OECD publishing

CROSS-BORDER DATA FLOWS

TAKING STOCK OF KEY POLICIES AND INITIATIVES

OECD BACKGROUND REPORT FOR THE G7 DIGITAL AND TECHNOLOGY TRACK

Germany **2022**

G7 GERMANY 2022

OECD
BETTER POLICIES FOR BETTER LIVES

This report was prepared by the Organisation for Economic Co-operation and Development (OECD) Directorate for Science, Technology and Innovation (STI) for the Federal Ministry for Economic Affairs and Climate Action, to inform discussions in the G7 Digital and Technology Track under the auspices of the German G7 Presidency in 2022. The opinions expressed and arguments employed herein do not necessarily represent the official views of the member countries of the OECD or the G7.

Acknowledgements

The report was authored by Francesca Casalini of the OECD Digital Economy Policy Division, headed by Audrey Plonk, with contributions from Gallia Daor and David Gierten (OECD), in co-ordination with Andreas Hartl, Alexander Wajnberg and Carl-Philipp Sassenrath of the German Federal Ministry for Economics and Climate Action and with the German 2022 G7 Presidency's digital team in the German Federal Ministry for Digital and Transport.

Many thanks to the German 2022 G7 Presidency and the working group members of the G7 Digital and Technology Track for their guidance in developing the report and to OECD colleagues, Clarisse Girot (Science, Technology and Innovation Directorate), Javier López González (Trade and Agriculture Directorate), and Nejla Saula and Raffaella Centurelli (Global Relations and Co-operation Directorate) for valuable feedback in its finalisation.

This document 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.

Cover image: © Martins Vanags/Shutterstock

© OECD, 2022

The use of this work, whether digital or print, is governed by the Terms and Conditions to be found at http://www.oecd.org/termsandconditions.

Table of contents

1. Introduction 4
2. Unilateral policies and regulations 5
3. Inter-governmental processes 6
3.1 The G7 and G20 deliberations in the areas of Data Free Flow with Trust and cross-border data flows 7
3.2 Multilateral approaches 8
3.3 Regional arrangements 11
3.4 Preferential trade agreements 13
4. Technological and organisational measures 14
4.1 Data spaces 15
5. Conclusion 17

References 18

1. Introduction

Over the past three decades, data access, sharing and use have become central drivers of economic growth and social well-being. Data, and in particular their transfer and sharing across borders, have become an integral part of every sector of the economy as well as a critical source of innovation for disruptive technologies such as the Internet of Things and Artificial Intelligence. However, the ubiquitous exchange of data across borders has amplified a range of concerns for governments, businesses, and citizens, eroding trust among them.

In response to this erosion of trust, policies and regulations addressing cross-border data flows are increasing. There are different reasons motivating countries to regulate cross-border data flows, often placing conditions on its sharing abroad. One reason is to safeguard the privacy of individuals and their personal data. Countries may also place conditions on the flow of data to ensure access by domestic authorities to data that are important for law enforcement or audit purposes. Conditions placed on cross-border data flows might also arise for the protection of information deemed to be sensitive from a security perspective. Lastly, some countries are using cross-border data regulation with a view to developing domestic capacity in digitally intensive sectors, as a form of digital industrial policy (OECD, 2020[1]).

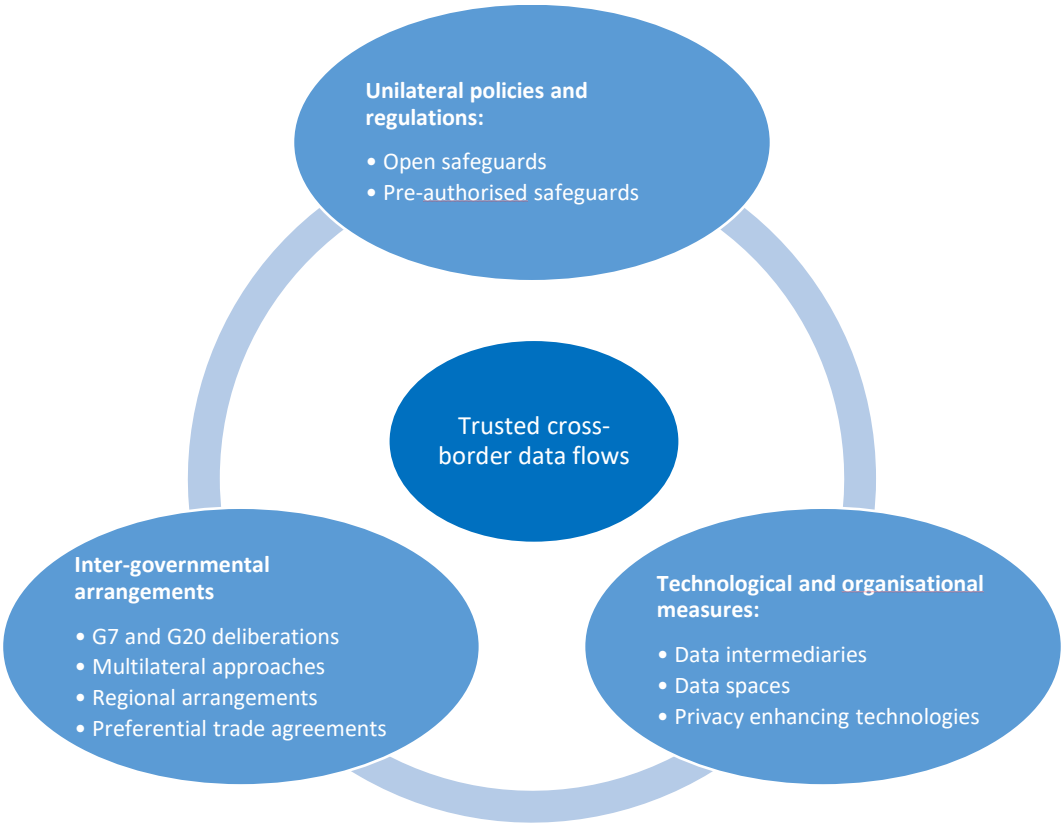
However, the resulting multi-layered landscape of policies and regulations governing cross-border data flows is creating additional costs, operational complexity and uncertainties for businesses and other entities to share data across borders, and for governments to enforce public policy objectives.

As data gain their rightful place as an important resource for the global economy, it is important to establish and advance trust to facilitate data sharing, domestically and especially across borders. Individuals may be reluctant to engage with businesses where they perceive a deficit of trust and, in turn, businesses may struggle to reap the benefits of scale unless they can operate with trust globally. The notion of trust also plays a role in how governments and individuals interact with other governments, enabling trusted cross-border regulatory cooperation.

In this context, the international policy community has demonstrated a growing interest in dialogue and processes to facilitate cross-border data flows with trust. Although the understanding of what trust means for individuals, business or governments can vary, significant momentum for this policy agenda in the G7, and G20, has gone hand in hand with a wide range of – often complementary – policy initiatives at the national and international levels.

This report takes stock of existing agreements, processes and initiatives involving the G7 countries that contribute to promoting trusted cross-border data flows, with a view to informing future G7 efforts in this area. This includes an overview of unilateral policies and regulations (Section 2); inter-governmental level processes (Section 3); and technological and organisational measures (Section 4). Sections 2-4 describe and examine key policies and initiatives under each of these categories (Figure 1) and section 5 summarises the findings and identifies possible next steps for this policy agenda.

Figure 1. Key policies and processes for trusted cross-border data flows



Source: Authors' own elaboration.

2. Unilateral policies and regulations

Throughout the past few decades, countries have developed and implemented a range of policies and regulations to unilaterally govern the flow of data across borders in an effort to establish trust. Although developed at different times, these unilateral policies and regulations share some common elements. First, they share the common purpose of enabling cross-border data flows while protecting other public policy objectives. Second, these policies and regulations increasingly share the types of provisions, mechanisms and instruments that they use or recognise to realise this common purpose (Casalini, López-González and Nemoto, 2021[2]).

In particular, the provisions or mechanisms used or recognised by unilateral policies and regulations can be grouped into two main categories:

(a) 'Open safeguards' that rely primarily on the transferring entity to ensure the continued protection of the public policy objectives involved without being generally prescriptive as to how these requirements must be met.

'Open safeguards' include, for instance, provisions such as the ex-post accountability principle, according to which data exporting entities must ensure that overseas recipients handle that data consistently with the requirements of local laws, or the general requirement for the transferring entity to put in place some form of contractual protection, or to assess the sufficiency of the level of protection after the transfer; and

(b) 'Pre-authorised safeguards' that are generally characterised by a greater involvement of the public sector ex-ante to ensure trusted data transfers. Such publicly 'pre-authorised safeguards' include, for instance, unilateral whitelisting of a recipient country by the public sector, the required incorporation into contracts of specific clauses pre-approved by the public sector (e.g., standard or model contractual clauses), or public sector's pre-approval of organisations' binding corporate rules, or domestic certification schemes whose operation is monitored directly (public certification scheme) or indirectly (public accreditation of private certifiers) by a public entity.

In recent years, an increasing number of countries have issued model or standard contractual clauses for cross-border data transfers as a type of 'pre-authorised safeguard' mechanism. Public authorities, in cooperation with Privacy Enforcement Authorities, have developed such contractual clauses that are in turn recommended or sometimes even required for contracts between entities seeking to share data across borders. When incorporated into contracts, these clauses are automatically considered as sufficient for a lawful transfer of data. Examples of countries that have developed such type of pre-approved contractual clauses include, among others (Robinson, Kizawa and Ronchi, 2021[3]):

- All European Economic Area's countries, through the European Commission's development of the recently modernised "Standard Contractual Clauses" (SCCs) (European Commission[4]);
- New Zealand's model contract clauses (Office of the Privacy Commissioner[5]);
- The United Kingdom's International Data Transfer Agreement (Information Commissioner's Office[6]); and
- Argentina's data protection contractual clauses (Ministry of Justice and Human Rights, Argentina[7]).

Testifying to the growing recognition of pre-approved contractual clauses as a useful tool to enable trusted cross-border data flows is the work undertaken also in some regional organisations to support their member countries to leverage this mechanism to achieve trusted cross-border data flows. In 2021, ASEAN published a set of Model Contractual Clauses for Cross-Border Data Transfers (ASEAN, 2021[8]). In the same year, the Ibero-American Data Protection Network adopted a resolution recognising the importance of SCCs as a transfer tool and triggering the adoption procedure for SCCs (RIPD, 2021[9]). Pre-approved contractual clauses are also a recognised instrument under the modernised version of the Council of Europe's Convention 108 (see Article 14(3) (b) (Council of Europe, 2018[10])).

3. Inter-governmental processes

A range of processes in inter-governmental fora have also taken place or are ongoing to help advance cooperation and enable trusted cross-border data flows. These include: deliberations by the G7 and the G20 (subsection 3.1); standard-setting efforts and research and analysis initiatives promoting dialogue in multilateral organisations (section 3.2); standard-setting or binding agreements among regional partners (section 3.3); and a variety of trade agreements of a preferential nature (section 3.4).

3.1 The G7 and G20 deliberations in the areas of Data Free Flow with Trust and cross-border data flows

For the past few years, the G7 and the G20 have increasingly emphasised the importance of promoting cross-border data flows in their deliberations.

In *2019,* at the World Economic Forum in Davos, Japanese Prime Minister Shinzo Abe first declared the launch of the 'Osaka Track' on Data Free Flow with Trust (DFFT), referring to a vision in which openness and trust in data flows co-exist and complement each other. That year, the Osaka Leaders' Declaration and G20 Ministerial Statement on Trade and the Digital Economy agreed to that concept and recognised that cross-border data flows raised "challenges related to privacy, data protection, intellectual property rights, and security" and agreed that "by continuing to collaborate on these challenges, we could further facilitate data free flow and strengthen consumer and business trust." They also agreed to cooperate to "encourage the interoperability of different frameworks".

In *2020*, the G20 Riyadh Leaders' Declaration re-affirmed agreement to "further facilitate data free flow and strengthen consumer and business trust".

In *2021*, the G7 Digital Track and Trade Tracks worked on the issue of DFFT. In April 2021, in the G7 Roadmap for Cooperation on Data Free Flow with Trust, G7 Digital and Technology Ministers recognised "the importance of unlocking the power of data in our economies and our societies, while continuing to address challenges related to privacy, data protection, intellectual property rights, and security." They also sought to draw upon "shared values as like-minded, democratic, open and outward looking nations to support a plan of work which realises the benefits of data free flow with trust." In parallel, the G7 Trade Ministers developed a set of digital trade principles, including about how "data should be able to flow freely across borders with trust, including the trust of individuals and businesses."

In *2021*, the G20 Rome Leaders' Declaration also acknowledged the importance of "data free flow with trust and cross-border data flows". Most notably, it expressed agreement 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."

Most recently, under the German G7 Presidency of 2022, G7 Digital and Technology Ministers declared "that [DFFT] underpins innovation, prosperity and democratic values." They also adopted a G7 Action Plan for Promoting Data Free Flow with Trust, expressing "commitment to strengthening the evidence base for DFFT, building on commonalities in order to foster future interoperability, continuing regulatory cooperation" and "promoting DFFT in the context of digital trade."

Building on this joint G7 aspiration, the G7 Digital Ministers also welcomed "the intention of the Japanese G7 Presidency in 2023 to continue work on the basis of this declaration on […] DFFT, including promoting regulatory cooperation for DFFT, in particular through round table discussions of data protection and privacy authorities."

The Financial Stability Board, a body established by the G7 and then G20 in 2009, has also recently concluded a survey seeking feedback on how existing national and regional data frameworks affect cross-border data flows and cross-border payments.

Overall, these developments signal consistent political commitment from G7 and G20 countries to collaboration to promote DFFT.

3.2 Multilateral approaches

Organisation for Economic Co-Operation and Development (OECD)

The OECD has long recognised the role that both cross-border data flows and trust play in the digital economy.

In the OECD's 2016 Ministerial Declaration on the Digital Economy (the Cancún Declaration), countries declared that they would "Support the free flow of information to catalyse innovation and creativity, support research and knowledge sharing, enhance trade and e-commerce, enable the development of new businesses and services, and increase people's welfare through policies, grounded in respect for human rights and the rule of law, that reinforce the Internet's openness, in particular its distributed and interconnected nature, while respecting applicable frameworks for privacy and data protection, and strengthening digital security" (OECD, 2016[11]).

The Cancún Declaration also underscored the need to adopt evidence-based policies to strengthen trust. In particular, it called "to promote digital security risk management and the protection of privacy, and to adopt policies and regulatory frameworks that strengthen consumer trust and product safety, to stimulate and help to reduce impediments to e-commerce" (OECD, 2016[11]).

In this context, the OECD work programme has focused on providing common frameworks on data governance to strengthen trust in the digital environment, either in the form of standards through OECD Council Recommendations, or in the form of analytical research and analysis.

OECD Council Recommendations

Several OECD Council Recommendations adhered to by member countries and partner economies provide high-level, actionable and result-oriented principles on data governance issues, while accommodating the differences between countries' regulatory systems and institutional set-up. By doing so, they promote coherence of regulatory frameworks in different countries. The process to develop these instruments, and periodically review them, also entails discussions and knowledge exchange at the international level, which can help to foster trust beneficial to promoting cross-border data flows. An overview of key OECD Council Recommendations in this area is provided in Box 1.

Box 1. Key OECD Council Recommendations contributing to trusted cross-border data flows

a. ***OECD Recommendation of the Council Concerning Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*** (2013[12]) (OECD/LEGAL/0188)

The OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Data were the first internationally agreed-upon set of privacy principles. The Guidelines were a response to two interrelated trends: a recognition of the importance of information – including personal information – in the global economy; and emerging concerns about the possible impact on the rights of individuals resulting from the automated processing of personal information made possible by the first generation of computer technology. Principle-based and technology-neutral, the Guidelines have served as an important guide and reference point for policy makers as they develop their privacy frameworks, helping to foster coherence and therefore trust when data crosses borders (OECD, 2013[12]).

b. ***OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy*** (2007[13]) (OECD/LEGAL/0352)

Changes in the character and volume of cross-border data flows have elevated privacy risks for individuals and highlighted the need for better co-operation among the authorities charged with providing them protection. This Recommendation reflects a commitment by governments to improve their domestic frameworks for privacy law enforcement to enable their privacy enforcement authorities to co-operate with foreign authorities, as well as to provide mutual assistance to one another in the enforcement of privacy laws, to foster trust in cross-border data flows.

c. ***OECD Recommendation on Enhancing Access to and Sharing of Data*** (2021[14]) (OECD/LEGAL/0463)

The OECD Recommendation on Enhancing Access to and Sharing of Data (EASD) is the first internationally agreed upon set of principles and policy guidance on how governments can maximise the cross-sectoral benefits of all types of data – personal, non-personal, open, proprietary, public and private – while protecting the rights of individuals and organisations. The Recommendation intends to help governments develop coherent data governance policies and frameworks to unlock the potential benefits of data across and within sectors, countries, organisations, and communities. It aims to reinforce trust across the data ecosystem, stimulate investment in data and incentivise data access and sharing, and foster effective and responsible data access, sharing and use across sectors and countries.

d. ***OECD Recommendations on digital security***, including: OECD Recommendation on Digital Security Risk Management for Economic and Social Prosperity (2015[15]) (OECD/LEGAL/0415); OECD Recommendation on Digital Security of Critical Activities (OECD/LEGAL/0456) (2019[16]); OECD Recommendation concerning Guidelines for Cryptography Policy (OECD/LEGAL/0289) (1997[17]).

Digital security threats and incidents can lead to significant economic and social consequences, as well as to loss of trust among public and private organisations and individuals. These Digital security Recommendations aim to bridge the technical and policy level, and guide policy makers to develop digital security strategies and policies that foster trust and resilience, that support digital transformation, competitiveness and growth, and that protect critical activities, human rights and fundamental values in a coherent manner.

OECD's research and analysis work

The OECD also produces a range of analytical reports and continuously facilitates dialogue on important policy issues, including with a specific attention to the policy agenda of cross-border data flows.

OECD research and convening processes have contributed to the discussion on cross-border data flows throughout the years. Most recently, the work has sought to develop the evidence-base to foster trust, and facilitate international dialogue and cooperation in areas that are particularly relevant to enabling trusted cross-border data flows. This has mostly taken place in the context of a transdisciplinary project on Data governance for growth and well-being (OECD Going Digital Phase III for the 2021-2022 biennium).

In particular, this OECD work has highlighted the growing number of measures affecting cross-border data flows and provided a taxonomy of approaches (Casalini and López González, 2019[18]). It has also identified commonalities across the different instruments for moving data across borders with a view to helping countries identify areas for potential collaboration (Casalini, López-González and Nemoto, 2021[2]). It then conducted a deep-dive on issues around ensuring the interoperability of privacy and data protection frameworks specifically, highlighting promising initiatives by governments and privacy enforcement authorities at the national and international levels to foster trust (Robinson, Kizawa and Ronchi, 2021[3]). The OECD has also been hosting

an effort to articulate shared principles on government access to personal data held by the private sector (CDEP, 2020[19]), which may represent a critical step to recognise commonalities in this respect where they exist and in doing so, complement other cooperation efforts to foster trust in data flows.[1]

Moreover, in the context of the review of the OECD Privacy Guidelines, work on data localisation has emphasised the need to recognise the effect that data localisation has on transborder data flows (Svantesson, 2020[20]). An exercise mapping data localisation measures then highlighted the rise in data localisation measures and their increasing restrictiveness (Lopez-Gonzalez, Casalini and Porras, 2022[21]).

Work at the OECD is also ongoing to help policy-makers navigate the role of privacy enhancing technologies (PETs) for data governance and stimulate international knowledge sharing in this area. Finally, there is also work at the OECD to improve the measurement of data, including efforts to quantitatively assess the effects of cross-border data policy options, including data localisation, with respect to different policy objectives (such as economic activity and trust) to inform policy discussions in the future.

United Nations (UN)

The United Nations (UN) is contributing to the discussion and has processes in place that are relevant to fostering trusted cross-border data flows.

The United Nations Conference on Trade and Development (UNCTAD)'s Digital Economy Report of 2021 addressed the issue of "Cross-border data flows and development: For whom the data flow". The Report found that the state of the international debate on how to regulate cross-border data flows was at an impasse, as positions tend to be polarised, with strong influences from the major economic powers. Moreover, global digital corporations are seeking to expand their own data ecosystems. In spite of the risk of fragmentation, this report also found that there are some signs of possible convergence among the main data realms. While the Report did not seek to provide an all-encompassing solution, it called for moving away from the silo approach towards a more holistic, coordinated global approach, including via new and innovative ways of global governance (UNCTAD, 2021[22]).

Implementing this approach, in 2022 the UN Committee of Experts on Big Data and Data Science for Official Statistics launched a UN PET Lab that has the specific aim to pilot a programme that would make international data sharing more secure by using PETs. The UN PET Lab will bring together statistical bodies to collaborate with technology providers that offer PET technologies to test solutions to transfer data across borders compliantly. The US Census Bureau, Statistics Netherlands, the Italian National Institute of Statistics, and the UK's Office for National Statistics are involved in the project (UN Stats, 2022[23]).

World Trade Organisation (WTO)

Since 2017, the WTO has focused its attention on trade-related aspects of e-commerce, under the heading of "Joint Statement Initiative on E-Commerce" (WTO, 2017[24]). As of May 2022, 86 WTO members representing over 90% of global trade, have been participating in the negotiations. According to a statement released in December 2021, text was being negotiated to

[1] In 2021 the Global Privacy Assembly, a forum of over 100 data protection authorities, adopted a resolution advocating for a set of principles to be applied for government access to personal data held by the private sector for national security and public safety purposes (Global Privacy Assembly, 2021[58]).

establish disciplines on cross-border data flows, recognised as a key building block for a high-standard and commercially meaningful outcome (WTO, 2021[25]).

In relation to this, a joint Industry Statement on Cross-Border Data Transfers and Data Localization Disciplines in the WTO Negotiations on E-Commerce released in January 2021 encourages WTO negotiators to agree on a framework to facilitate the seamless and secure movement of information across borders (ICC, 2021[26]).

World Bank

The World Bank's "World Development Report 2021: Data for Better Lives" sought to answer questions about the governance arrangements that are needed to support the generation and use of data in a safe, ethical, and secure way, while also delivering value equitably.

In relation to cross-border data flows specifically, the report argued that the expanding role of data in ubiquitous platform business models is reshaping competition, trade, and taxation in the real economy, posing important risks for low- and middle-income countries. On that basis, the report called for internationally coordinated action—on antitrust enforcement, regulation of platform firms, data standards, trade agreements, and tax policy—to ensure efficient, equitable policies for the data economy that respond to countries' needs and interests (World Bank, 2021[27]).

3.3 Regional arrangements

Regional arrangements have also addressed the issue of cross-border data flows. In particular, the Asia-Pacific Economic Cooperation (APEC), the Association of Southeast Asian Nations (ASEAN), the European Union (EU)[2], and the Council of Europe are key regional entities where G7 members are involved that have developed regional standards or binding agreements to promote trusted cross-border data flows among their members and beyond.

The **APEC**[3] Privacy Framework (originally developed in 2005 and modelled upon the OECD Privacy Guidelines) sets out the APEC information privacy principles and it provides guidance for their domestic and international implementation. Updated in 2015 to reflect the 2013 revisions to the OECD Privacy Guidelines, the APEC Privacy Framework calls on member economies to give practical effect to the Framework, including by encouraging and supporting the development of international arrangements that promote interoperability among the respective privacy instruments.

The APEC Privacy Framework also forms the basis for the APEC Cross-border Privacy Enforcement Arrangement (CPEA) and the APEC Cross-Border Privacy Rules (CBPR) System. The APEC CBPR System, which has been in place since 2011, is a framework developed by APEC economies to promote the interoperability of privacy regulation through enforcement of minimum standards. The CBPR System is not mandatory for APEC economies, and once an economy has adhered to the System, companies can choose whether to seek certification under

[2] EU's regulations are considered as an inter-governmental effort for the purpose of this exercise. However, in light of the involvement of the European Commission in the initiation and the European Parliament in the approval of these regulations, and the unique nature of the EU legislation and integration process more broadly, EU's regulations may be regarded as a *sui-generis* inter-governmental effort.

[3] APEC's member economies are: Australia; Brunei Darussalam; Canada; Chile; People's Republic of China; Hong Kong (China); Indonesia; Japan; Korea; Malaysia; Mexico; New Zealand; Papua New Guinea; Peru; Philippines; Russian Federation; Singapore; Chinese Taipei; Thailand; United States; Viet Nam.

the System (cbrs.org[28]). To date, seven of the twenty-one APEC economies are participating in the System and in April 2022, the participating economies have launched a Global CBPR Forum to establish the Global Cross Border Privacy Rules (CBPR) and Privacy Recognition for Processors (PRP) Systems. These would be data privacy certifications that help companies demonstrate compliance with internationally recognised data privacy standards (U.S. Department of Commerce, 2022[29]).

The **ASEAN**[4] Framework on Personal Data Protection serves to strengthen the protection of personal data in ASEAN countries and to facilitate cooperation among participants in the Framework. The Framework does not create legally binding domestic or international obligations, but it encourages participating economies to endeavour to cooperate, promote, and implement the privacy principles set out in the Framework while continuing to ensure and facilitate the free flow of information among ASEAN Member States (ASEAN, 2016[30]; ASEAN, 2018[31]).

In January 2021 the ASEAN's first Digital Ministers' Meeting (ADGMIN) also approved the ASEAN Data Management Framework (DMF) (ASEAN, 2021[32]) and Model Contractual Clauses for Cross Border Data Flows (MCCs) (ASEAN, 2021[8]). The initiatives were developed by the Working Group on Digital Data Governance chaired by Singapore.

In particular, the ASEAN MCCs are key resource and tool for ASEAN businesses. The MCCs are template contractual terms and conditions that may be included in the binding legal agreements between businesses transferring personal data to each other across borders. This helps to reduce the negotiation and compliance cost and time, especially for SMEs, while ensuring personal data protection when data is transferred across borders (ASEAN, 2021[33]).

In the EU, arguably the most ambitious attempt to establish trusted cross-border data flows has taken place with the adoption of the General Data Protection Regulation (GDPR). The GDPR establishes mandatory rules for how organisations and companies can process personal data and is directly applicable in all countries participating in the European Economic Area (EEA). This means that data protection law is virtually harmonised across countries where the regulation applies, by virtue of which free flow of data is ensured among them. GDPR also establishes common rules to govern transfers from EEA countries to third (non-EEA) countries, including through mechanisms such as adequacy decisions, standard contractual clauses or binding corporate rules, among others (European Union, 2016[34]).

In 2018, the EU also adopted a Regulation on a framework for the free flow of non-personal data in the European Union, which provides for companies and public administrations to store and process non-personal data wherever they choose in the EU, prohibiting for its member countries to impose data localisation requirements (i.e. obligations to store data domestically), except when a restriction or a prohibition is justified by public security reasons. This is based on the agreement that competent authorities will be able to access data in any EU member state, in accordance with Union or national law, and they cannot be refused access to data on the basis that data are processed in another Member State (European Union, 2016[35]).

In 2022, the EU Data Governance Act (DGA) has come into force. The DGA regulates the processing of electronic data, whether personal or not, with the aim to harmonise data governance among Member States and thereby ensure the free flow of all types of data among them. It sets up mechanisms to facilitate the reuse of certain categories of protected public-sector data and fosters instruments such as data intermediation services and data altruism. Notably, it provides rules for data transfers to third countries, including envisaging mechanisms such

[4] ASEAN Member States are: Brunei Darussalam; Cambodia; Indonesia; Lao People's Democratic Republic; Malaysia; Myanmar; Philippines; Singapore; Thailand; Viet Nam.

adequacy decisions and standard contractual clauses for non-personal data (European Commission, 2020[36]).

Finally, the 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, commonly referred to as **Convention 108 of the Council of Europe**, is a treaty protecting the right to privacy of individuals with respect to personal data that are automatically processed (Council of Europe[37]). To date, fifty-three states, mostly European but also beyond, have committed to establish, under their own domestic law, sanctions and remedies for violations of the Convention's provisions.

Convention 108 establishes that states that are signatories to the Convention could not restrict the free flow of personal data between each other. Conversely they were to allow transfers to non-signatory countries only where an adequate level of protection was ensured in the recipient entity or where safeguards were in place (Council of Europe, 2001[38]).

A modernised Convention, commonly referred to as "C108+", was adopted by the Committee of Ministers on 18 May 2018 and opened for signature on 10 October 2018. When it will enter into force, it will repeal the 2001 Additional Protocol. The new Protocol of 2018 still provides that States that are party to the Convention should not restrict the flow of personal data among themselves. Like the original Convention, exceptions apply to cases where there is a risk that the transfer could lead to the circumvention of the provisions of the Convention, and it provides an additional exception where a party is bound by harmonised rules of protection shared by States belonging to a regional international organisation (Council of Europe, 2018[10]).

This means that when the 2018 Protocol enters into force the signatories to the Convention will not be bound to ensure the free flow of data between each other if one of the exceptions apply. The newly introduced exception, for example, applies to the Member States of the European Union. However recitals of the EU's GDPR suggest that a third country's accession to Convention 108 and its implementation would be an important factor when applying the European Union's international transfer regime, in particular when assessing whether the third country offers an adequate level of protection (Official Journal of the European Union, 2016[39]).

3.4 Preferential trade agreements

In parallel to the endeavours discussed above, multiple preferential trade and digital economy agreements are increasingly addressing issues around cross-border data flows and trust (in the context of both personal and non-personal data). Since 2008, and up to December 2020, 29 agreements involving 72 economies have introduced some form of data flow provisions (Casalini, López-González and Nemoto, 2021[2]).

At the same time, the depth of these provisions varies among agreements. Around half of these 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) (sice.oas.org[40]; sice.oas.org[41]). The other half, most of which signed in the last five years, contains binding commitments on data flows (of all types of data) – with notable cases being the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP)[5] (New Zealand Ministry of Foreign Affairs and Trade[42]), the United States, Mexico, and Canada Agreement (USMCA) and the EU-UK Trade and Cooperation Agreement.

[5] Parties to CPTPP are: Canada, Australia, Brunei, Chile, Japan, Malaysia, Mexico, New Zealand, Peru, Singapore and Viet Nam.

Almost all of these agreements also include exceptions allowing parties to restrict data flows to meet "legitimate public policy objectives" and most notably, all these include provisions on the need for domestic privacy legislation (including references to the inter-governmental arrangements outlined above).

In this sense, 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 inter-governmental arrangements.

Recently, 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".

Relatedly, these agreements increasingly include provisions prohibiting requirements that computing facilities be located domestically as a condition for conducting business, such as in the case for CPTPP (see Article 14.13) and USMCA (see Article 19.12), among others (Nemoto and López González, 2021[43]).

In parallel, countries have also started negotiating broader digital economy agreements (DEAs) which 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. For example, the United Kingdom and Singapore have signed a Digital Economy Agreement (UKSDEA) in 2022 (mti.gov.sg, 2022[44]).

4. Technological and organisational measures

While different entities hold vast amounts of data, they and other companies, organisations, individuals, and governments may not always be drawing the most benefit from that data due to issues of trust, incentives that prevent data sharing, or other operational issues that prevent finding and accessing data strategically, especially across borders.

Recognising this need, a range of technological and organisational measures have started being developed to help to overcome some of those issues, breaking silos between organisations, sectors and countries. Various types of technological and organisational measures exist, that can also be complementary between them to achieve more secure data access and sharing.

In particular, 'data intermediaries' have emerged. The term 'data intermediary' is not universally defined and stocktaking exercises about data intermediaries may indeed suffer from terminological inconsistency and vagueness (Wernick, Olk and Von Grafenstein, 2020[45]). Broadly speaking, they can be understood as a loosely defined category of actors brokering the relationship between actors sharing data and those accessing data through technical and organisational means, facilitating if not enhancing the use and re-use of data across societies (World Economic Forum, 2022[46]; Centre for Data Ethics and Innovation, 2021[47]; OECD, 2019[48]).

Data intermediaries may refer to organisations that work through a centralised or decentralised approach. Centralised approaches range from entities that provide analytical services in siloed environments, to organisations that act as mediators negotiating sharing arrangements, to organisations managing access rights and ensuring compliance with relevant data protection regulations, or to organisations offering as-a-service new technological solutions for sharing

data[6]. For example, some data intermediaries of this kind leverage PETs to enable sensitive data to be more widely utilised, or to enable data to be accessed in a more privacy-focused way, allowing stakeholders to extract relevant information from a dataset without gaining access to the raw data (Centre for Data Ethics and Innovation, 2021[47]; OECD, 2019[48]).

This section focuses on data spaces as one type of decentralised data intermediary for promoting cross-border data flows.

4.1 Data spaces

An innovative approach known as "data spaces" or "data industrial platforms" is gaining momentum as an option to overcome some of the challenges related to sharing data, including across borders, especially with respect to "industrial" or "non-personal" data.

Data spaces are a system where data is shared based on standards that are open and transparent with the objective to enable cooperation, lower barriers to entry, and promote innovation in the digital economy (GAIA-X, 2019[49]; International Data Spaces Association, 2022[50]).

Examples of data spaces in recent years include:

- Gaia-X is a European initiative to develop a software framework of control and governance and implement a common set of policies and rules to be applied to any existing cloud/ edge technology stack to obtain transparency, controllability, portability and interoperability across data and services. The framework is meant to be deployed on top of any existing cloud platform that adheres to the Gaia-X standard. Through this standard, the aim is to establish an ecosystem in which data is made available, collated and shared in a trustworthy environment, where generators of data maintain full control and visibility on the context and purpose for which other actors access data. However, Gaia-X is not conceived to be a market operator, nor will it operate directly or exclusively any of the services required by the framework. Gaia-X services are to be created, operated, and adopted by the market through operators voluntarily deciding to adopt the Gaia-X standard (GAIA-X, 2019[49]).
    - A first example of application of Gaia-X is Catena-X. Catena-X plans to organise itself as a registered association in Germany. Catena-X sees itself as an extensible ecosystem in which automotive manufacturers and suppliers, dealer associations and equipment suppliers, including the providers of applications, platforms and infrastructure, can all participate equally. The purpose of the association is to create a uniform standard for information and data sharing throughout the entire automotive value chain (Catena-X, 2022[51]).
- The International Data Spaces (IDS) Association, a coalition of over 130 companies, developed an open standard for data platforms that could be used for the development of specific data spaces. In particular, the IDS aims to enable new "smart services" and innovative business processes to work across companies and industries while ensuring that the self-

[6] The following may be considered as sub-categories of data intermediaries including centralised approaches such as data trusts, data custodians, trusted or certified third parties, or decentralised approaches such as industrial data platforms, data spaces, personal information management systems (PIMS), data sandboxes, data cooperatives, data collaboratives; although these terms may sometimes be used interchangeably or one term may refer to an actor fulfilling multiple intermediary roles. This list is non-exhaustive and other types of data intermediaries may emerge with ongoing and fast developments in this area.

determined control of data use (data sovereignty) remains in the hands of data providers (International Data Spaces Association, 2022[50]).

- Following up on the European strategy for data of 2020, possibilities of development of data spaces have also picked up speed in the context of the European Data Act proposal published by the European Commission in February 2022 ("Proposal for a Regulation on harmonised rules on fair access to and use of data"). According to the proposal, key features of a common European data space would include:
  - A secure and privacy-preserving infrastructure to pool, access, share, process and use data;
  - A clear and practical structure for access to and use of data in a fair, transparent, proportionate and non-discriminatory manner and clear and trustworthy data governance mechanisms;
  - European rules and values, in particular personal data protection, consumer protection legislation and competition law, are fully respected;
  - Data holders will have the possibility, in the data space, to grant access to or to share certain personal or non-personal data under their control;
  - Data that is made available can be reused against compensation, including remuneration, or for free;
  - Participation of an open number of organisations/ individuals.

  These, potentially sectoral, data spaces would for example contribute to the green transition by improving the management of energy consumption, enabling the delivery of personalised medicine, and facilitating access to public services. Several priority sectors for data spaces in Europe have already been identified, including green economy, smart communities, mobility, and health, among others (European Commission, 2022[52]; European Commission, 2022[53]).

- The Data Society Alliance (DSA), a coalition of industry, academia and the public sector in Japan, has established DATA-EX, a platform to promote and facilitate data exchange between different domains such as education, agriculture, disaster risk management, healthcare, infrastructure and smart city. DATA-EX is developed and operated by DSA in close collaboration with the government (Office of IT, Cabinet Secretariat, 2021[54]).
- A Japan Data Exchange Inc. (JDEX) has also been established in Japan as a private sector led initiative to create a large data trading community in the country, spanning across industry, academia, and government, and contribute to the promotion of a cross-industry and cross-border data exchange environment. According to the platform's website, the platform, relying on Dawex Data Exchange technology and operated by Kanematsu, will serve multinational trading corporations' domestic and foreign networks. The JDEX platform would thus enable the sourcing, exchange, sharing and commercialisation of data products leveraging the platform's features and capabilities (JDEX, 2022[55]).
- The Data Exchange Association (DXA) is a global non-profit association that brings together public and private organisations to accelerate cross-sector, cross-border data exchanges while developing decisive standards. To achieve these objectives, DXA is taking various steps, including creating a training and certification program to allow organisations to assess their maturity and compliance to the common standards and best practices of data exchange (DXA, 2022[56]).

Overall, the common feature of “data spaces” is the aim to bring together data providers, users and intermediaries, increasing interoperability and trust to enhance data sharing across entities and individuals. This can apply horizontally across sectors, as well as vertically within sectors.

At a technical level, data spaces rely on common standards for pooling, or linking, accessing, processing, using and sharing data between different endpoints. They are based on a shared understanding of data governance and data-related policy objectives (for example, relating to privacy and security) (International Data Spaces Association, 2022[50]).

Depending on their functioning, data intermediaries may be more or less relevant to enabling trusted cross-border data flows. Data spaces depend on common rules developed for the space that allow overcoming legal and technical barriers to data sharing across organisations, achieving trust through technical, semantic, organisational, and legal interoperability (European Commission, 2022[53]). It logically follows that a key condition for data spaces to scale internationally is coherence among the data governance frameworks in the countries where participants in the data space are located. The shared ambition of governments for “data free flow with trust” could thus drive them to promote international data spaces as an additional tool towards this objective.

5. Conclusion

Data and their flow across borders is critical to realising the potential of digital technologies for thriving digital economies and societies, enabling the development of new and innovative business models and enhancing traditional ones that depend on moving and aggregating data around the world. In this context, maintaining a high degree of trust in cross-border data flows for businesses, citizens and societies is key to realising the benefits of digital transformation for our global economy while upholding high data protection standards.

The stocktaking of key policies and initiatives seeking to promote trusted cross-border data flows provided in this report aims to offer a basis for G7 countries to continue advancing on this policy priority in a coordinated and coherent manner.

This report identifies key efforts at the unilateral, inter-governmental and technological and organisational level that are underway to help advance the cross-border data flows agenda. These efforts have: supported a better understanding of the current policy landscape; started to develop an architecture for trusted cross-border data flows including through common standards, mechanisms and provisions where possible; and consistently called for governments to step up their cooperation efforts to promote cross-border data sharing in a trusted manner. In this sense, these efforts are largely complementary to one another.

In the future, it will be useful to continue improving the understanding of the concrete barriers for moving data across borders. This will be critical to support well-informed efforts on measures that may help to overcome those barriers, and to orient future international cooperation towards the design of an enabling policy environment that offers practical solutions to promote trusted cross-border data flows.

Advancing this understanding among G7 countries, and beyond, will be crucial to support future policy and regulatory approaches that leverage the full potential of data for global economic and social prosperity.

References

(n.a.) (n.d.), *「DATA-EX」の取り組み – 一般社団法人データ社会推進協議会(DSA)*, https://data-society-alliance.org/data-ex/ (accessed on 29 April 2022). [59]

ASEAN (2021), "ASEAN Data Management Framework", https://asean.org/wp-content/uploads/2021/08/ASEAN-Data-Management-Framework.pdf. [32]

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. [8]

ASEAN (2021), "Implementing Guidelines for ASEAN Data Management Framework and Cross Border Data Flows", https://asean.org/wp-content/uploads/2021/08/Implementing-Guidelines-for-ASEAN-Data-Management-Framework-and-Cross-Border-Data-Flows.pdf. [33]

ASEAN (2018), "ASEAN Framework on Digital Data Governance", https://asean.org/wp-content/uploads/2012/05/6B-ASEAN-Framework-on-Digital-Data-Governance_Endorsedv1.pdf. [31]

ASEAN (2016), "ASEAN Framework on Personal Data Protection", https://asean.org/wp-content/uploads/2012/05/10-ASEAN-Framework-on-PDP.pdf. [30]

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. [18]

Casalini, F., J. López-González and T. Nemoto (2021), *Mapping commonalities in regulatory approaches to cross-border data transfers*, https://doi.org/10.1787/ca9f974e-en (accessed on 3 March 2022). [2]

Catena-X (2022), *Catena-X Automotive Network*, https://catena-x.net/de/. [51]

cbrs.org (n.d.), *Cross Border Privacy Rules System*, http://cbprs.org/ (accessed on 22 April 2022). [28]

CDEP (2020), "DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INNOVATION COMMITTEE ON DIGITAL ECONOMY POLICY Statement of the Committee on Digital Economy Policy", http://www.oecd.org/digital/trusted-government-access- (accessed on 25 April 2022). [19]

Centre for Data Ethics and Innovation (2021), *Unlocking the value of data: Exloring the Role of Data Intermediaries*, 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- [47]

of-data-intermediaries.

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. [10]

Council of Europe (2001), *Protocol 2011*. [38]

Council of Europe (n.d.), *1981 Convention for the Protection of Individuals with regard to Automatic Porcessing of Personal Data*. [37]

dfat.gov.au (2020), *Australia-Singapore Digital Economy Agreement*, https://www.dfat.gov.au/sites/default/files/australia-singapore-digital-economy-agreement.docx. [61]

DXA (2022), *Data Exchange Association*, https://www.dataexchange-association.org/ (accessed on 22 April 2022). [56]

European Commission (2022), *COMMISSION STAFF WORKING DOCUMENT on Common European Data Spaces*, https://ec.europa.eu/newsroom/dae/redirection/document/83562. [53]

European Commission (2022), *Data Act: measures for a fair and innovative data economy*, https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113 (accessed on 22 April 2022). [52]

European Commission (2020), "REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on European data governance (Data Governance Act)", https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R0868&qid=1661868250374 (accessed on 28 April 2022). [36]

European Commission (n.d.), "Standard Contractual Clauses (SCC)", https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en (accessed on November 2021). [4]

European Union (2016), *General Data Protection Regulation (GDPR) Compliance Guidelines*, https://gdpr.eu/ (accessed on 28 April 2022). [34]

European Union (2016), *Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union (Text with EEA relevance.)*, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1807. [35]

GAIA-X (2019), *GAIA-X - Home*, https://www.data-infrastructure.eu/GAIAX/Navigation/EN/Home/home.html (accessed on 22 April 2022). [49]

Global Privacy Assembly (2021), "43rd Closed Session of the Global Privacy Assembly", https://ico.org.uk/media/about-the-ico/documents/4018242/g7-attachment-202109.pdf (accessed on 28 April 2022). [58]

ICC (2021), *Multi-Industry Statement on Cross-Border Data Transfers and Data Localization Disciplines in WTO Negotiations on E-Commerce*, https://iccwbo.org/publication/multi-industry-statement-on-cross-border-data-transfers-and-data-localization-disciplines-in-wto-negotiations-on-e-commerce/. [26]

Information Commissioner's Office (20222), *International Data Transfer Agreement*, [6]

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance/.

International Data Spaces Association (2022), *International Data Spaces*, https://internationaldataspaces.org/ (accessed on 22 April 2022). [50]

JDEX (2022), *Japan Data Exchange Inc.*, https://j-dex.co.jp/en/index.html (accessed on 22 April 2022). [55]

Lopez-Gonzalez, J., F. Casalini and J. Porras (2022), "A preliminary mapping of data localisation measures", *OECD Trade Policy Papers N. 262, OECD Publishing, Paris*. [21]

mfat.gov.nz (2020), *Digital Economy Partnership Agreement*, https://www.mfat.govt.nz/assets/Trade-agreements/DEPA/DEPA-Signing-Text-11-June-2020-GMT-v3.pdf. [60]

Ministry of Justice and Human Rights, Argentina (n.d.), "Dirección Nacional de Protección de Datos Personales", http://servicios.infoleg.gob.ar/infolegInternet/anexos/265000-269999/267922/norma.htm. [7]

mti.gov.sg (2022), *UK - Singapore Digital Economy Agreement*, https://www.mti.gov.sg/-/media/MTI/Microsites/DEAs/UKSDEA/Text-of-the-UKSDEA/2022-02-25---UK-Singapore-Digital-Economy-Agreement.pdf. [44]

mti.gov.sg (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. [62]

Nemoto, T. and J. López González (2021), "DIGITAL TRADE INVENTORY RULES, STANDARDS AND PRINCIPLES OECD TRADE AND AGRICULTURE DIRECTORATE Digital Trade Inventory: Rules, Standards and Principles". [43]

New Zealand Ministry of Foreign Affairs and Trade (n.d.), *Comprehensive and Progressive Agreement for Trans-Pacific Partnership text and resources*, https://www.mfat.govt.nz/vn/trade/free-trade-agreements/free-trade-agreements-in-force/comprehensive-and-progressive-agreement-for-trans-pacific-partnership-cptpp/comprehensive-and-progressive-agreement-for-trans-pacific-partnership-text-and-resources/ (accessed on 22 April 2022). [42]

OECD (2021), *Recommendation of the Council on Enhancing Access to and Sharing of Data*. [14]

OECD (2020), *https://www.oecd.org/digital/trusted-government-access-personal-data-private-sector.htm*. [57]

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. [1]

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. [48]

OECD (2019), *Recommendation of the Council on Digital Security of Critical Activities*. [16]

OECD (2016), *MINISTERIAL DECLARATION ON THE DIGITAL ECONOMY: INNOVATION,* [11]

GROWTH AND SOCIAL PROSPERITY ("CANCÚN DECLARATION"), https://www.oecd.org/digital/Digital-Economy-Ministerial-Declaration-2016.pdf (accessed on 7 April 2022).

OECD (2015), *Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity*, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0415. [15]

OECD (2013), *Recommendation of the Council Concerning Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188. [12]

OECD (2007), *Recommendation of the Council on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy*, https://www.oecd.org/sti/ieconomy/38770483.pdf. [13]

OECD (1997), *Recommendation of the Council concerning Guidelines for Cryptography Policy*. [17]

Office of IT, Cabinet Secretariat (2021), "National Data Strategy". [54]

Office of the Privacy Commissioner (n.d.), "Model contract clauses for sending personal information overseas", https://privacy.org.nz/blog/model-contract-clauses-for-sending-personal-information-overseas/ (accessed on November 2021). [5]

Official Journal of the European Union (2016), *REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC*, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679. [39]

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. [9]

Robinson, L., K. Kizawa and E. Ronchi (2021), "Interoperability of privacy and data protection frameworks", *Going Digital Toolkit Note, No. 21*, http://goingdigital.oecd.org/data/notes/No21_ToolkitNote_PrivacyDataInteroperability.pdf (accessed on 3 March 2022). [3]

sice.oas.org (n.d.), *Trade Agreements: Peru-Korea Free Trade Agreement*, http://www.sice.oas.org/tpd/per_kor/per_kor_texts_e/per_kor_toc_e.asp (accessed on 22 April 2022). [40]

sice.oas.org (n.d.), *Trade Policy Developments: Central America - Mexico*, http://www.sice.oas.org/tpd/CACM_MEX/CACM_MEX_e.asp (accessed on 22 April 2022). [41]

Svantesson, D. (2020), "Data localisation trends and challenges: Considerations for the review of the Privacy Guidelines", *OECD Digital Economy Papers, No. 301*, https://doi.org/10.1787/7fbaed62-en. [20]

U.S. Department of Commerce (2022), *Statement by Commerce Secretary Raimondo on Establishment of the Global Cross-Border Privacy Rules (CBPR) Forum*, https://www.commerce.gov/news/press-releases/2022/04/statement-commerce-secretary-raimondo-establishment-global-cross-border (accessed on 2022). [29]

UN Stats (2022), *UN launches first of its kind 'privacy lab' to unlock benefits of international data* [23]

sharing.

UNCTAD (2021), *DIGITAL ECONOMY REPORT 2021 - Cross-border data flows and development: For whom the data flow*, https://unctad.org/system/files/official-document/der2021_overview_en_0.pdf (accessed on 7 April 2022). [22]

Wernick, A., C. Olk and M. Von Grafenstein (2020), "Defining Data Intermediaries", *Technology and Regulation*, Vol. 2020, pp. 65-77, https://doi.org/10.26116/TECHREG.2020.007. [45]

World Bank (2021), *World Development Report 2021: Data for Better Lives*, https://wdr2021.worldbank.org/the-report/. [27]

World Economic Forum (2022), "Advancing Digital Agency: The Power of Data Intermediaries", https://www3.weforum.org/docs/WEF_Advancing_towards_Digital_Agency_2022.pdf (accessed on 22 April 2022). [46]

WTO (2021), "Statement by Ministers of Australia, Japan and Singapore", *Joint Statement Initiative on E-commerce*, https://www.wto.org/english/news_e/news21_e/ji_ecom_minister_statement_e.pdf. [25]

WTO (2017), "JOINT STATEMENT ON ELECTRONIC COMMERCE", *Ministerial Conference*, World Trade Organization, https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/WT/MIN17/60.pdf&Open=True (accessed on 7 April 2022). [24]