy Framework	
Australia; Brunei Darussalam; **Canada**; Chile; China; Hong Kong, China; Indonesia; **Japan**; Malaysia; **Mexico**; **New Zealand**; Papua New Guinea; Peru; the Philippines; the Russian Federation; Singapore; **Korea**; Chinese Taipei; Thailand; Viet Nam; the **United States**	
Binding plurilateral arrangements	
Malabo Convention **African Union Convention on Cyber Security and Personal Data Protection**	**Convention 108** **(Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data)**
The African Union Convention on Cyber Security and Personal Data Protection has not entered into force yet, the following are the ratifying countries as of latest available data published 18/06/2020: Angola; Ghana; Guinea; Mozambique; Mauritius; Namibia; Rwanda; Senegal[1]	Albania; Andorra; Armenia; **Austria**; Azerbaijan; **Belgium**; Bosnia and Herzegovina; Bulgaria; Croatia; Cyprus; **Czech Republic; Denmark; Estonia**; **Finland**; **France**; Georgia; **Germany**; **Greece**; **Hungary**; **Iceland**; **Ireland**; **Italy**; **Latvia**; Liechtenstein; **Lithuania**; **Luxembourg**; North Macedonia; Malta; Monaco; Montenegro; **Norway**; **Netherlands**; **Poland; Portugal**; Republic of Moldova; the Russian Federation; **Slovak Republic;** Romania; San Marino; Serbia; **Spain**; **Slovenia**; **Sweden**; **Switzerland**; **Turkey**; Ukraine; the **United Kingdom**; Argentina; Cabo Verde; Morocco; Mauritius; **Mexico**; Senegal; Tunisia; Uruguay
APEC Cross-Border Privacy Rules (CBPR) System[2]	*2001 Additional Protocol to the Convention*
The **United States**; **Mexico**; **Japan**; **Canada**; Singapore; **Korea; Australia**; the Philippines; and Chinese Taipei. More countries are expected to join soon.	Albania; Andorra; Armenia; **Austria**; Bosnia and Herzegovina; Bulgaria; Croatia; Cyprus;[3] **Czech Republic**; **Denmark**; **Estonia**; **Finland**; **France**; Georgia; **Germany**; **Hungary; Ireland; Latvia**; Liechtenstein; **Lithuania**; **Luxembourg**; **Mexico**; North Macedonia; Monaco; Montenegro; Netherlands; Poland; **Portugal**; Republic of Moldova; the Russian Federation; **Slovak Republic**; Romania; Serbia; **Spain**; **Sweden**; **Switzerland**; **Turkey**; Ukraine; Argentina; Cabo Verde; Morocco; Mauritius; Senegal; Tunisia; Uruguay
	2018 Protocol amending the Convention
	Bulgaria; Croatia; Cyprus; **Estonia; Lithuania;** Malta; **Poland;** Serbia; Mauritius

Notes: OECD countries in bold. Data valid as of 02/11/2020.
1. According to the most recent accessible official document online.
2. Although the APEC CBPR System is not mandatory for APEC economies, it contains a binding element as companies that acquire the CBPR certification assume liability under the CBPR framework *vis-á-vis* participating economies.
3. Note by Turkey:
The information in this document with reference to "Cyprus" relates to the southern part of the Island. There is no single authority representing both Turkish and Greek Cypriot people on the Island. Turkey recognises the Turkish Republic of Northern Cyprus (TRNC). Until a lasting and equitable solution is found within the context of the United Nations, Turkey shall preserve its position concerning the "Cyprus issue".
Note by all the European Union Member States of the OECD and the European Union:
The Republic of Cyprus is recognised by all members of the United Nations with the exception of Turkey. The information in this document relates to the area under the effective control of the Government of the Republic of Cyprus.

Table A A.2. Trade agreements with data provisions

Agreement
CPTPP (Australia, Brunei, Canada, Chile, Japan, Malaysia, Mexico, New Zealand, Peru, Singapore, and Viet Nam)
USMCA (Canada, Mexico and the United States)
Korea-US FTA
Chinese Taipei - Nicaragua FTA
Canada - Peru FTA
Caribbean Forum - EC EPA
Cameroon - EC Interim EPA
Hong Kong, China - New Zealand FTA
Korea - Peru FTA
Central America – Mexico FTA
Colombia - Costa Rica FTA
Canada - Honduras FTA
Pacific Alliance Additional Protocol (PAAP)
Mexico - Panama FTA
Canada - Korea FTA
Japan - Mongolia FTA
Korea – Viet Nam FTA
Chile - Uruguay FTA
Australia – Singapore FTA
Argentina - Chile FTA
Singapore – Sri Lanka FTA
Australia - Peru FTA
EU - Mexico Modernised Global Agreement
Brazil - Chile FTA
EU - Japan EPA
Indonesia - Australia CEPA
Japan - US Digital Trade Agreement
Digital Economy Partnership Agreement between Chile, New Zealand and Singapore (DEPA)
TPP (Australia, Brunei, Canada, Chile, Japan, Malaysia, Mexico, New Zealand, Peru, Singapore, Viet Nam and US)

Source: Own calculations from the TAPED database.

Annex B. Methodology for the analysis of regulatory instruments

1. Capturing the frequency of approaches and instruments for transferring data across borders

The results discussed in Section 3.1 arise from an exercise designed to sketch a more granular picture of the tools and mechanisms that each country uses in its unilateral approaches to cross-border data transfers. The exercise involves a text-as-data method that enables the computation of a streamlined database describing the principles and regulations of each country's regulation to data flows, which can help identify commonalities and clusters of approaches. The results are based on the survey of 76 economies.[50]

Designing a template of approaches and instruments for transferring data across borders

To generate a comparable representation of approaches to cross-border data flows, a template is created. It includes a list of economies (columns), each composed of a list of different possible tools for transfer (rows). Each cell is filled with binary yes or no values, 1 or 0, marking whether a given cross-border transfer tool is cited by the regulation under consideration or not. Sixteen types of elements relating to the regulation of cross-border transfers of data are tracked, providing a stylized representation of each regulation's approach to data flows that can be summarised as a combination of 15 values that are either 1 or 0.

A few additional clarifications with regard to the way the template is filled are in order. First, regulations may have slightly different definitions of what constitutes an international transfer. Variations arise from whether data is in the public domain already or whether data is in transit but not disclosed abroad. These specifications are not considered in this exercise. Similarly, for regulations that foresee different rules depending on whether the international transfer happens as a controller-to-controller, or as controller-to-processor (that is, as a service outsourcing) transfer, different rules are coded together in a same column. When the regulatory framework of a country for a same type of data is composed of more than one piece of legislation, these different rules are also coded together, as a same economy-column.

In addition, to correctly interpret what information is tracked by this template, it is important to clarify that almost all personal data protection regulations establish rules for *domestic* transfers of data (i.e. for transfers of data between two entities in the same country). However, in this coding, only rules or elements that are an *additional* requirement for transfers of a cross-border nature are considered. For example, many countries, including countries that abide by the accountability principle, require that any two entities exchanging data for processing purposes stipulate a contract to protect the personal privacy of the individuals involved. This rule, however, would not correspond to a 1, or yes, for the variable 'legal instrument' in this template, as that is a rule that constitutes an integral part of the level of protection afforded by the country's regulation, irrespective of geographical location, and hence is unlikely to have specific interest or relevance to international trade.

As shown in Figure A B.1, the template tracks 15 elements that can help to define the approach of countries to cross-border data transfers. This means that any element encountered even just once is taken into consideration. For regulations that cite instruments such as contracts, corporate codes of conduct, or certification schemes, the template differentiates between cases where the clauses of these instruments are standardised or must be approved by a public authority, and where this is left to the discretion of the transferring entity.

[50] EU GDPR is applicable across a number of EEA member countries.

Figure A B.1. Representation of template for Data Transfer Tools

	Country A	Country B
Data protection rights without *ex ante* rule	0	0
Accountability rule	0	0
Private adequacy	0	0
Public adequacy	1	1
Standard contracts	0	0
Approved legal instrument	0	0
BCRs	0	0
Approved code of conduct	0	0
Certification scheme	0	0
International agreement	1	1
Transmission of privacy notice	0	0
Safeguards provided	0	0
Consent	0	0
Necessity / public interest / contract	1	1
Ad hoc authorisation	1	1

Source: Authors' calculation sheet.

Specific definitions or procedural requirements of each element are not, at present, evaluated when filling in the template. For example, the different conditions for consent to be valid, or the different definitions of what constitutes a same corporation for the purpose of corporate rules, or again the difference in the processes for obtaining approval of contractual clauses or codes of conduct, where this is required, are not the object of differentiation and are not captured by this exercise. This does not mean that these variations may not also have significance for trade, but the goal of the exercise at this stage is that of developing a tool for mapping instruments for cross-border transfers, and hence some proxy is unavoidable.

In addition, the approach taken to filling in the template is as formal as possible. In particular, an issue can arise as different regulations take a more or less broad approach in defining the rules for transfers, some indicating principles and some others detailing much more specific requirements, with variations in between. The challenge is that where broad formulas are used, tools that other regulations specifically cite, could be implied. In these cases, to limit the arbitrariness of the exercise, 1 and 0 values are assigned reflecting the level of specificity that is *explicitly* recognised in the text of the regulation – that is, the coding is only as specific as the text of the regulation is. Hence, where, for example, "legal instruments" or "adequate legal measures" are envisioned, the coding does not assign a 1 (yes) value to instruments such as codes of conduct or binding certification mechanisms, although these could be implied.

The countries or economies considered so far are: Algeria, Albania, Angola, Andorra, Argentina, Australia, Botswana, Brazil, Canada, Cape Verde, Chile, China, Colombia, Cote d'Ivoire, Ethiopia, European Economic Area (Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and United Kingdom + Iceland, Liechtenstein, Norway), Faroe Islands, Ghana, Hong Kong China, India, Indonesia, Israel, Jamaica, Japan, Kazakhstan, Kenya, Korea, Malaysia, Morocco, Mexico, Namibia, New Zealand, Nigeria, Panama, Peru, Philippines, Russia, Serbia, Singapore, South Africa, Switzerland, Taiwan, Tajikistan, Turkey, United States, Uruguay.

Analysing the results

For drawing insights from the exercise, the analysis in this preliminary draft has focused on measuring the *frequency* of certain unilateral approaches to enabling the cross-border transfer of data across different domestic regulations. In particular, the analysis does not focus on the combination of different elements within a regulation, such as to describe its overall approach to data transfers, but only looks at whether specific instruments are formally cited within it.

2. Comparing privacy and personal data protection regulations

The results provided in section 3.2 arise from an exercise designed to support the comparison of different regulatory instruments – in this case, of privacy and data protection frameworks across different countries. The aim is that of generating quantitative metrics to facilitate the visualisation of information, highlighting relative distance between dyads of regulations. Looking at the overlapping dyads informs about the extent to which countries might already be implementing common approaches to their domestic privacy and data protection regulation. It has the advantage of not relying on subjective evaluations of what a good or a bad regulation looks like since all regulations are evaluated against each other with respect to their distance.

At this stage, the results are based on the survey of 26 privacy and data protection frameworks which capture 56 economies,[51] with this (preliminary) sample chosen to include some of the world's biggest economies. For federal countries, where no federal regulation exists, the regulation of one state was chosen.

Designing a template for privacy and data protection regulation

To create a comparable representation of each country's privacy or data protection frameworks a template is created. It includes a list of economies (columns), and of different characteristics, principles or rights, that each framework may feature (rows). Each cell is filled with binary yes or no values, 1 or 0, marking whether a given privacy or data protection element is cited by the regulation under consideration or not. 25 variables that may help to outline a privacy or data protection framework are tracked. This enables the compilation of a streamlined database that describes the approach of each different country as a combination of 16 values that are 1 or 0.

As shown in Figure A B.2, the chosen set of variables attempts to capture the key features, processing principles, and individual rights that each regulation may contain. It tries to account for the variety of elements that are encountered in privacy and data protection regulation. Nevertheless, this exercise inevitably provides only a stylized representation of the sampled privacy and data protection frameworks.

In particular, it may be worth clarifying that some principles and rights that are in practice the same might be called differently in different economies. These have been grouped under a single variable. Similarly, a same principle or right will often be differently defined or differently applied in different regulations. The jurisprudence, or case law, and other secondary sources that exist in relation to each privacy or data protection framework can also further accentuate the nuances that a same principle or right assumes in different jurisdictions. However, a formal approach is taken in filling in this template, and there is no attempt to evaluate the scope and broadness of each principle or right in different regulations. Generally, and to the extent possible, the coding takes into consideration the appearance or non-appearance in the text, and in material referenced within that, of the keywords of the label of the element in question, or a close synonym.

Similarly, procedural elements of the regulations are not captured by this exercise, such as whether an entity must be registered in a given country to process data, or the type of sanctions and enforcement methods foreseen, or what are the rules, if any, for domestic transfers of data.

[51] EU GDPR is applicable across a range of EEA member countries.

Figure A B.2. Representation of template for privacy and data protection regulation

	Country A	Country B
Notification/consent in data collection	1	1
Purpose specification/transparency	1	1
Collection limitation/proportionality	1	1
Use limitation	1	1
Data retention limitation	1	1
Security and confidentiality	1	1
Data quality/accuracy	1	1
Sensitive data additional measures	1	1
DPO requirement	0	0
Breach notification	0	1
Automated decision (right of review/info)	1	0
Right of access	1	1
Right of objection (processing/marketing)	1	1
Right of deletion ("right to be forgotten")	1	1
Right to rectification	1	1
Right to data portability	0	0

Source: Authors' calculation sheet.

Analysing the results

For drawing insights from this exercise, a first step involves the calculation of the frequency of the different privacy and data protection variables across all sampled regulations. This makes it possible to visualise the characteristics, principles and rights that are more commonly, or even universally, recognised. At the same time, it makes it possible to identify what the elements on which there is lesser agreement are. The results of this analysis are shown in Figure 8 in the main text.

Another type of analysis focuses on computing indicators of the level of overlap between dyads of regulations, which can help to provide a portrait of the broad overlaps across this policy area. In particular, this approach makes it possible to look at the *relative* similarity of regulations, without prejudice, nor intent to identify, a given combination of privacy and data protection elements as a benchmark or standard.

The results presented in Figure 9 in the text are obtained as follows. For each dyad, the percentage of elements for which both countries have a 1 (i.e. they enshrine that element) is computed across the list of 16 variables – the higher the resulting percentage value, the higher the similarity between the two regulations. This gives a matrix of relative overlaps across regulations. For each regulation, the overlaps with all other regulations can then be averaged yielding an average convergence indicator for the specific regulation. This can be used to identify the extent to which a privacy or data protections regulation has positive overlaps with others.

OECD TRADE POLICY PAPERS

This report was declassified by the OECD Working Party of the Trade Committee in March 2021 and was prepared for publication by the OECD Secretariat.

This report, as well as any data and any map included herein, are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

The statistical data for Israel are supplied by and under the responsibility of the relevant Israeli authorities. The use of such data by the OECD is without prejudice to the status of the Golan Heights, East Jerusalem and Israeli settlements in the West Bank under the terms of international law.

Comments are welcome and can be sent to tad.contact@oecd.org.