OECD publishing

FOSTERING CROSS-BORDER DATA FLOWS WITH TRUST

OECD DIGITAL ECONOMY PAPERS

December 2022 **No. 343**

OECD
BETTER POLICIES FOR BETTER LIVES

This report was approved and declassified by the Committee on Digital Economy Policy on 27 September 2022 and prepared for publication by the OECD Secretariat.

This publication is a contribution to Phase III of the OECD Going Digital project, which aims to provide policy makers with the tools they need to design and implement better data policies to promote growth and well-being.

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

#GoingDigital

Note to Delegations:

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

DSTI/CDEP/2022/7/FINAL

Foreword

This report summarises how different countries and other stakeholders are pursuing cross-border data flows with trust through direct and indirect approaches, across different levels, fora and policy communities. It highlights commonalities, complementarities and elements of convergence in these approaches pursuing what is often referred to as “data free flow with trust”, and underscores emerging challenges. The report aims to support policymakers as they seek pathways to advance this important policy agenda.

This report was drafted by Francesca Casalini, Javier López González and Audrey Plonk with contributions from Gallia Daor, Marianna Karttunen and Miguel Amaral. This publication is a contribution to IOR 1.3.1.2.3 of the 2021-2022 Programme of Work and Budget (PWB) of the Committee on Digital Economy Policy and to item 3.1.1.2.2 Data and data flows of the PWB of the Trade Committee. The authors are grateful for comments received: by other co-leads of the Horizontal Project; at the various inter-directorate meetings; and to the Committee on Digital Economy Policy and the Working Party of the Trade Committee.

Table of contents

FIGURES

Executive summary

What is the issue and why is it important?

Cross-border data flows are critical for global economic and social activities, underpinning daily business operations, logistics, supply chains and global communication. However, cross-border data flows also pose challenges between and among governments, businesses and individuals, as they amplify concerns about privacy and data protection, intellectual property protection, digital security, national security, regulatory reach, trade, competition and industrial policy.

Addressing these concerns by establishing trust is necessary to support globally connected economies. Countries thus share a common challenge of promoting a global and interoperable digital environment where data can move across borders with trust – a concept also known as "data free flow with trust" (DFFT).

What did we learn?

International discussions on DFFT are challenging because countries maintain different policy and regulatory approaches in relation to data and cross-border data flows. However, beyond these differences, countries can build on commonalities, complementarities and elements of convergence in their approaches to governing cross-border data flows to build trust and advance policy dialogue:

- There are commonalities between different instruments used to enable data to flow across borders with trust. First and foremost, the dual objective of enabling cross-border data flows while upholding trust commonly underpins domestic regulations, intergovernmental arrangements and trade agreements. There are also commonalities within instruments. For example, most unilateral mechanisms rely on combinations of adequacy determinations, individual consent, certifications and contractual arrangements.
- There is evidence of convergence towards common principles on privacy and personal data protection including those found in the OECD Privacy Guidelines, as well as towards common language and binding commitments in the context of trade agreements.
- There are important complementarities between existing instruments. Unilateral mechanisms are being increasingly discussed in international arrangements and trade agreements; and unilateral mechanisms and trade agreements increasingly refer to international arrangements.

Privacy interoperability was introduced in the 2013 Revision of the OECD Privacy Guidelines. According to OECD work, privacy interoperability can be understood operationally as the ability of different privacy and data protection regimes, or legal frameworks, to work together at multiple levels through policy and practical arrangements and thereby bridge different approaches and systems of privacy and personal data protection across countries to facilitate cross-border flows of personal data.

An emerging challenge to data flows concerns the practices applied by law enforcement and national security agencies when accessing personal data held by the private sector. While countries apply safeguards to such access as part of their legal framework, there is a notable gap in international norms around these safeguards. The OECD is working to identify commonalities in approaches to enhance trust among like-minded countries and facilitate data flows between them.

Similarly, data localisation measures are increasingly being considered as a means to address policy concerns around cross-border data flows. Better evidence about the scope and practical implications of such policies is critical to promote a shared understanding and build trust.

Through its evidence-based policy analysis, the OECD can support multi-stakeholder dialogue on different policy options for governing cross-border data flows and help countries to harness their commonalities to facilitate cross-border data flows with trust.

1 Introduction

Today's globally interconnected world is underpinned by the transfer and exchange of data across borders. While this creates new opportunities for economic and social interactions, it also amplifies concerns about privacy and data protection, digital security, national security, regulatory reach, trade, competition and industrial policy. At the heart of this tension is the notion of trust.

1.1. Cross-border data flows with trust

Today's digitalised and globally interconnected world is underpinned by the movement of data across borders. Data flows enable international social interactions; they support research to address global challenges; they help co-ordinate production along global value chains; and they allow firms, notably smaller ones, to access global markets. In sum, cross-border data flows are the lifeblood of modern day social and economic interactions.

However, the increasingly pervasive transfer and exchange of data across borders, while creating a range of new opportunities, also amplify concerns about privacy and data protection, digital security, national security, regulatory reach, trade, competition and industrial policy. The Internet was conceived as global and borderless, but most regulations are not. The challenge is twofold. First, to promote regulatory and policy approaches that enable the movement of data while ensuring the desired oversight and/or protection for data when they cross a border. Second, to ensure that these regulatory approaches can work together across borders (Robinson, Kizawa and Ronchi, 2021[1]; OECD, 2021[2]; Casalini, López González and Moïsé, 2019[3]).

At the centre of this discussion is the notion of "trust." The benefits of digitalisation depend strongly on the degree of trust in the digital environment that underpins economic and social interactions. As individuals and societies become increasingly impacted by how data are shared, transferred and used, trust grows in

importance. For example, businesses' ability to reap the benefits of scale may be hindered unless they can operate with trust globally. The notion of trust also plays a role in the way governments and individuals interact with other governments, enabling regulatory co-operation.

Different countries, individuals and businesses may have a different understanding of what "trust" means. The growing acceptance of "data free flow with trust" (DFFT) encapsulates the international policy impetus to find a solution to this challenge. Japan championed DFFT at the 2019 World Economic Forum Annual Meeting in Davos. Subsequently, leaders at the G20 Osaka Summit of 2019 also endorsed the concept.

Against this backdrop, the report explores different facets of this evolving environment. Section 2discusses the importance of cross-border data flows for economic and societal objectives, highlighting the perspectives of individuals and businesses. Section 3 provides an overview of the rationales for regulating cross-border data flows and outlines the challenges created by this evolving and increasingly complex policy and regulatory landscape. Section 4 maps and identifies commonalities in emerging approaches to governing cross-border data flows, showing how countries promote the dual goal of enabling transfers while ensuring that data receive the desired oversight and/or protection. Section 5 focuses on two critical issues on which further international dialogue is needed to promote and maintain trust in cross-border data flows: government access to personal data held by the private sector and data localisation requirements. Section 6, the last section, provides preliminary policy observations, arguing that countries should harness existing commonalities to promote further dialogue on cross-border data flows with trust.

To support dialogue in this area, this synthesis report unpacks some of the underlying issues at stake in this debate, drawing on previously published OECD work. Given differences of views on some of the issues covered, the report describes the regulatory environment and does not call into question the prerogative of governments to establish the mix of instruments or mechanisms that best serve their policy interests and objectives.

2 Data free flows with trust are critical for individuals and businesses

Cross-border data flows enable new opportunities and raise new challenges for both individuals and businesses. For individuals, cross-border data flows fuel new and improved social and economic interactions. However, concerns arise about how data are used once they cross a border and the risks associated with misuse. Cross-border data flows also enable critical business activities like the coordination of production along global value chains and participation in digital trade. However, business are also expected to meet customers' expectations of data protection, privacy and security.

2.1. The perspective of individuals

Cross-border data flows are key to enable social interactions and allow individuals to benefit from improved access to goods and services from global suppliers. People benefit from sharing personal information across borders, connecting with friends using social networks or accessing a myriad of innovative digital solutions for entertainment, scheduling or navigation. They also enjoy opportunities for remote work.

However, the data trail left by individuals in today's economic and social interactions is richer than ever before. In the past, for example, information collected by firms for a DVD rental would be limited to the name and address of the user, the titles, and dates of collection and returns of rented films. Now, with digital streaming services, firms can also collect data on the time a particular movie was watched. In addition, they can track whether the film was finished or not, if it was watched multiple times and when it was paused. Through ratings, they can also assess the extent to which it was enjoyed by the viewer.

Such data, which often cross a number of international borders, are processed to compile user profiles that can help generate more targeted recommendations, improving service delivery. At the same time, this data trail, including the amount of data collected and processed and how they will be subsequently used, is often not clear to the individual. While individuals are increasingly engaged and savvy, the type and amounts of data they generate are often difficult to understand. Additional concerns about privacy and data protection arise when the data gathered are directly monetised. Data could be sold, for example, to other firms who may make use of it for marketing or other purposes (e.g., data brokers).

Privacy and data protection are difficult to define and mean different things to different people (Solove, 2006[4]). The value individuals or societies attach to privacy and data protection can be subjective (Acquisti, Taylor and Wagman, 2016[5]), reflecting different cultural and social traditions and norms.[1] Regulation can also differ within countries whose regions or states have regulatory autonomy on related matters. This raises important challenges for privacy and data protection, especially when personal data cross borders. Individuals may have expectations that when their personal data are transferred to different countries, they enjoy similar safeguards as domestically. Individuals may also have access to remedy or redress mechanisms in a domestic context that might not be accessible or even exist in another country. Given these challenges, it is important to promote an environment where individuals can understand and trust how their data are safeguarded at home and all the more so abroad.

2.2. The perspective of business

Today, firms across all sectors rely on data and cross-border data flows – both personal and non-personal data – to support their business activities (National Board of Trade Sweden, 2015[6]; National Board of Trade Sweden, 2014[7]). For instance, in manufacturing, data help co-ordinate research and design outputs; exercise overarching control and co-ordination of geographically dispersed processes of production; and track and trace products as they travel to the border and beyond (Casalini and López González, 2019[8]). In agriculture, data are supporting a move towards precision agriculture techniques. These rely on data analytics to optimise resources and enable savings on seed, fertiliser and irrigation, as well as allowing for new traceability and connections to markets (Jouanjean, 2019[9]).

Firms rely on data and their flow across borders at all stages of the supply chain – from design and production to delivery and use (Figure 2.1).

At the design stage, research and development for manufacturing activities increasingly involve co-ordinating individual researchers, scientists, designers and IT specialists working in different countries and sharing ideas, information, prototypes and test data.

At the production stage, exercising overarching control and co-ordination of geographically dispersed processes of production also involves transferring data across different locations. This includes organising input flows of goods and services, working with subcontractors and suppliers, and handling internal operations. This work, in turn, may require sending data about inventories, sales, demand forecasts, order status, human resources and production schedules. As manufacturing becomes increasingly mechanised, data transfers may be needed to instruct robotics. Sensors on the factory floor send real-time data that can be transferred abroad to be analysed and used to adjust production activities or equipment maintenance. Increasingly, this in-plant production can also require the transfer of personal data of employees working alongside robots (“cobot”).[2]

At the delivery stage, data transfers are needed to track and trace products as they travel to the border, across the border and beyond: data flows underpin modern trade facilitation practices (López González and Jouanjean, 2017[10]).

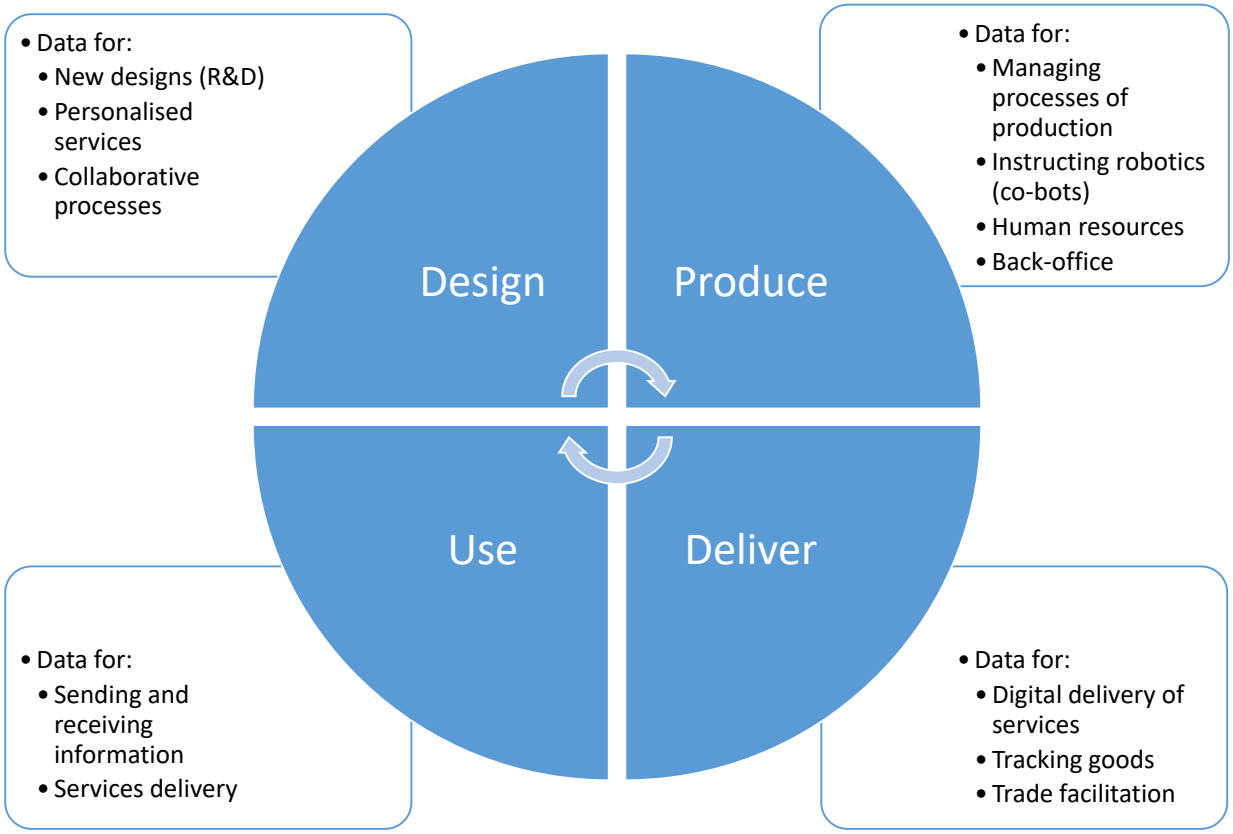
At the use stage, if the product being traded is a “smart” good, the delivery of services and information – the elements that make the product “smart” – will depend on the ability to collect and transfer different

types of data. When the product gets to the consumer, the experience of the consumer might then depend on the ability of the firm to receive, process and respond to continuous feedback. Increasingly, firms also offer after-sale services. To that end, they need to monitor performance of products in view of handling maintenance, repairs and spare parts, a process often connected through cross-border data flows.

All these elements require constant digital connectivity supporting a "digital thread" (Figure 2.1). Businesses have an interest in ensuring that cross-border data flows supporting this digital thread take place in the context of "trust." They want to ensure they are meeting expectations from individuals to safeguard their privacy and protect their data. At the same time, they want to ensure their data are secure and their intellectual property is properly safeguarded.

However, businesses relying on cross-border data flows will also be concerned about measures that condition access to and use of data along the digital thread. In particular, they want to know how these measures might affect the efficacy of individual stages, as well as the viability of the value chain as a whole (Casalini and López González, 2019[8]). These concerns will only amplify given wider adoption and use of new technologies such as the Internet of Things or artificial intelligence for which reliance on cross-border data flows in production processes across both goods and services is expected to increase.

Figure 2.1. Data are pervasive across modern value chains



Source: Casalini and López González (2019[8]), "Trade and Cross-Border Data Flows", *OECD Trade Policy Papers*, No. 220, OECD Publishing, Paris, https://doi.org/10.1787/b2023a47-en.

3 Why countries are updating and adopting cross-border data flow regulation

Governments have been updating and adopting regulation that affects cross-border data flows. There are six areas of particular concern to government when it comes to cross-border data flows: privacy and data protection, intellectual property rights, regulatory control or audit purposes, national security, digital security and digital industrial policy.

3.1 Regulating cross-border data flow

Promoting the flow of data across borders is a recognised policy objective for many governments. Data are clearly linked to economic considerations and can be used to tackle some of the most pressing societal challenges. As such, data can benefit both individuals and businesses. Individuals, for example, can enjoy better and greater access to information, goods and services, while businesses can use data to access markets and co-ordinate global value chains. Cross-border data flows can also promote better research outcomes in areas such as health, environment or law enforcement. For instance, sharing of health data across international borders can enable targeted research as seen during the COVID-19 pandemic. Sharing of data in the context of environmental research or to fight crime and detect money laundering can also help find better outcomes for societies and individuals.

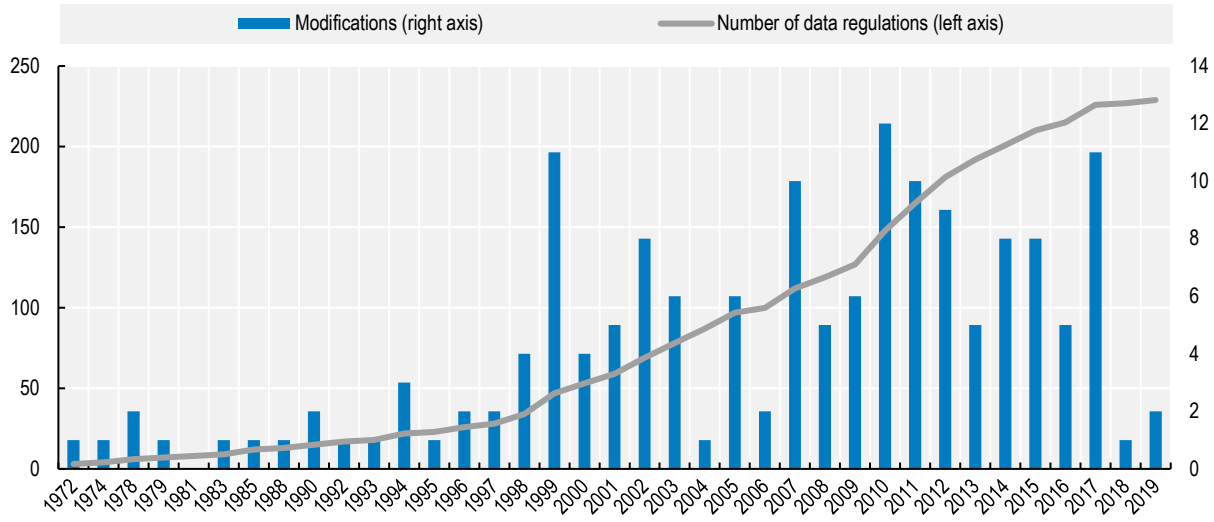
However, cross-border data flows also entail risks and challenges with respect to a range of public policy objectives. As illustrated in the previous section, the growing and pervasive use and flow of data, including across borders, has fuelled concerns about the use and especially the misuse of data, including in the context of power relations among firms, between firms and consumers, and between governments and citizens, especially with respect to privacy and personal data protection.

These concerns are compounded when data move beyond the reach of domestic regulatory bodies. They may also be subject to different rules and regulations depending on where they are located and the type of information they contain. Indeed, while data and digital activity are inherently borderless, regulations are not. Consequently, ensuring privacy and digital security, protecting intellectual property rights, enabling economic development and maintaining the reach and oversight of regulatory and audit bodies can become more complex when data crosses jurisdictions (OECD, 2021[11]).

Moreover, different types of data (e.g., personal, public, proprietary, financial) are subject to different and often overlapping data governance frameworks. These include, for example, privacy and data protection and intellectual property rights (OECD, 2022[12]). Understanding which data are subject to what data governance framework in the context of domestic transactions is complex. This issue is amplified when data move to foreign countries where definitions, policy domains and data governance frameworks can differ.

In light of emerging challenges, governments have been updating and adopting regulation that affects cross-border data flows. This has resulted in a growing number of countries placing conditions on the transfer of data across borders or requiring that data be stored locally (Figure 3.1).

Figure 3.1. Growing number of regulations affecting cross-border data flows



Note: Regulations include different types 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, conditions on cross-border data flows for different types of data, and local storage requirements.
Source: Casalini and López González (2019[8]), "Trade and Cross-Border Data Flows", *OECD Trade Policy Papers*, No. 220, https://doi.org/10.1787/b2023a47-en.

The reasons why countries are reviewing their cross-border data policies fall into six broad categories. Much of the debate about data flows revolves around the movement of personal data, raising concerns about **privacy and data protection**. For some, the challenge is to ensure that data protections follow the person i.e. when data are transferred outside a specific jurisdiction, they continue to receive equivalent oversight/protection as in the jurisdiction where the person resides. However, views and practices to ensure privacy and personal data protection vary significantly across cultures and countries.

When data cross borders, governments also worry that protection of **intellectual property rights** may be undermined, including trademark, copyrights and trade secrets.

Some measures that condition data flows aim to secure access to data deemed necessary for **regulatory control or audits** (i.e. law enforcement). This concerns ensuring that data be readily accessible to regulators and typically involves data such as personal data, telecommunication data, and banking data.

Measures related to **national security** often mandate that data be stored and processed locally. This aims to protect information deemed to be sensitive or to enable national security services to access and review data.[3]

Governments also promote local storage and processing with a view to ensuring **digital security**. The rationale for such policies is that in a domestic setting, specific rules and protections can be mandated.

Finally, conditioning the flow of data or mandating local storage can be motivated by the desire to use a pool of data to encourage or help develop domestic capacity. This serves as a kind of **digital industrial policy,** including in the context of economic development. Indeed, it can reflect a view that the domestic economy should be the primary beneficiary of this valuable asset. These approaches can be sector-specific or apply to a range of data types.

While there are legitimate reasons for diversity in regulation, the regulatory landscape that underpins cross-border data flows and local storage requirements is becoming increasingly complex. The emerging patchwork of approaches risks undermining the policy objectives they were intended to serve in the first place. Evolving, overlapping or sometimes conflicting requirements for entities involved in data processing can create operational uncertainty about which rules to apply to which data. This, in turn, can generate legal uncertainty and administrative burden and costs. Individuals may also find it difficult to trust a regulatory environment they do not understand. Lack of trust can emerge due to unclear or insufficient information or because of the ineffectiveness of protection overseas, including for obtaining redress in case of non-compliance. Similarly, a firm must understand levels of data protection required for customers in different jurisdictions to engage in trade. Effective government enforcement action can also be hindered by complexity and a lack of co-ordination on these inherently transboundary issues.

4 How countries pursue data free flows with trust

Government policy can enable trusted data flows in diverse ways including regulatory approaches such as unilateral mechanisms, intergovernmental arrangements, and trade and digital economy agreements. A range of complementary initiatives that involve informal dialogue among different stakeholders and highlight technological and organisational tools also support building trust.

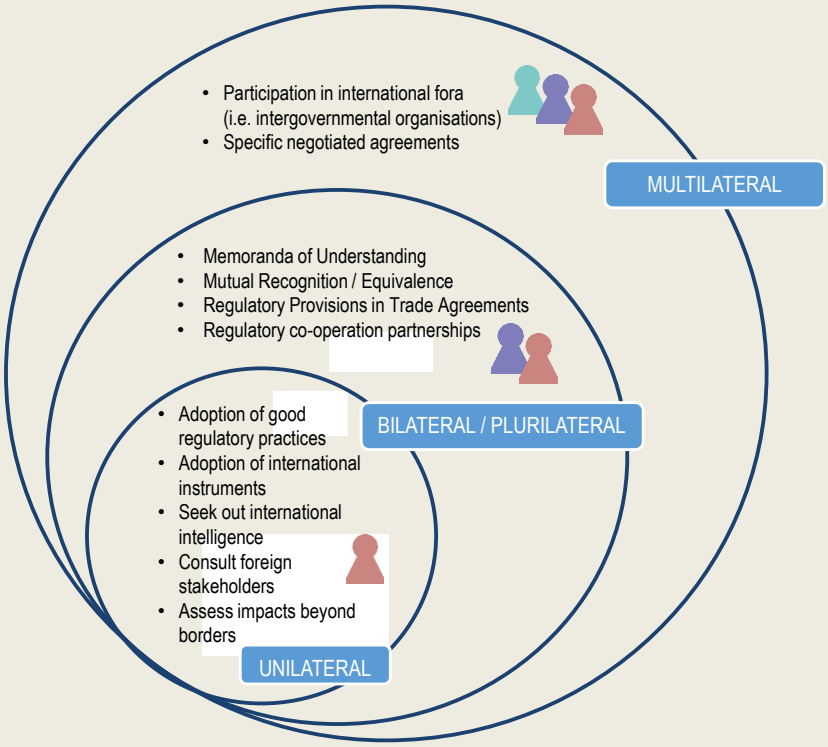
4.1. Data flows with trust in practice

Governments have a variety of ways to reinforce trust through their regulatory frameworks. These range from introducing international considerations unilaterally within domestic rulemaking to diverse and complementary forms of bilateral, regional and multilateral co-operation (Box 4.1). Within this spectrum, specific mechanisms are useful for certain policy issues.

Box 4.1. Fostering regulatory coherence across borders: Lessons from international regulatory co-operation

OECD work shows the multiplicity of international regulatory co-operation (IRC) approaches. They may cover activities from the exchange of information to the harmonisation of rules. They may focus on the stage preceding the development of rules – such as evidence gathering – or apply to the regulatory delivery side (in enforcement/inspection, for example). They may involve specific institutional arrangements or rely on peer-to-peer agreements. In practice, they take the form of complementary mechanisms ranging from unilateral to international multilateral action (Figure 4.1).

Figure 4.1. The multiplicity of international regulatory co operation approaches



The OECD Recommendation on Agile Regulatory Governance for Harnessing Innovation recommends that governments consider "the international innovation ecosystem to draw on the most relevant evidence and regulatory approaches", and also strengthen "regulatory co-operation across policy-making departments and regulatory agencies, as well as between national and subnational levels of government." The OECD Best Practice Principles on IRC complements this Recommendation. It offers key principles to help governments lay the institutional foundations for co-operation and joined-up approaches, while also applying a whole of government approach to IRC.

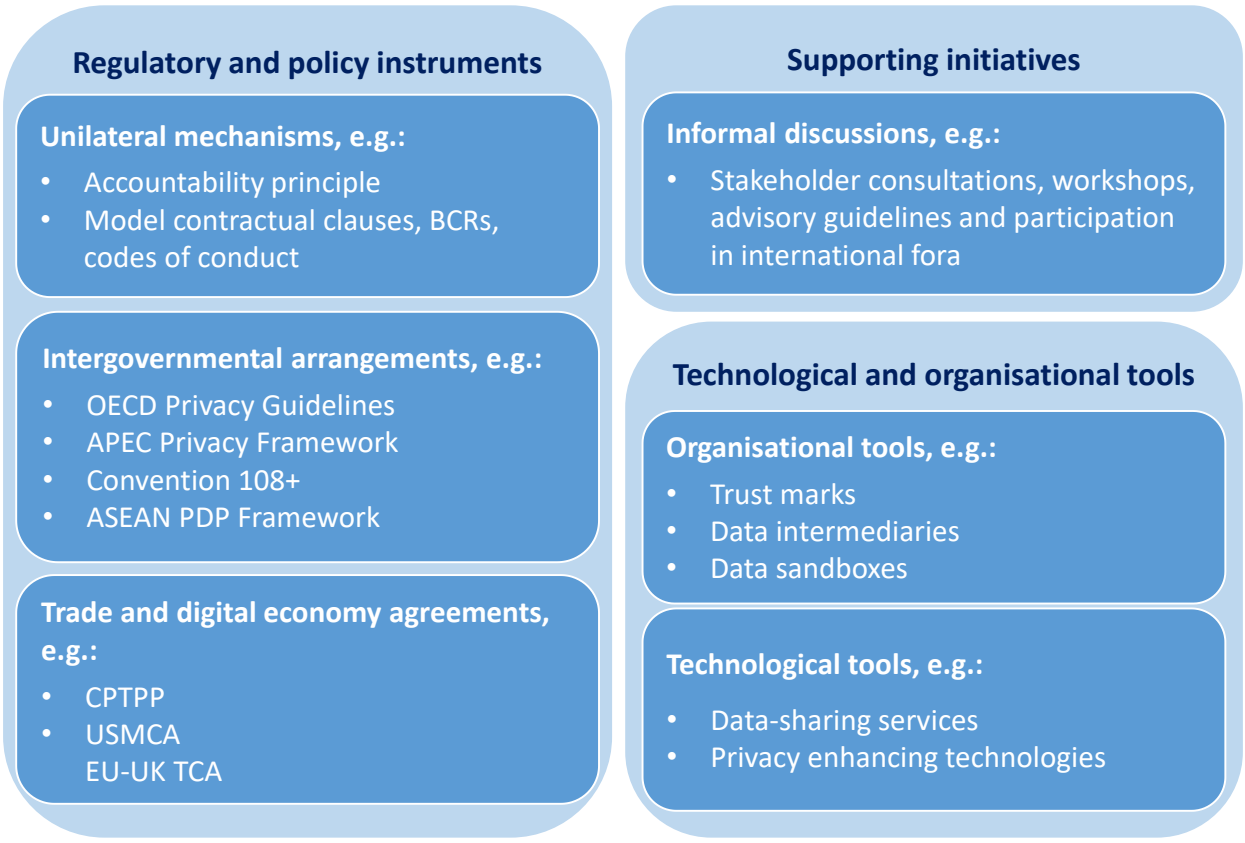
Source: Recommendation of the Council for Agile Regulatory Governance to Harness Innovation (OECD/LEGAL/0464) https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0464; OECD (2021[2]), *International Regulatory Co-operation*, OECD Best Practice Principles for Regulatory Policy, https://doi.org/10.1787/5b28b589-en.

In the case of cross-border data flows, governments, data protection authorities, and other stakeholders increasingly use a range of approaches. These enable entities to transfer data across borders while ensuring that, upon crossing a border, data are granted the desired oversight and/or protection

(Figure 4.2). First, different "regulatory and policy instruments" enable data flows with trust (often in the context of personal data). These are complemented by "supporting initiatives" that involve informal dialogue with different stakeholders. Alongside these efforts, the private sector is also increasingly active in promoting "technological and organisational tools" to facilitate data free flows with trust, sometimes with the support of the public sector. [4]

Each approach tackles the issue of cross-border data flows from a different perspective, and approaches are not mutually exclusive: countries simultaneously and synergistically leverage different approaches for different purposes, partners, types of data and situations. Mapping *commonalities* across approaches can help governments in their ongoing efforts to identify combinations of data free flows and trust that can foster future interoperability.

Figure 4.2. Approaches to facilitate cross-border data flows with trust



Note: BCRs = Binding corporate rules; APEC = Asia-Pacific Economic Cooperation; ASEAN PDP = Association of Southeast Asian Nations Personal Data Protection; CTPP = Comprehensive and Progressive Agreement for Trans-Pacific Partnership; USMCA = United States-Mexico-Canada Agreement; EU-UK TCA = European Union – United Kingdom Trade and Cooperation Agreement.
Source: Based on Casalini, López González and Nemoto (2021[13]), "Mapping commonalities in regulatory approaches to cross-border data transfers", *OECD Trade Policy Papers*, No. 248, https://doi.org/10.1787/ca9f974e-en and Robinson, Kizawa and Ronchi (2021[1]) "Interoperability of privacy and data protection frameworks", *OECD Going Digital Toolkit Notes*, No. 21, https://doi.org/10.1787/64923d53-en.

4.2. Regulatory and policy instruments

Three types of regulatory and policy instruments directly govern cross-border data flows with a view to fostering trust: unilateral mechanisms; intergovernmental arrangements; and trade and digital economy agreements.

4.2.1. Unilateral mechanisms

Unilateral mechanisms enable transfer of certain types of data to countries across borders under certain conditions. These domestic mechanisms are largely developed in the context of transfers of personal data. They include use of "open safeguards" such as ex-post accountability principles, contracts and private sector adequacy, as well as "pre-authorised safeguards" such as public adequacy decisions, standard or pre-approved contractual clauses and binding corporate rules. Pre-authorised safeguards generally require some form of public sector approval before the data transfer. For their part, open safeguards leave more discretion to entities as to how to safeguard the data being transferred, making entities accountable for any misuse.

Analysis across OECD countries and selected economies (76 economies in total) shows that most countries envision data transfer mechanisms to provide some form of safeguard. However, they differ in implementation, with more or less involvement by the public sector. Pre-authorised safeguards feature in 65% of surveyed economies and open safeguards in 54%. This changes to 79% and 33%, respectively, when countries subject to the General Data Protection Regulation (GDPR) are counted individually (Casalini, López González and Nemoto, 2021[13]).

Notwithstanding the differences between the two categories, some commonalities emerge. Both types of safeguards include approaches that rely on some form of adequacy decision or use of contracts. Nearly half (48%) of economies using open safeguards rely on the notion of adequacy or contracts. Meanwhile, 77% of economies using pre-authorised safeguards rely on adequacy decisions and 37% recognise contracts.

The key difference relates to who designs and evaluates conformity. In the case of open safeguards, the transferring entity assesses adequacy, provided they meet objectives set by the government. In the case of pre-authorised safeguards, governments make the adequacy determination. For open safeguards, the firm decides what provisions the contracts or corporate rules will include. Conversely, in the case of pre-authorised safeguards, the government drafts the model contracts that must be used by firms or approves corporate rules after review.

The number of countries developing model contractual clauses is growing. These ready-made clauses provide protection when data are transferred abroad. They have variations depending on the type of transfers concerned (e.g., to data controllers, or to data intermediaries or processors). These clauses, designed to be incorporated into contracts, are developed by public authorities. They are generally considered to provide sufficient safeguards for the transfer of data, even to countries that do not enjoy an equivalence or adequacy recognition. These model clauses include:

- the European Union's recently modernised "Standard Contractual Clauses" (European Commission[14])[5]
- New Zealand's model contract clauses (Mabbett[15])
- Argentina's data protection contractual clauses (Ministry of Justice and Human Rights, Argentina[16]).

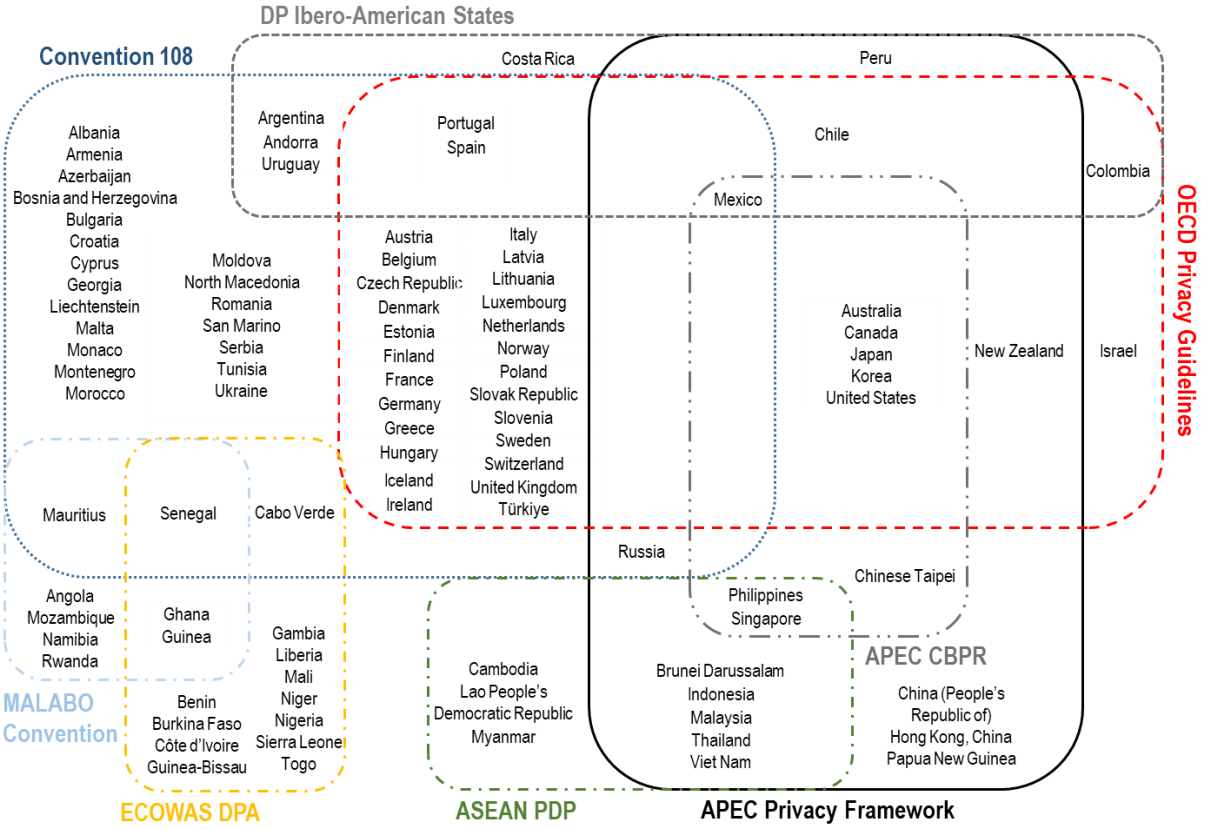
Regional groups increasingly recognise these model contract clauses as tools to support cross-border data flows with trust across participating countries. In 2021, for instance, the Association of Southeast Asian Nations published a set of Model Contractual Clauses for Cross-Border Data Transfers (ASEAN, 2021[17]). In the same year, the Ibero-American Data Protection Network adopted a resolution recognising the importance of these clauses as a transfer tool and triggering a procedure to adopt model contractual clauses (RIPD, 2021[18]). Pre-approved contractual clauses are also a recognised instrument under the modernised version of the Council of Europe's Convention 108 (C108) (see Article 14(3) (b) (Council of Europe, 2018[19])). The Council of Europe's C108 Committee has also recently started work on C108+ Standard Contractual Clauses. These examples illustrate the emerging commonality among the unilateral

mechanisms used by countries,[6] as well as emerging complementarities between unilateral mechanisms and intergovernmental arrangements.

4.2.2. Intergovernmental arrangements

Intergovernmental arrangements aim to generate consensus around the transfer of specific types of data. The most well-known examples are in the field of privacy and personal data protection. Examples include the OECD Privacy Guidelines (OECD, 2013[20]), the APEC Cross-Border Privacy Rules (CBPR) System (CBPRs[21]) and the Council of Europe Convention 108 and related instruments (Council of Europe, 2018[19]). These arrangements collectively involve at least 96 economies, some of which are party to several arrangements (Figure 4.3).

Figure 4.3. Overlapping memberships of intergovernmental arrangements

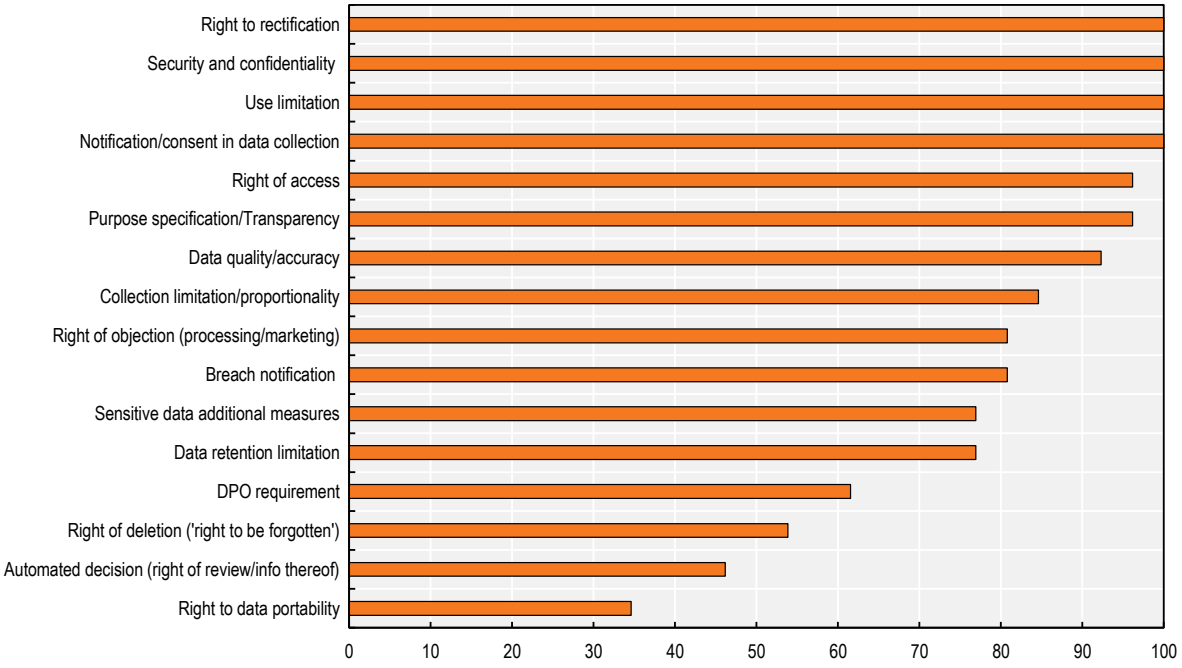


Note: Figure accurate as of February 2021. ECOWAS DPA = Economic Community of West African States Data Protection Agreement; DP Ibero-American States = Data Protection for Ibero-American States; APEC = Asia-Pacific Economic Cooperation.
Source: Casalini, López González and Nemoto (2021[13]), "Mapping commonalities in regulatory approaches to cross-border data transfers", *OECD Trade Policy Papers*, No. 248, https://doi.org/10.1787/ca9f974e-en.

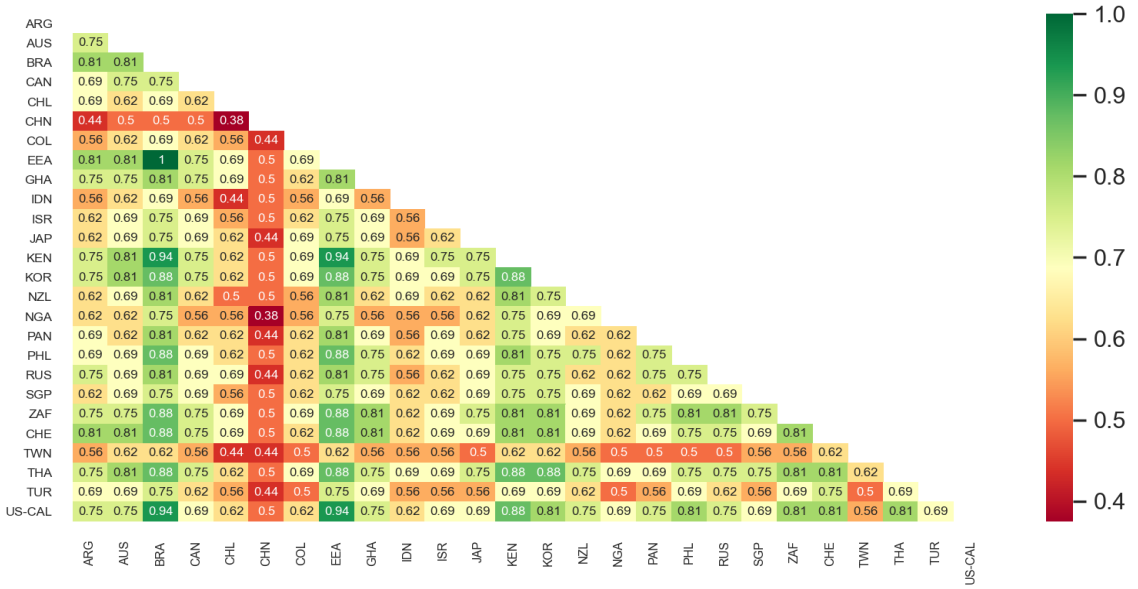
Although the emerging landscape of intergovernmental arrangements appears complex, it is underpinned by a number of common privacy and data protection principles. Indeed, overall, 68% of the elements covered in existing domestic privacy and data protection regulations (across a sample of OECD countries and emerging economies) overlap (Figure 4.4a). Overlaps are generally larger among economies that are party to the same arrangements (Figure 4.4b). This suggests the presence of *commonalities* on which to explore building mechanisms to enable data transfers.

Figure 4.4. Issues covered in privacy and personal data protection regulation across economies strongly overlap

a. Principles covered in privacy and personal data protection regulation



b. Overlap in economies' approaches to privacy and personal data protection regulation



Note: Panel a: 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]. Panel b: Overlap measures the extent to which economy pairs contain similar privacy and personal data protection principles in their regulation. See (Casalini, López González and Nemoto, 2021[13]) for method for calculating overlap. Overlap is based on stated elements in the regulation, each equally weighted, and not in how these are defined, implemented or enforced. It is therefore a stylised representation of emerging overlaps. New rules on personal data protection are under discussion in many economies, including in Chile and the People's Republic of China. Data last updated December 2020.

Source: Casalini, López González and Nemoto (2021[13]), "Mapping commonalities in regulatory approaches to cross-border data transfers", *OECD Trade Policy Papers*, No. 248, https://doi.org/10.1787/ca9f974e-en.

Overall, these figures also suggest there are elements of *convergence* in the principles enshrined in different privacy and data protection regulations. This may have come as a result of intergovernmental arrangements themselves. It may also have driven the formation of intergovernmental arrangements as like-minded countries form coalitions. Either way, intergovernmental arrangements might be an avenue to, or an important building block in, finding greater agreement on privacy and personal data protection issues. This, in turn, could facilitate the movement of personal data across borders with "trust." Indeed, in the context of work on the Privacy Guidelines in 2021, many countries reported their laws were based on, and still reflect, the 2013 Privacy Guidelines (OECD, 2021[22]).

From a privacy enforcement authorities' perspective, feedback reflected that the Privacy Guidelines continue to be relevant as a "unifying regime for encouraging co-operation among OECD Member countries and a set of benchmark norms for non-member countries that encourage uniformity and better data privacy across the globe." At the same time, there are personal data protection issues beyond the scope of privacy enforcement authorities, which do not benefit from intergovernmental arrangements like the OECD Privacy Guidelines. These include the access and processing of data for law enforcement and national security purposes.

Intergovernmental arrangements to strengthen cross-border enforcement co-operation of privacy laws can also help foster trust and often support many intergovernmental arrangements in the area of privacy. As such these arrangements are strongly linked to discussions on advancing DFFT (Box 4.2).

Box 4.2. Cross-border co-operation for enforcement of privacy laws

In 2021, in response to a questionnaire on the OECD Privacy Guidelines, approximately two-thirds of respondent countries said their privacy enforcement authority had sought assistance from, or referred a privacy violation complaint to, a privacy enforcement authority in another country and/or vice versa (OECD, 2021[22]). In practice, cross-border enforcement co-operation can take many forms. These include simply sharing information and evidence, formal or informal consultations, joint investigations and co-ordinated compliance actions. It could also include establishing frameworks detailing the conditions for such sharing through Memoranda of Understanding between two or more countries, depending on the needs, purposes and tools available. To advance co-operation in cross-border enforcement of privacy laws, participation in the Global Privacy Enforcement Network ("GPEN", a network for privacy enforcement co-operation created by the OECD in 2010) was the most cited in a recent OECD survey. This was followed by the Global Privacy Assembly (GPA) Enforcement Cooperation Arrangement and the APEC Cross-border Privacy Enforcement Arrangement (CPEA) (OECD, 2021[22]). Also of note is the binding enforcement co-operation mechanism under Council of Europe's Convention 108 and related instruments.

Respondents also reported benefiting from regional networks of data protection authorities from countries that share similarities in terms of language and culture. Such networks helped facilitate and promote cross-border enforcement co-operation and capacity building by sharing knowledge and best practices for data protection. Such networks include the Asia Pacific Privacy Authorities (APPA) Forum for Asia-Pacific countries, the Common Thread Network for Commonwealth countries, l'Association Francophone des Autorités de Protection des Données Personnelles for data protection authorities of French-speaking countries and the International Organization of La Francophonie, as well as Ibero-American Data Protection Network (RIPD) of Latin American supervisory authorities.

Finally, the 2007 OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy (OECD, 2007[23]) reflects a commitment by governments to improve their domestic frameworks for privacy law enforcement to better enable their authorities to co-operate with foreign authorities, as well as to provide mutual assistance in the enforcement of privacy laws. This Recommendation is being reviewed.

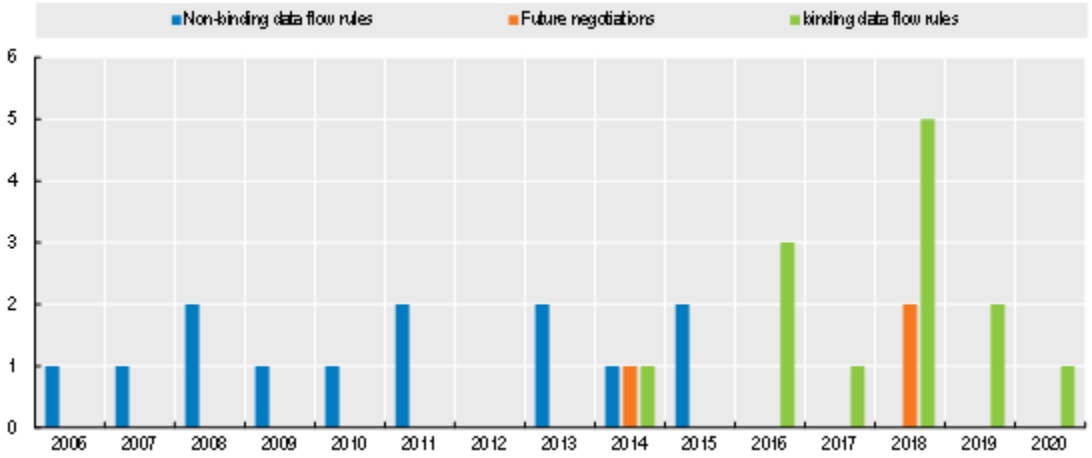
Note: For the latest information on international enforcement activities within the GPA, please see the Annual Report of the International Enforcement Cooperation Working Group: 1.3e-version-4.0-International-Enforcement-Cooperation-Working-Group-adopted.pdf (globalprivacyassembly.org).
Source: Robinson, Kizawa and Ronchi (2021[1]) "Interoperability of privacy and data protection frameworks", *OECD Going Digital Toolkit Notes*, No. 21, https://doi.org/10.1787/64923d53-en.

4.3.3. Trade and digital economy agreements

Trade and digital economy agreements are increasingly addressing issues around cross-border data flows (both personal and non-personal data). Since 2008, and up to December 2020, 29 trade agreements involving 72 economies introduced some form of data flow provisions. However, the nature, depth and specificity of provisions varies among agreements. Approximately 45% of these trade agreements include non-binding guidance on data flows, with broad provisions affirming the importance of working to maintain cross-border data flows (e.g., Korea-Peru Free Trade Agreement (FTA) and Central America-Mexico FTA). Another 45% of trade agreements, most of which were signed in the last five years, contain binding commitments on data flows (of all types of data). These include the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) FTA and the United States-Mexico-Canada Agreement (USMCA). Almost all of these also include exceptions allowing parties to restrict data flows to meet

"legitimate public policy objectives." In addition, all include provisions on the need to have in place a domestic privacy framework (including references to the intergovernmental arrangements outlined above such as the OECD Privacy Guidelines or the APEC CBPR System). There is some evidence of *convergence*: trade agreements are increasingly binding and include more similar language on data flow issues – Figure 4.5.

Figure 4.5. Binding data flow provisions in trade agreements have been on the rise



Note: The table does not reflect most of the recent agreements that have yet to be covered by the latest TAPED database. This includes. for instance, the Regional Comprehensive Economic Partnership (RECP) and the Japan-UK CEPA. Future negotiations refer to instances where parties to an agreement indicate an intention to reconvene to discuss specific issues at a later date.
Source: Casalini, López González and Nemoto (2021[13]), "Mapping commonalities in regulatory approaches to cross-border data transfers", *OECD Trade Policy Papers*, No. 248, https://doi.org/10.1787/ca9f974e-en.

Trade agreements also increasingly 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 these topics, all agreements that include binding data flow rules also require or promote adoption of domestic privacy and personal data protection frameworks. This includes encouraging parties to consider international standards and guidelines on protection of personal information (including those discussed in intergovernmental arrangements). Of 18 economies that signed agreements with binding cross-border data flow provisions, 15 are also party to at least one of the intergovernmental arrangements listed in the previous section highlighting *complementarities* across approaches. Other provisions in such agreements include requiring parties to publish information on the personal information protection applicable in the country.

In parallel, countries have also started negotiating broader digital economy agreements (DEAs). These touch on a range of issues, from artificial intelligence to e-payments. These new types of trade arrangements often include binding provisions on both maintaining personal data protection frameworks, and allowing cross-border data flows, subject to certain exceptions.

Examples of DEAs include:

- the Digital Economy Partnership Agreement (DEPA) between Chile, New Zealand and Singapore (Government of New Zealand, 2020[24])
- the Singapore-Australia Digital Economy Agreement (Government of Australia, 2020[25])
- the United Kingdom-Singapore Digital Economy Agreement (UKSDEA) (Government of Singapore, 2022[26])

- the Korea-Singapore Digital Partnership Agreement (Government of Singapore, 2021[27]).

Overall, this suggests that binding data flow provisions go hand in hand with exceptions for legitimate public policy objectives and/or with 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 must be accompanied by safeguards for personal data protection, including via reference to intergovernmental arrangements.

In 2020, the EU-UK Trade and Cooperation Agreement (TCA) introduced a clause stating that "measures on the protection of personal data and privacy, including with respect to cross-border data transfers" should include "instruments enabling transfers under conditions of general application for the protection of the data transferred" (European Union, 2020[28]). This also highlights some emerging *complementarities* between instruments where trade agreements call on unilateral instruments for enabling transfers.

Relatedly, trade and DEAs increasingly include provisions prohibiting requirements that computing facilities be located domestically as a condition for conducting business. Trade agreements are increasingly addressing data localisation, as further explained in section 4.2.

4.3. Supporting initiatives

Alongside policy and regulatory approaches directly governing cross-border data flows, governments, regulators, notably data protection authorities, and other stakeholders are also pursuing a range of supporting initiatives to foster trust and facilitate cross-border flows (OECD, 2021[22]). Informal ad-hoc discussions to promote cross-border data flows, for example, can include stakeholder consultations, workshops, and advisory guidelines. They also include still-informal discussions in the context of more formal initiatives (e.g., discussions in established fora such as the United Nations, the OECD or Asia-Pacific Economic Cooperation (APEC).

Some of these efforts involve discussions and co-operation across stakeholders, especially in relation to privacy and data protection. They provide a forum for regulators, practitioners and policy makers to share best practices, track trends and advance privacy management issues, including specifically relating to cross-border data flows.

For example, the Global Privacy Assembly (GPA) (former International Conference of Data Protection and Privacy Commissioners: ICDPPC) is a global forum for data protection authorities joined by more than 130 authorities across the globe. The GPA operates through working groups on a range of topics and issues, one of which focuses on Global Frameworks and Standards; it has a current work stream on cross-border transfers. In 2020, the GPA adopted the working group's analysis of ten global data protection frameworks, which had found a high degree of commonality between them. In 2021, the GPA adopted the working group's further analysis and report on cross-border transfer mechanisms.[7]

The Asia Pacific Privacy Authorities Forum (APPA) (appaforum.org[29]) is also an important platform for informal co-operation and capacity building for privacy regulators and governments with data protection competence in the Asia-Pacific region. It includes the United States, Canada, and Latin and South American countries.

Similarly, international organisations like APEC, Association of Southeast Asian Nations, or the OECD through bodies such as the Committee on Digital Economy Policy and the Trade Committee, have been increasingly facilitating dialogue and hosting workshops on the issue of data free flow with trust (DFFT).

Also of relevance, the UN Committee of Experts on Big Data and Data Science for Official Statistics launched a UN PET Lab in 2022. The lab aims to pilot a programme to make international data flows more secure by using privacy-enhancing technologies (PETs). It will bring together statistical bodies to collaborate with technology providers that offer PET technologies to test solutions to transfer data across

borders privacy-compliantly. The US Census Bureau, Statistics Netherlands, the Italian National Institute of Statistics and the UK's Office for National Statistics will be involved in the project (unstats.un.org, 2022[29]).

4.4. Technological and organisational tools

Amid dynamic policy activity in the area of data protection and cross-border data flows, diverse technological and organisational tools have also emerged. These are tools developed to better handle issues around cross-border data transfers, often in the context of privacy and digital security protection. They are developed by non-governmental and private sector organisations but sometimes benefit from the support of governments or regulators. Two key typologies can be identified: trust marks and data sharing services. It may be premature to draw definitive conclusions about the scope and usefulness of technological and organisational tools. However, these tools are emerging as a priority area for future work, testifying to their growing importance in the evolving DFFT environment.

4.4.1. Trust marks

Standards, certifications and codes of conduct, collectively known as "trust marks", are being increasingly explored and proposed to foster trust in data sharing domestically and across borders. Although there is no common definition, these tools are generally designed to help organisations demonstrate that their practices comply with international standards in the field of privacy, data protection or digital security. In this way, they help consumers recognise "trustworthiness." Such trust marks may facilitate data sharing across organisations, irrespective of geographic location. For example, several ISO standards provide guidance when establishing, implementing, maintaining and improving Privacy Information Management Systems (PIMS) (ISO, 2019[30]).[8]

4.4.2. Data sharing services

Technological and organisational tools also include an emerging type of business – so-called data intermediaries or data sharing services. Data intermediaries are defined by the OECD as "service providers that facilitate data access and sharing under commercial or non-commercial agreements between data holders, data producers, and/or users" (OECD, 2019[31]).

Data intermediaries are expected to play a key role in the data ecosystem, facilitating the aggregation and exchange of data, both bilaterally and for effective data pooling. In particular, data intermediaries may leverage technology-driven pathways such as PETs to facilitate cross-border sharing of personal data (WEF, 2022[32]; CDEI, 2021[33]; OECD, 2019[31]).

5 Other issues affecting data free flows with trust

In this complex and evolving policy environment, two additional issues are also increasingly affecting the free flow of data with trust: government access to personal data held by the private sector for the purposes of law enforcement and national security; and data localisation measures.

5.1. Government access to personal data held by private sector entities for law enforcement and national security purposes

The practice of governments accessing personal data held by private sector entities for law enforcement and national security is increasingly recognised as a concern that hinders cross-border data flows. While access to these data can be valuable to promote the public interest by supporting national security and law enforcement actions, government access may affect privacy and other rights (ICC, 2022[34]).

The OECD Privacy Guidelines (OECD, 2013[20]) provide a common baseline privacy standard for OECD member countries and beyond. However, they include exceptions for law enforcement and national security purposes. This is reflected in most domestic privacy and data protection frameworks of OECD countries, where this type of access is governed by separate legal frameworks and falls largely outside the jurisdiction of data protection authorities.

Nonetheless, OECD countries' legal frameworks implement safeguards to protect privacy when personal data held by private entities is accessed by law enforcement and national security authorities. However, there is currently no mutual understanding or shared articulation across countries of existing frameworks, policies and practices to safeguard individuals' rights when governments access data for law enforcement and national security purposes.

Lack of clarity, transparency and consistency with respect to national approaches to government access to data held by the private sector affects trust between individuals, governments and companies. In response, privacy frameworks sometimes include explicit provisions that seek to prevent transfers of data to countries whose governments may be accessing personal data held by the private sector without "appropriate" safeguards. In other words, some regulations foresee that the transferring entity verify whether rules and practices in the destination countries may pose a risk to data protection standards as applicable domestically.

A high-profile case at the Court of Justice of the European Union provides an illustrative example. The case involved invalidation of the adequacy decision of the EU-US Privacy Shield Framework, which was based on concerns about surveillance laws in the United States. These laws were deemed to allow the government to access personal data in ways inconsistent with domestically applicable laws in EU member states (European Parliament, 2020[35]).

Ultimately, these transparency gaps and perceived differences erode trust and threaten to disrupt cross-border data flows. This erosion of trust may also serve as the rationale for an increasing number of compelled data localisation measures globally. Such measures are seen as a way to prevent access by foreign government altogether (ICC, 2022[34]).

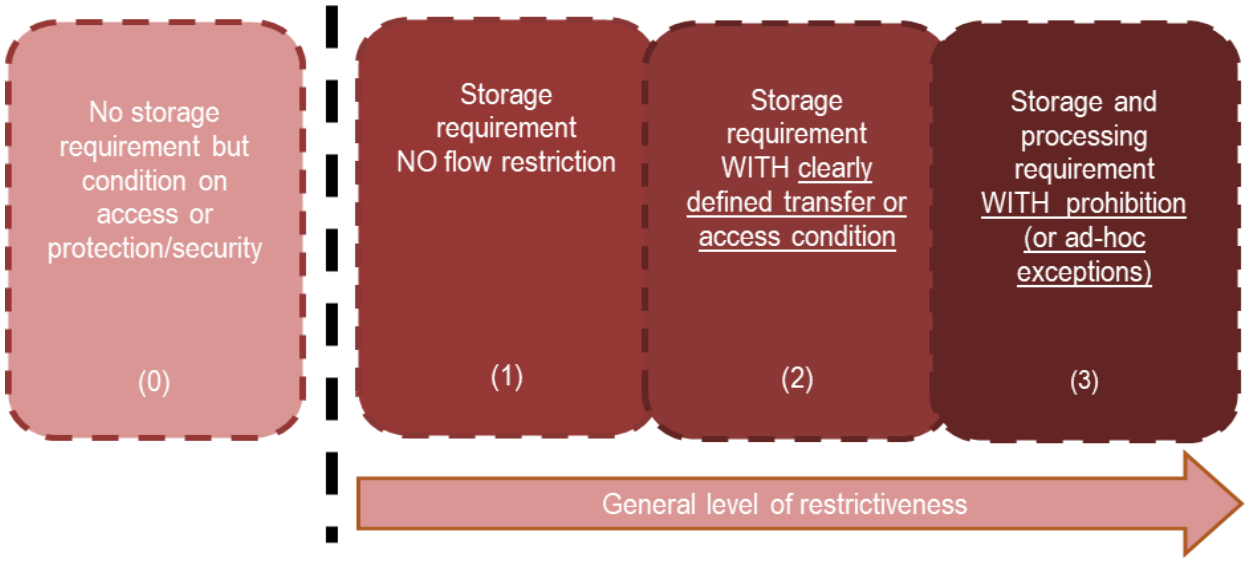
In line with this, the OECD has identified unconstrained and disproportionate government access to personal data held by the private sector as a crucial issue for data governance and the protection of individual rights. It has also identified the issue as a potential barrier to enabling the free flow of data with trust (CDEP, 2020[36]). Consequently, it seeks to identify and flesh out commonalities across OECD countries' relevant practices. The work to date suggests a high degree of commonality among policies and practices of OECD countries for government access to data for the purposes of law enforcement and national security. The G7 also expressed support for this work in its 2022 Action Plan in Annex to the Digital Ministers' Declaration (G7, 2022[37]).

5.2. Data localisation measures

Although there is no single and widely accepted definition of data localisation, it is generally understood to refer to implicit or explicit requirements that data be stored and/or processed within the domestic territory. There are three broad types of data localisation measures. The first relates to measures that mandate local storage but allow copies to be sent and processing to take place abroad. The second relates to measures that mandate local storage and allow transfer or processing abroad under clearly defined conditions. The third relates to measures that mandate local storage and processing and prohibit transfers abroad (with ad-hoc exceptions) (López González, Casalini and Porras, 2022[38]).

Outside this typology of data localisation measures, a new category of approaches is emerging (Category 0). These are measures with no requirement for local data storage. However, firms are required to guarantee access to data for regulatory purposes.

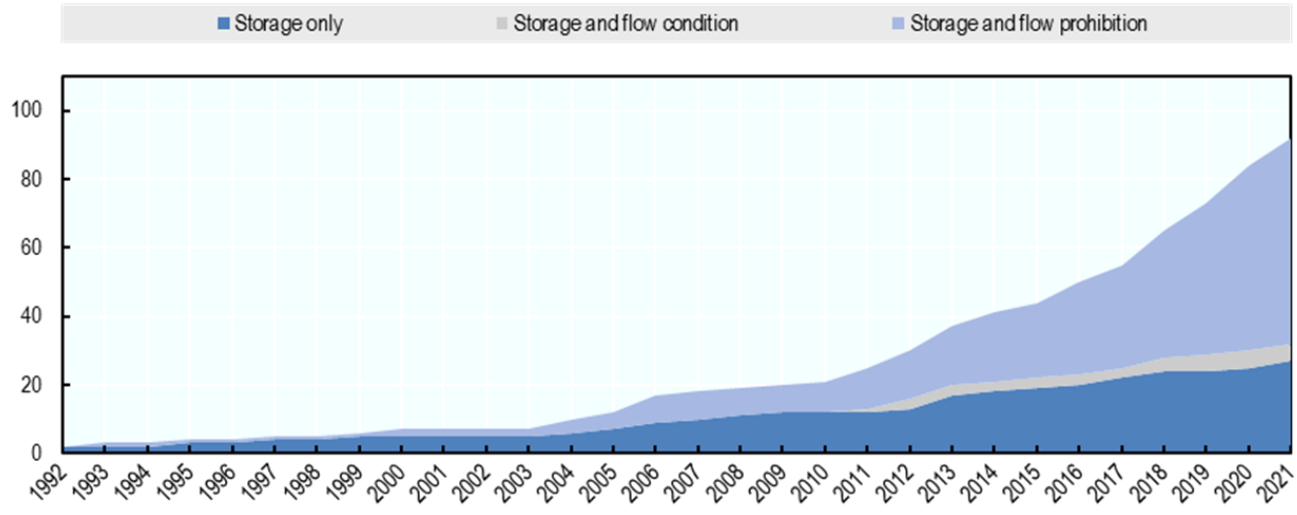
Figure 5.1. Typology of data localisation measures and requirements for data flow



Note: Figure is schematic; elements do not singularly identify any given country's approach to data localisation. Different approaches tend to apply to different types of data, even within the same jurisdiction.
Source: López González, Casalini, and Porras (2022[38]), "A Preliminary Mapping of Data Localisation Measures", *OECD Trade Policy Papers* No. 262, https://doi.org/10.1787/c5ca3fed-en.

Analysis of existing measures reveals that data localisation is on the rise. By 2021, there were 92 data localisation measures in place across 39 countries (Figure 5.2). More than half of these have emerged over the last five years. Importantly, the measures themselves are becoming more restrictive; by 2021, two-thirds of measures in place involved a storage requirement with a flow prohibition.

Figure 5.2. Data localisation measures are increasing and becoming more restrictive



Note: Data localisation measures are defined as explicit requirements that data be stored or processed domestically.
Source: López González, Casalini, and Porras (2022[38]), "A Preliminary Mapping of Data Localisation Measures", *OECD Trade Policy Papers* No. 262, https://doi.org/10.1787/c5ca3fed-en.

Measures appear to be more restrictive in non-OECD countries. Indeed, in OECD member countries, 60% of data localisation measures involve only storage requirements. Conversely, in non-OECD, the vast majority of measures (83) involve storage requirements with flow prohibitions.

International commitments banning data localisation, including for personal data (albeit with exceptions), have largely been established in the context of FTAs. By 2021, there were 17 agreements with provisions banning data localisation (albeit with different exceptions). This is a recent trend, starting in 2014, which seems to have coincided with the growth in the number of data localisation measures. Nevertheless, international commitments banning local storage requirements do not appear to have been developed in other contexts than FTAs.

Discussions on data localisation have also taken place in the context of the G7. Under the UK G7 Presidency in 2021, the G7 Trade Ministers agreed on a set of Digital Trade Principles (G7, 2021[39]). Within these, countries express concern "about situations where data localisation requirements are being used for protectionist and discriminatory purposes, as well as to undermine open societies and democratic values, including freedom of expression".

The 2021 review of the implementation of the OECD Privacy Guidelines highlighted the need to recognise the possible effect of data localisation of personal data on cross-border data flows. The report emphasises the relevance of the accountability principle and the proportionality test articulated in the OECD Privacy Guidelines in evaluating data localisation measures (Svantesson, 2020[40]).

6 Pathways to foster trust and enable greater interoperability

Promoting data free flow with trust remains a challenge for policy makers. However, the diversity of approaches has led to a fragmented regulatory environment. This makes it difficult for individuals, businesses and governments to operate in a "trusted" environment. There are, nevertheless, a number of commonalities, complementarities, and elements of convergence for policymakers to build on as they look for pathways to advance trust and foster future interoperability.

6.1. Paths towards greater trust and interoperability

Ensuring the free flow of data with trust remains a challenge for policy makers. Different solutions to this complex challenge have emerged, leading to a fragmented regulatory environment that makes it difficult for individuals, businesses and governments to operate in a "trusted" environment. This report highlights a number of commonalities, complementarities, and elements of convergence for policy makers to build on as they look for pathways to further foster trust and promote future interoperability.

First, **commonalities** between the regulatory and policy instruments are emerging. For instance, whether through unilateral mechanisms, trade agreements or intergovernmental arrangements, there appears to be consensus on the dual goal of safeguarding data and enabling its flow across borders (although differences arise in how these goals may best be achieved). Moreover, domestic frameworks tend to provide relatively similar unilateral mechanisms to transfer data with safeguards (albeit with differences related to how and by whom the safeguarding is done). All trade agreements that contain binding provisions

on cross-border data flows also include similar exceptions for legitimate public policy objectives and have provisions on maintaining privacy or consumer protection frameworks.

Second, there is also growing evidence of elements of **convergence**, often based on the aforementioned commonalities. For instance, there are signs of growing convergence towards more similar principles in privacy and personal data protection frameworks, including in the context of intergovernmental arrangements. Trade agreements are also showing signs of convergence, with data flow provisions that are increasingly binding and use more similar language. Convergence is also emerging in the context of more recognition of data intermediaries as approaches to promote data sharing (e.g., those leveraging privacy-enhancing technologies).

Finally, there is a high degree of **complementarity** between instruments. Unilateral instruments draw from, and contribute to, intergovernmental arrangements. Meanwhile, trade agreements increasingly reference intergovernmental arrangements on data protection as part of their binding data flow provisions. Recently, the EU-UK Trade and Cooperation Agreement also introduced the requirement that protection of personal data and privacy measures include unilateral instruments to enable data transfers.

Complementarity is also observed in the way converging rules, standards and principles are perceived as more likely to deliver data free flow with trust (DFFT) if underpinned by solid networks of enforcement authorities to tackle cross-border cases. In that same vein, engagement in international fora on issues that are seen as critical to promoting DFFT. For example, the OECD's ongoing work on government access to personal data held by the private sector, or on data localisation measures, are key complements to other regulatory co-operation efforts in this area.

Together, these elements indicate the potential for an 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. In particular, the notion of interoperability of privacy regimes was introduced in the 2013 revision of the OECD Privacy Guidelines. According to OECD work, privacy interoperability can be understood operationally as the "ability of different privacy and data protection regimes, or legal frameworks, to work together at multiple levels through policy and practical arrangements and thereby bridge any differences in approaches and systems of privacy and personal data protection to facilitate transborder flows of personal data" (Robinson, Kizawa and Ronchi, 2021[1]).

Discussions are underway. Indeed, at the 2021 G20 under the Italian Presidency, Leaders agreed to "continue to further common understanding and to work towards identifying commonalities, complementarities and elements of convergence between existing regulatory approaches and instruments enabling data to flow with trust, in order to foster future interoperability" (G20, 2021[41]). Similar language has also been used in the Digital and the Trade declarations of the G7 in 2021 and 2022 (G7, 2021[42]; G7, 2022[43]).

As a trusted forum for evidence-based analysis and multi-stakeholder dialogue, the OECD can continue to help countries harness their commonalities and advance discussions promoting DFFT. Through its evidence-based policy analysis and multi-stakeholder engagement, the OECD can support discussions on how to approach different policy options for governing cross-border data flows, including data localisation. By continuing to help build the evidence base, it can help think through the effectiveness of different measures in achieving their stated aims. It can also identify the associated costs and trade-offs of such measures, as well as any alternatives that would enable to maximise overall benefits for societies by making the global regulatory landscape more interoperable.

International co-operation on these issues, while not without challenges, can help reconcile differences. The OECD can focus on areas of commonalities and help highlight complementarities and elements of convergence between approaches. In so doing, it can help identify promising areas and actions to advance trust and interoperability. Ultimately, it can help countries design an enabling environment for a thriving, global and trusted digital economy.

References

Acquisti, A., C. Taylor and L. Wagman (2016), "The economics of privacy", *Journal of Economic Literature*, Vol. 54/2, pp. 442-492, https://www.aeaweb.org/articles?id=10.1257/jel.54.2.442. [5]

ASEAN (2021), "ASEAN Model Contractual Clauses for Cross Border Data Flows", https://asean.org/wp-content/uploads/2021/08/ASEAN-Model-Contractual-Clauses-for-Cross-Border-Data-Flows.pdf. [17]

Casalini, F. and J. López González (2019), "Trade and Cross-Border Data Flows", *OECD Trade Policy Papers*, No. 220, OECD Publishing, Paris, https://doi.org/10.1787/b2023a47-en. [8]

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://doi.org/10.1787/818a7498-en. [3]

Casalini, F., J. López González and T. Nemoto (2021), "Mapping commonalities in regulatory approaches to cross-border data transfers", *OECD Trade Policy Papers*, No. 248, OECD Publishing, Paris, https://doi.org/10.1787/ca9f974e-en (accessed on 3 March 2022). [13]

CBPRs (n.d.), *Cross Border Privacy Rules System*, website, http://cbprs.org/ (accessed on 22 April 2022). [21]

CDEI (2021), *Unlocking the value of data: Exploring the role of data intermediaries*, Centre for Data Ethics and Innovation, Government of the United Kingdom, https://www.gov.uk/government/publications/unlocking-the-value-of-data-exploring-the-role-of-data-intermediaries/unlocking-the-value-of-data-exploring-the-role-of-data-intermediaries. [33]

CDEP (2020), "Statement of the Committee on Digital Economy Policy", OECD, Paris, https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/CDEP(2020)22/FINAL&docLanguage=En (accessed on 25 April 2022). [36]

Council of Europe (2018), "Convention 108 + Convention for the protection of individuals with regard to the processing of personal data", https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1. [19]

European Commission (n.d.), "Standard Contractual Clauses", webpage, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en (accessed on xx November 2021). [14]

European Parliament (2020), "The CJEU judgment in the Schrems II case", European Parliament, Brussels, https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATA(2020)65207 [35]

3_EN.pdf.

European Union (2020), *Trade and Cooperation Agreement between the European Union and the European Atomic Energy Community, of the one part, and the United Kingdom of Great Britain and Northern Ireland, of the other part*, European Parliament, Brussels, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:22021A0430(01)&from=EN. [28]

G20 (2021), *G20 Rome Leaders' Declaration*, https://www.consilium.europa.eu/media/52730/g20-leaders-declaration-final.pdf. [41]

G7 (2022), "G7 Digital Ministers' Track - Annex 1", *G7 Action Plan for Promoting Data Free Flow with Trust*, https://bmdv.bund.de/SharedDocs/DE/Anlage/K/g7-praesidentschaft-final-declaration-annex-1.pdf?__blob=publicationFile. [37]

G7 (2022), *MInisterial Declaration, G7 Digital Ministers' meeting*, https://bmdv.bund.de/SharedDocs/DE/Anlage/K/g7-praesidentschaft-final-declaration.pdf?__blob=publicationFile. [43]

G7 (2021), *G7 Trade Ministers' Digital Trade Principles*, https://www.gov.uk/government/news/g7-trade-ministers-digital-trade-principles. [39]

G7 (2021), *Ministerial Declaration, G7 Digital and Technology Ministers' meeting*, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/981567/G7_Digital_and_Technology_Ministerial_Declaration.pdf. [42]

Government of Australia (2020), *Australia-Singapore Digital Economy Agreement*, https://www.dfat.gov.au/sites/default/files/australia-singapore-digital-economy-agreement.docx. [25]

Government of New Zealand (2020), *Digital Economy Partnership Agreement*, https://www.mfat.govt.nz/assets/Trade-agreements/DEPA/DEPA-Signing-Text-11-June-2020-GMT-v3.pdf. [24]

Government of Singapore (2022), *United Kingdom - Northern Ireland - Singapore Digital Economy Agreement*, Government of Singapore, https://www.mti.gov.sg/-/media/MTI/Microsites/DEAs/UKSDEA/Text-of-the-UKSDEA/2022-02-25---UK-Singapore-Digital-Economy-Agreement.pdf. [26]

Government of Singapore (2021), *Korea – Singapore Digital Partnership Agreement*, https://www.mti.gov.sg/-/media/MTI/Newsroom/Press-Releases/2021/12/Singapore-and-the-Republic-of-Korea-conclude-negotiations-on-a-Digital-Economy-Agreement.pdf. [27]

ICC (2022), *White Paper on Trusted Government Access to Personal Data Held by the Private Sector*, ICC, Paris, https://iccwbo.org/publication/icc-white-paper-on-trusted-government-access-to-personal-data-held-by-the-private-sector (accessed on 24 May 2022). [34]

ISO (2019), "Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines", No. ISO/IEC 27701:2019, International Organization for Standardization, Geneva, https://www.iso.org/standard/71670.html. [30]

Jouanjean, M. (2019), "Digital Opportunities for Trade in the Agriculture and Food Sectors", *OECD Food, Agriculture and Fisheries Papers*, No. 122, OECD Publishing, Paris, https://doi.org/10.1787/91c40e07-en. [9]

López González, J., F. Casalini and J. Porras (2022), "A Preliminary Mapping of Data Localisation Measures", *OECD Trade Policy Papers*, No. 262, OECD Publishing, Paris, https://doi.org/10.1787/c5ca3fed-en. [38]

López González, J. and M. Jouanjean (2017), "Digital Trade: Developing a Framework for Analysis", *OECD Trade Policy Papers*, No. 205, OECD Publishing, Paris, https://doi.org/10.1787/524c8c83-en. [10]

Mabbett, C. (2020), "Model contract clauses for sending personal information overseas", *New Zealand Privacy Commission*, Privacy Commissioner blog, https://privacy.org.nz/blog/model-contract-clauses-for-sending-personal-information-overseas/. [15]

Ministry of Justice and Human Rights, Argentina (2016), "Provision 60 - E/2016", Dirección Nacional de Protección de Datos Personales (National Directorate for the Protection of Personal Data), Ministry of Justice and Human Rights, Argentina, http://servicios.infoleg.gob.ar/infolegInternet/anexos/265000-269999/267922/norma.htm. [16]

National Board of Trade Sweden (2015), *No Transfer, No Production – a Report on Cross-Border Data Transfers, Global*, Kommerskollegium, Stockholm, https://www.kommerskollegium.se/globalassets/publikationer/rapporter/2016-och-aldre/no-transfer-no-production-a-report-on-crossborder-data-2015.pdf. [6]

National Board of Trade Sweden (2014), *No Transfer, No Trade – the Importance of Cross-Border Data Transfers for Companies Based in Sweden*, Kommerskollegium, Stockholm, https://www.kommerskollegium.se/globalassets/publikationer/rapporter/2016-och-aldre/no_transfer_no_trade_webb.pdf. [7]

OECD (2022), *Going Digital Guide to Data Governance Policy Making*, OECD Publishing, https://doi.org/10.1787/40d53904-en. [12]

OECD (2021), *International Regulatory Co-operation*, OECD Best Practice Principles for Regulatory Policy, OECD Publishing, Paris, https://doi.org/10.1787/5b28b589-en. [2]

OECD (2021), "Recommendation of the Council for Agile Regulatory Governance to Harness Innovation", No. OECD/Legal 0464, OECD, Paris, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0464. [11]

OECD (2021), "Report on the implementation of the Recommendation of the Council concerning guidelines governing the protection of privacy and transborder flows of personal data", No. C(2021)42, OECD, Paris, https://one.oecd.org/document/C(2021)42/en/pdf. [22]

OECD (2019), *Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies*, OECD Publishing, Paris, https://doi.org/10.1787/276aaca8-en. [31]

OECD (2013), "Recommendation of the Council Concerning Guidelines on the Protection of Privacy and Transborder Flows of Personal Data", No. OECD/LEGAL/0188, OECD, Paris, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188. [20]

OECD (2007), "OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy", https://www.oecd.org/sti/ieconomy/38770483.pdf. [23]

RIPD (2021), "Declaración Final del XIX Encuentro de la Red Iberoamericana de Protección de Datos", https://www.redipd.org/sites/default/files/2021-11/declaracion-final-xix-encuentro.pdf. [18]

Robinson, L., K. Kizawa and E. Ronchi (2021), "Interoperability of privacy and data protection frameworks", *Going Digital Toolkit Note, No. 21*, OECD Publishing, Paris, http://goingdigital.oecd.org/data/notes/No21_ToolkitNote_PrivacyDataInteroperability.pdf. [1]

Solove, S. (2006), "A taxonomy of privacy", *University of Pennsylvania Law Review*, Vol. 154/3, pp. 477-564, https://doi.org/10.2307/40041279. [4]

Svantesson, D. (2020), "Data localisation trends and challenges: Considerations for the review of the Privacy Guidelines", *OECD Digital Economy Papers*, No. 301, OECD Publishing, Paris, https://doi.org/10.1787/7fbaed62-en. [40]

unstats.un.org (2022), *UN launches first of its kind 'privacy lab' to unlock benefits of international data sharing*, UN stats, https://unstats.un.org/bigdata/events/2022/unsc-un-pet-lab/UN%20PET%20Lab%20-%20Press%20Release%20-%2025%20Jan%202022.pdf (accessed on 7 April 2022). [29]

WEF (2022), *Advancing Digital Agency: The Power of Data Intermediaries*, World Economic Forum, Cologny, Switzerland, https://www3.weforum.org/docs/WEF_Advancing_towards_Digital_Agency_2022.pdf. [32]

Notes

[1] Notwithstanding, Article 12 of the Universal Declaration of Human Rights recognises privacy as a human right. Articles 7 and 8 of the Charter of Fundamental Rights of the European Union recognise privacy and data protection as fundamental rights.

[2] In the case of agricultural supply chains, albeit with a different motivation, firms are increasingly sharing information with consumers about the persons engaged in producing and delivering agricultural products in response to consumer demand to know more about how goods are produced.

[3] Measures that give extraterritorial reach to a country's authorities are a different option from local storage requirements to protect national security.

[4] These approaches fall along the lines of the OECD Best Practice Principles for Regulatory Policy (OECD, 2021[2]).

[5] In June 2021, following the Court of Justice of the European Union's Schrems II ruling, the European Data Protection Board has issued non-binding Recommendations on supplementary measures to assist controllers and processors acting as data exporters with their duty to identify and implement appropriate supplementary measures where they are needed to ensure an essentially equivalent level of protection to the data they transfer to third countries.

[6] Efforts to leverage commonalities across arrangements have taken place in the past. For instance, an initiative between Asia-Pacific Economic Cooperation (APEC) and the European Union in 2014 aimed to develop a "Referential." This is an informal and pragmatic checklist for organisations applying for authorisation of corporate rules and/or certification under the Cross-Border Privacy Rules System. The aim was to facilitate the design and adoption of personal data protection policies compliant with both systems (Robinson, Kizawa and Ronchi, 2021[1]).

[7] These can be found in the following documents: 2020 Global Frameworks and Standards WG annual report - includes the analysis of global frameworks; 2021 Global Frameworks and Standards WG annual report - includes further analysis and report on cross border transfer mechanisms (Annex A, page 14).

[8] Examples of relevant standards include: ISO/IEC 27701:2019; ISO/IEC 27701, 7.5.2; ISO/IEC 27701, 8.5.5.