OECD GOING DIGITAL TOOLKIT

POLICY NOTE

Interoperability of privacy and data protection frameworks

OECD
BETTER POLICIES FOR BETTER LIVES

going digital

This Toolkit note was written by Lisa Robinson, Kosuke Kizawa and Elettra Ronchi. It was reviewed by the OECD Working Party on Data Governance and Privacy (DGP) and the OECD Committee on Digital Economy Policy (CDEP) and it was declassified by the CDEP on 8 December 2021. The note was prepared for publication by the OECD Secretariat.

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

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

#GoingDigital

Please cite this publication as:

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* .

Note to Delegations:

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

DSTI/CDEP/DGP(2020)15/FINAL.

Table of contents

Figures

Boxes

Interoperability of privacy and data protection frameworks

The significant increase in flows of personal data has spurred policy makers to try to develop a coherent approach to privacy governance both domestically and across borders. In this context, the need for the interoperability of privacy and data protection frameworks ("privacy interoperability") has taken on greater importance. While there is broad agreement on the importance of privacy interoperability, how to achieve this in practice is less well understood. This Going Digital Toolkit note describes the issues around ensuring the interoperability of privacy and data protection frameworks, and it highlights promising initiatives by governments and privacy enforcement authorities at the national and international levels. This note seeks to contribute to a shared understanding of privacy interoperability in the context of the governance of privacy and data protection and transborder flows of personal data.

As transborder flows of personal data have grown in volume and importance worldwide, policy makers are increasingly seeking to develop a coherent approach to privacy governance both domestically and across borders. Technology trends such as cloud computing, the Internet of Things (IoT), big data analytics, and artificial intelligence (AI), as well as organisational practices and business models based on the global collection, processing and commercialisation of personal data, have accentuated the cross-border dimensions of privacy and data protection, and the corresponding need for both international co-operation and the interoperability of privacy and data protection frameworks ("privacy interoperability").

This need for privacy interoperability was recognised at the OECD level as part of the 2013 revision of the OECD Recommendation concerning *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* (OECD Privacy Guidelines) (OECD, 1980[1]). At that time a greater emphasis was put on the interoperability of privacy and data protection frameworks. In particular, the "International Co-operation and Interoperability" section [Part Six] of the OECD Privacy Guidelines introduced new provisions (at paragraphs 20 and 21) calling for:

> *(i) encouragement and support of the* ***development of international arrangements that promote interoperability among privacy frameworks****, thereby giving practical effect to the Guidelines, together with (ii) appropriate measures to facilitate cross-border privacy law enforcement co-operation, in particular by enhancing information sharing among privacy enforcement authorities.* (emphasis added)

This revision aimed to encourage a more harmonious approach to global privacy governance, recognising that creating global cross-border transfer mechanisms and ensuring interoperability and mutual recognition between different privacy laws can help simplify compliance by organisations, and enhance individuals' and organisations' understanding of their rights in a global environment. It reflected the need for greater interoperability among privacy frameworks, particularly in the context of increased flows of personal data across global networks and jurisdictions (OECD, 2013[2]).

The widespread adoption of privacy and data protection legislation has continued since 2013 at both the OECD and global level, hand in hand with the growth in volume and importance of transborder flows of personal data. Today, all OECD countries[1] have data protection and privacy legislation in place (OECD, 2021[3]). Worldwide, as of April 2020, 66% of all countries (128 out of 194) had in place data protection or privacy legislation, with a further 10% of countries planning to introduce such legislation (UNCTAD, 2020[4]). Data protection and privacy legislation

[1] Australia, Austria, Belgium, Canada, Chile, Colombia, Costa Rica, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Israel, Italy, Japan, Korea, Latvia, Lithuania, Luxembourg, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, the Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Turkey, the United Kingdom, and the United States.

is also increasingly seen at the regional level, as well as throughout the Global South. For example, across both Africa and Asia, approximately 55% of countries have adopted such laws, as have 45% of the world's least developed countries (UNCTAD, 2020[4]). The number of data protection and privacy frameworks globally is likely also higher than the number of countries themselves, given that decentralised or federated countries may have more than one law covering these issues, or there may be rules for specific sectors, as is the case in the United States.

Whilst this global take-up of privacy and data protection legislation is important for both safeguarding individuals' privacy and enabling the free flow of data across borders, the number of privacy and data protection frameworks can present challenges for both public and private actors when navigating the digital economy, particularly when there is a need to transfer personal data across borders. Transactions which imply complying with more than one legal framework can create uncertainty regarding the applicable legal framework. Even where different privacy and data protection frameworks converge towards the same underlying principles, there may be certain differences in their practical application.

For many years, the importance of privacy interoperability in addressing these challenges has been stressed in high-level international fora (Box 1). At the OECD, since at least the 1980s the interest in privacy has not been limited to establishing common principles for effective protection of individuals and their privacy, but has also included promoting common international good practices and approaches to that protection so that data flows could take place with no detriment for privacy.

Box 1. Discussions on privacy interoperability in high-level international fora

In 2011, the G8 Deauville Declaration recognised the challenges in promoting interoperability and convergence on the protection of personal data and transborder data flows. Subsequently, as noted above, the 2013 revision to the OECD Privacy Guidelines placed an emphasis on the development of international arrangements that could promote interoperability among privacy frameworks. In 2016, as part of the OECD Declaration on the Digital Economy: Innovation, Growth and Social Prosperity (Cancún Declaration) (2016[5]), Ministers and Representatives of 42 countries plus the European Union[2] agreed to share experiences and work collaboratively to "support the development of international arrangements that promote effective privacy and data protection

[2] Argentina, Australia, Austria, Belgium, Canada, Chile, Colombia, Costa Rica, the Czech Republic, Denmark, Ecuador, Egypt, Estonia, the European Union, Finland, France, Germany, Greece, Hungary, Iceland, Indonesia, Ireland, Israel, Italy, Japan, Korea, Latvia, Lithuania, Luxembourg, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, the Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Turkey, the United Kingdom, and the United States.

across jurisdictions, including through interoperability among frameworks" (OECD, 2016[5]).

Similarly, in April 2017, the G20 Ministers[3] responsible for the digital economy agreed in their G20 Digital Economy Ministerial Declaration *Shaping Digitalisation for an Interconnected World* to "encourage the development of national privacy strategies while taking into account the different needs in countries [recognising] the importance of promoting interoperability between privacy frameworks of different countries" (G20, 2017[6]).

With the concept of data free flows with trust, championed by Japan under the G20 'Osaka Track', co-operation and interoperability were also stressed as major factors for building trust and facilitating the free flow of data. In particular, in the G20 (2019[7]) Ministerial Statement on Trade and Digital Economy, Ministers declared that "[they] will cooperate to encourage the interoperability of different frameworks" (G20, 2019[7]).

In 2020, building on the achievements and commitments of past Presidencies, G20 Digital Economy Ministers under the Saudi Presidency recognised "the need to address [the] challenges [raised by the free flow of data] in accordance with relevant applicable legal frameworks, which can further facilitate data free flow and strengthen consumer and business trust" (G20, 2020[8]). In this context, Ministers recognised "sharing experiences and good practices for data policy, in particular interoperability and transfer mechanisms" as means to address these challenges.

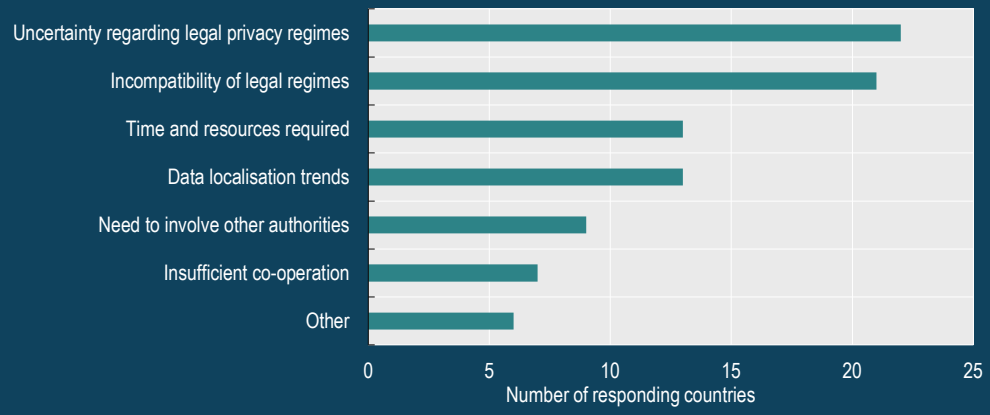
In 2021, as part of the G7 Digital and Technology Ministers Declaration (endorsing the G7 Roadmap for Cooperation on Data Free Flow with Trust), Ministers committed to promote "work to identify commonalities in regulatory approaches to cross-border data transfers, as well as good regulatory practices and cooperation between nations (and) interoperability between members" (G7, 2021[9]). At the same time, the G20 Digital Economy Ministers acknowledged on 5 August 2021 in Trieste the work of the OECD on Mapping Commonalities in Regulatory Approaches to Cross-border Data Transfers (OECD, 2021[10]) and the value in an approach which identifies the "commonalities, complementarities and elements of convergence" across different approaches. Such commonalities can foster future interoperability".

The important role of privacy interoperability for transborder flows of personal data was also reflected in responses to the survey underpinning the 2021 review of the OECD Privacy Guidelines (OECD, 2021[3]). When identifying the main challenges to

[3] The G20 comprises 19 countries plus the EU. These countries are Argentina, Australia, Brazil, Canada, the People's Republic of China ("China"), France, Germany, India, Indonesia, Italy, Japan, Korea, Mexico, the Russian Federation, Saudi Arabia, South Africa, Turkey, the United Kingdom and the United States.

transborder data flows, respondents to the OECD Privacy Guidelines Questionnaire[4] most often noted uncertainty regarding legal privacy regimes. This was followed by the incompatibility of legal regimes (Figure 1).[5]

Figure 1. Main challenges to transborder flows of personal data
OECD Countries, 2019



Note: This figure is based on the responses of 31 respondents to a questionnaire shared by the OECD Secretariat in 2019 on national and international developments and on the relevance of the OECD Privacy Guidelines.
***Source*:** Report on the Implementation of the Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (OECD, 2021[3]).

This Toolkit note sets out the importance of working towards global solutions that promote interoperability amongst privacy and data protection frameworks, whilst outlining existing challenges and promising initiatives by governments and privacy enforcement authorities (PEAs) at the national and the international level. It seeks to contribute to a shared understanding of "privacy interoperability" in the context of the governance of privacy and data protection and transborder flows of personal data. The note builds upon work carried out in the context of the review of the OECD Privacy Guidelines (OECD, 2021[3]) and, more specifically, analytical work on national privacy strategies and a Roundtable on Interoperability held in 2018 ('the May 2018 Roundtable') (OECD, 2021[3]).

[4] Australia, Brazil, Canada, Chile, Colombia, Denmark, Estonia, Finland, France, Germany, Iceland, Israel, Italy, Japan, Korea, Latvia, Lithuania, Luxembourg, Mexico, New Zealand, Norway, Poland, Portugal, Singapore, the Slovak Republic, Slovenia, Switzerland, Thailand, Turkey, the United Kingdom.

[5] It should be noted that the survey answer "incompatibility of legal regimes" can be ambiguous, as it is not clear which legal regimes respondents refer to (and in particular whether they refer to the regimes of adherents or non-adherents to the OECD Privacy Guidelines), and where that incompatibility lies.

What is interoperability of privacy and data protection frameworks?

Given the substantial legislative activity currently taking place in the area of personal data protection and privacy across the globe (OECD, 2021[10]), it is important to develop a shared understanding of the term. Firstly, it should be noted that the OECD Privacy Guidelines themselves or the Supplementary Explanatory Memorandum do not attempt to define privacy interoperability, although the latter provides examples of a range of initiatives undertaken to bring together different approaches to interoperability among privacy frameworks (OECD, 2013, p. 34[2]). The 2013 OECD Privacy Guidelines also recognise that while effective laws are essential, the strategic importance of privacy today also requires a multifaceted and coherent national policy strategy co-ordinated at the highest levels of government.

Expert discussions at the May 2018 Roundtable provided a jumping-off point for understanding the term. At this Roundtable, different concepts were discussed and put forward. For example, it was noted that the General Data Protection Regulation [Regulation (EU) 2016/679, "GDPR"] facilitates privacy interoperability through legislative harmonisation, allowing the flow of personal data within the European Union. Of note, "interoperability" was defined by some as the ability of various privacy regimes, or legal frameworks, to work together to facilitate transborder data flows while ensuring the consistent protection of these data (OECD, 2021, p. 55[3]). Another description considered interoperability to be a pragmatic arrangement to promote policy coherence in the context of a shifting regulatory environment and multiple privacy frameworks and data regulations (e.g. data localisation requirements). This is true particularly in the Asia-Pacific context, where jurisdictions display more divergences than countries in other regions (Box 2) (Asian Business Law Institute, 2020[11]).

Box 2. Data protection & privacy legal frameworks – The Asia-Pacific context

A growing number of Asia-Pacific countries have either introduced comprehensive privacy laws or plan to update their existing laws. Whilst there is a clear trend across the region for adopting such laws, there is significant variation amongst them.

A recent comparative study (Asian Business Law Institute, 2020[11]) of the data protection and privacy legal frameworks across the region (focusing on regulations and mechanisms in place to enable cross-border flows of data) reported significant differences with practical implications for organisations operating across borders.

These differences include:

1. The rationale and policy objectives underpinning the rules relating to cross-border data flows (e.g. access by law enforcement authorities);
2. The regulatory structures that impact the compliance process (e.g. whether the regime is 'consent-first', 'adequacy-first');
3. The coverage of legal mechanisms for cross-border data transfers (e.g. consent, adequacy decisions, contracts, binding corporate rules, certification, codes of conduct) available in each jurisdiction;
4. Approaches to implementation (e.g. some jurisdictions may be more prescriptive than others on how to obtain consent); and
5. Enforcement (some Asian countries lack financial resources, skills/expertise and have not yet established independent privacy enforcement authorities).

In addition, "data localisation" requirements and data transfer safeguards often co-exist in Asian data protection laws. The uncertainty over their interplay can be a source of confusion. To reduce fragmentation, the study calls for regional capacity building initiatives and a pan-Asian coordination mechanism to monitor regional developments and ensure convergence between the different legal frameworks.

The study shows there is, "potential for convergence in many transfer provisions of the data protection laws, in particular for interoperability of contracts, binding corporate rules, and certification (in multiple forms), and statutory exemptions".

Source: Asian Business Law Institute (2020[11]); GSM Association (2018[12]).

At the Roundtable, a general consensus emerged that "interoperable" does not necessarily mean identical, or even harmonised. As part of a recent mapping study conducted by the OECD, there is growing evidence of commonalities at the level of

principles across privacy legal regimes, largely reflecting the OECD Privacy Guidelines, and of convergence within and between legal instruments (OECD, 2021[10]). Nonetheless, the same study notes that "the emerging approaches to data regulation vary significantly across countries and types of data, reflecting differences in preferences for privacy and data protection and governments' pursuit of a range of other policy objectives" (OECD, 2021, p. 6[10]).

In the context of this report, and with the aim of progressing towards a shared definition, "privacy interoperability" can thus 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.

Why is privacy interoperability important?

The effective use of data can help boost productivity and improve or foster new products, processes, organisational methods and markets. Although there is still little reliable quantification of the economic effects of data use, firm-level studies suggest that firms that use data exhibit faster productivity growth than those that do not, by approximately 5% to 10% (OECD, 2015[13]; OECD, 2020[14]). In recent years, the scale and scope of data used by companies has changed and data have moved to the core of many business models[6]. Emerging technologies such as big data analytics and artificial intelligence have accelerated the growth of these new data-driven business models (OECD, 2020[14]). Furthermore, digital tools can help governments make better social policy choices and improve well-being, for example insight into the impact of policies on communities can be obtained by linking longitudinal and multi-domain data about individuals, families, and the environment (OECD, 2020[14]).

The increasing digitalisation of the global economy is not only driving data flows within countries, but also across borders (European Commission, 2017[15]). Cross-border data transfers enable businesses to build and maintain complex global value chains. In other words, the creation of economic value is often very much dependent on the ability to move and aggregate data across a number of locations scattered around the globe. The ability to transfer data internationally enables firms to effectively co-ordinate their research and development, supply chains, production, sales, and post-sales processes (US Department of Commerce, 2016[16]) (Casalini, 2019[17]).

[6] The Economist headlined that "The world's most valuable resource is no longer oil, but data" (The Economist, 2017[47]). This is underpinned by the fact that the most valuable companies nowadays include a number of technology giants that critically rely on intangible assets, including vast databases, to generate large shares of their revenue (e.g. Apple, Microsoft, Amazon, Alphabet, Meta (Facebook), and Alibaba).

These benefits of data flows for economies and societies require trust in the activities of different players operating in the digital space. Individuals will not engage with businesses they do not trust, and businesses will struggle to reap the benefits of scale unless they can operate globally.

Where there is a patchwork of rules and regulations, it is difficult both for policy makers to effectively enforce privacy and data protection goals across different jurisdictions, and also for firms to operate across markets (OECD, 2021[10]). At the same time, where there are limitations on cross-border data flows it is clear that, in many cases, impediments to international data transfers (which may be imposed for legitimate reasons such as data privacy concerns, or national security can have negative economic impacts on businesses and ultimately on complex value chains and trade.

The benefit of privacy interoperability is that it can serve to clarify the guiding principles for effective privacy and data protection in data transfers spanning jurisdictions and in particular clarify for businesses the legal requirements with which they need to comply. As the next sections highlight, there is great potential for privacy interoperability of some data transfer mechanisms in current privacy laws, which should be explored further Measures that foster and promote privacy interoperability can help promote convergence, reduce barriers to investment and reduce the transaction costs of transborder data flows due to the uncertainty over the applicable rules and regulations. As a consequence, interoperability can uphold a high level of trust also in transborder data flows.

Measures to foster and promote interoperability

To achieve privacy interoperability, joint international action is needed at multiple levels through policy and practical initiatives. Measures that can foster and promote the interoperability of privacy and data protection frameworks often rely on bilateral and multilateral approaches, as well as on regional and international co-operation. This can be at the level of principles, mutual recognition mechanisms, domestic legislative or regulatory actions, policy measures, and other initiatives (such as technical measures or certification schemes).

The following sections consider some of the most common measures that exist to foster and promote privacy interoperability. Firstly, bilateral and multilateral approaches are considered, including international and regional arrangements, mutual recognition and harmonisation, and initiatives involving the private sector. Thereafter, this note considers the role of privacy enhancing policy measures and cross-border enforcement co-operation.

Bilateral and multilateral approaches

Across the OECD, a number of bilateral and multilateral measures are currently in place. All OECD countries are parties to the OECD Privacy Guidelines, and in 2021

over 84% of countries[7] who participated in a review of their implementation are parties to at least one multilateral agreement or legal framework[8] to promote interoperability (OECD, 2021[3]). Likewise, in response to the 2017 OECD Digital Economy Outlook questionnaire, 26 out of 34 countries could name at least one initiative through which they co-operate internationally, support interoperability among privacy frameworks, and/or facilitate cross-border privacy law enforcement co-operation[9].

Below, three main types of measures which serve to foster and promote interoperability are considered in detail: 1) international and regional agreements; 2) harmonisation and mutual recognition; and 3) initiatives involving the private sector (i.e. model contract clauses, binding corporate rules (BCRs), the APEC Cross-Border Privacy Rules ("CBPR") System, BCR/CBPR Referential, codes of conduct, and private sector initiatives).

International and regional agreements

There are many different approaches within this category, each with different levels of enforceability. Non-binding multilateral agreements rely on "soft law" to encourage parties to adopt data protection principles and promote interoperability between privacy protection regimes in order for data to be transferred between them seamlessly. For example, of the growing number of countries that have introduced privacy legislation in recent years, many are aligned with multilateral international instruments such as the OECD Privacy Guidelines.

Regional examples of non-binding multilateral approaches are the APEC Privacy Framework (which itself is based upon the OECD Privacy Guidelines) and the ASEAN Framework on Personal Data Protection (ASEAN PDP Framework), which sets out principles of personal data protection for ASEAN Member States to implement in their domestic laws (Box 3). Both frameworks aim to promote common regional standards for data sharing (GSM Association, 2018[12]). Other examples of regional non-binding multilateral approaches include the Standards for Data Protection for the Ibero-American States of the Ibero-American Data Protection Network (RIPD, 2017[18]), as well as the Updated Principles on Privacy and Personal Data Protection of the Organization of American States (Organization of American States[19]).

[7] See footnote 4.

[8] Provisions on transborder data flows in trade agreements can also have a complementary role in promoting interoperability of regulatory frameworks including those for privacy and data protection. Trade agreements are however out of scope of this policy note.

[9] In this survey, participation in the Global Privacy Enforcement Network (GPEN) was most frequently cited as a key arrangement for privacy cooperation, beside the European Data Protection Board (in the case of EU member countries) and the Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Enforcement Arrangement (in the case of APEC countries).

Box 3. ASEAN initiatives

Introduced in 2016, the **ASEAN Framework on Personal Data Protection** (ASEAN PDP Framework (ASEAN, 2016[20])) seeks to foster a closer understanding of data protection amongst ASEAN countries, including through information sharing, exchanges of good practices, joint activities and cooperation. It serves to strengthen the protection of personal data in ASEAN countries[10] and to facilitate cooperation among them.

The Framework sets out a number of privacy principles, which take account of: (1) consent, notification and purpose; (2) accuracy of personal data; (3) security safeguards; (4) access and correction; (5) transfers to another country or territory; (6) retention; and (7) accountability.

Of note, Principle 5 (transfers to another country or territory) requires that prior to a transborder transfer of data, the ASEAN Member State should either obtain the consent of the individual concerned or "take reasonable steps to ensure that the receiving organisation will protect the personal data consistently with (the) Principles".

In December 2018, ASEAN Telecommunications and Information Technology Ministers endorsed **the ASEAN Framework on Digital Data Governance** (ASEAN, 2018[21]) which sets out the strategic priorities, principles and initiatives to guide ASEAN Member States in their policy and regulatory approaches towards digital data governance in the digital economy. It identified four strategic priorities: (1) data life cycle and ecosystem; (2) cross-border data flows; (3) digitalisation and emerging technologies; and (4) legal, regulatory and policy.

Subsequently, a number of initiatives have been undertaken in order to implement these strategic priorities. In November 2019, ASEAN Ministers adopted 'Key Approaches for the **ASEAN Cross Border Data Flows Mechanism'** (ASEAN, 2021[22]), which proposed that ASEAN focus on developing two mechanisms in particular: 1) **ASEAN Model Contract Clauses** (MCCs); and 2) **ASEAN Certification for Cross Border Data Flows**. MCCs (approved by ASEAN in January 2021 (ASEAN, 2021[23])) serve as template contractual terms and conditions that may be included in the binding legal agreements between businesses who seek to transfer personal data to each other across borders, helping reduce the negotiation and compliance cost and time (especially for SMEs), while ensuring personal data protection. Implementation guidance for the ASEAN Certification for Cross Border Data Flows is expected by 2021.

In January 2021, the ASEAN Digital Ministers approved the **ASEAN Data Management Framework** (DMF) (ASEAN, 2021[24]), which provides voluntary,

[10] ASEAN countries include Brunei Darussalam, Cambodia, Indonesia, the Lao People's Democratic Republic, Malaysia, Myanmar, Philippines, Singapore, Thailand, and Viet Nam.

non-binding guidance for businesses (including SMEs), in establishing a data management system, including data governance structures and safeguards.

In addition to these mechanism, ASEAN specifically recognises that other mechanisms for cross-border data transfer include consent, codes of conduct, binding corporate rules, and other certification systems (e.g., ISO, APEC Cross Border Privacy Rules and Privacy Recognition for Processors Systems).

Source: ASEAN (2016[20]) ; (2018[21]) ; (2021[24]) ; (2021[23]) ; (2021[22])

A growing number of international regional binding multilateral instruments also serve to foster privacy interoperability. For instance, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, opened for signature in 1981 (commonly referred to as Convention 108) under the auspices of the Council of Europe, is a binding treaty protecting the right to privacy of individuals with respect to personal data which is automatically processed. The ratification process requires States to implement the Convention into their domestic law. To date, fifty-five States have committed to establish, under their own domestic law, sanctions and remedies for violations of the Convention's provisions. The 2018 Amending Protocol will update the data protection safeguards, including the provisions on the flow of personal data between signatories (creating what is commonly known as Convention 108+).

Another example of a binding multilateral approach is the African Union Convention on Cyber Security and Personal Data Protection (known as the Malabo Convention). This Convention aims at addressing the absence of specific legal rules that protect consumers, intellectual property rights, personal data and information system, and includes data protection principles, enforcement mechanism, rights of data subjects, as well as obligations for data controllers (African Union, 2014[25]). The Convention was adopted in 2014 and is open to all Member States of the African Union. To date, 14 countries have signed the Convention and 8 countries have ratified it[11].

Harmonisation and mutual recognition

Among the most notable binding approaches and legal frameworks, the GDPR harmonises privacy protection rules within the European Economic Area (EEA). It provides for various transfer tools for international data flows, designed to ensure that the level of data protection in the EEA is not undermined, and also includes tools to ensure co-operation and consistency[12]. Transfer tools include cross-border

[11] The Convention requires ratification of 15 countries to enter into force. See African Union (2020[51]).

[12] See, for example, Article 50 on international cooperation for the protection of personal data, Article 60 on cooperation between the lead supervisory authority and the other supervisory authorities concerned, Article 61 on mutual assistance, Article 62 on joint operations of supervisory authorities,

data transfers to a "third country" on the basis of an adequacy decision by the European Commission (Art. 45 GDPR)[13]. The effect of such a decision is that personal data can flow from the EU, Norway, Liechtenstein and Iceland to that third country freely. In some cases, this might involve the third country putting in place additional safeguards for data transfers from the EEA where this would help to bridge relevant differences and thus allow for an adequacy finding. Adequacy or equivalence determination is a unilateral recognition certifying that the data protection regime of another country meets certain privacy requirements and so data can be transferred unimpeded to this country. Adequacy decisions are typically subject to periodic review to ensure a continued level of protection. Adequacy recognition can be mutual where similar transfer frameworks exist for both parties involved.

Several countries have recently engaged in bilateral negotiations and review processes with the European Commission so as to be recognised and added to the list of countries with an adequate level of protection. The European Commission has so far recognised Andorra, Argentina, Canada (commercial activities), the Faroe Islands, Guernsey, Israel, the Isle of Man, Japan (private sector), Jersey, New Zealand, Switzerland, the United Kingdom and Uruguay as providing adequate protection (European Commission[26])[14].

Following the United Kingdom's withdrawal from the European Union, in February 2021, the European Commission, at the request of the UK, assessed the UK's level of data protection in view of a possible finding of adequacy for transfers of personal data from the EU to the UK. Two adequacy decisions were adopted in June 2021[15] (European Commission, 2021[27]). The UK had previously already recognised the EU and EEA member states as adequate, as part of its commitment to establish a smooth transition[16] (United Kingdom Government, 2021[28]).

Japan provides another example of a country taking active steps to promote international co-operation and interoperability, and has privacy co-operation and collaboration built into its legal regime. Of note, Article 6 of the Act on the Protection of Personal Information ("APPI") provides that "the government shall [...]

Article 63 on the consistency mechanism, and Article 70(1)(e) on guidelines, recommendations and best practices by the European Data Protection Board to encourage consistent application of the GDPR.

[13] A decision finding that a third country ensures a level of protection essentially equivalent to that in the EU

[14] Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland and Uruguay were recognised as providing adequate protection under the previous Data Protection Directive (Directive 95/46), and Japan (private sector) and the United Kingdom as providing adequate protection under the GDPR. As at the time of writing, the European Commission has triggered the adoption procedure on an adequacy decision with respect to South Korea.

[15] These adequacy decisions include one under the GDPR and the other for the Law Enforcement Directive (Art. 36 of Directive (EU) 2016/680)

[16] Arrangements were also made between the UK and Japan regarding the existing EU-Japan mutual recognition so that data can continue to flow between the UK and Japan following Brexit.

take necessary legislative and other action for protecting personal information [...], and shall take necessary action in collaboration with the governments in other countries to construct an internationally conformable system concerning personal information through fostering cooperation with an international organization and other international framework" (Personal Information Protection Commission, Government of Japan[29]).

The Japanese privacy authority, the Personal Information Protection Commission (PPC), promotes international co-operation and interoperability in cross-border data transfers through dialogue with the EU, the US, the UK and the APEC region (OECD, 2021[3]). Additionally, similarly to Article 45 of the GDPR, the PPC can designate a foreign country or region as providing a personal information protection system with equivalent standards to those which serve to protect an individual's rights and interests in Japan (Article 24 of the APPI).

Additionally, the European Commission and the PPC agreed on a framework for cross-border transfers of personal data in January 2019; just as Japan has been recognised by the European Commission to provide an adequate level of protection based on the GDPR (European Union, 2019[46]), the PPC has designated the EEA countries as providing an equivalent level of protection based on Article 24 of the APPI. (Personal Information Protection Commission, Government of Japan, 2019[30]) [17] [18].

Initiatives involving the private sector

A number of initiatives involving the private sector exist, which can serve to foster and promote privacy interoperability, and support the transborder flows of personal data. For example, this can be achieved through model contract clauses, binding corporate rules, codes of conduct, and certification schemes such as those under the APEC CBPR System or the EU's GDPR (Article 46(2)(f)) [19]. The following section considers the role of such initiatives.

[17] These mutual decisions will be reviewed by the EC and the PPC respectively, two years from the date of the original notification of the decisions, and thereafter at least every four years.

[18] In 2020 the PPC determined that the cross-border transfer of personal data with the UK could continue, following the UK's withdrawal from the EU.

[19] Europrivacy is an example for certification schemes under the EU's GDPR. It is developed by the European Research Programme Horizon 2020 and co-funded by the European Commission and Switzerland, managed by the European Centre for Certification and Privacy (ECCP), and maintained by the Europrivacy International Board of Experts in data protection. Europrivacy provides a methodology to certify the conformity of all sorts of data processing with the GDPR, including cross-border data transfer under GDPR Article 46. See, https://europrivacy.org/en

Model contract clauses

One important – and increasingly used[20] – instrument which can foster interoperability is comprised of model contract clauses (MCCs) setting out data protection safeguards, which, when incorporated into commercial contracts, are binding on the data exporter (sender) and the data importer (recipient in the third country). Typically, MCCs are pre-approved by the competent domestic authorities (e.g. a data protection authority) and provide a ground – under domestic rules – for the transfer of personal data without the need for those domestic authorities to grant a further individual authorisation. MCCs establish a data protection regime at contractual level, and can therefore help to bridge existing differences in the level of privacy and data protection under the respective domestic legal frameworks.

Over time, MCCs can contribute to interoperability as they set common standards with which companies become familiar. This may make it easier to align data protection rules in domestic laws in the future. The MCCs' nature as "model" (i.e. with a fixed content) and their public availability can help ensure transparency and legal certainty for both companies and individuals. The fixed content and the pre-approval mean that companies do not have to negotiate them in each individual case, but can simply rely on what has been pre-approved, with the assumption that in doing so they fulfil their obligations as regards data transfers. Their low cost may also make them particularly attractive for small and medium-sized companies.

Currently, an increasing number of jurisdictions have developed MCCs. This includes for instance: the European Union, which recently modernised its so-called "Standard Contractual Clauses" (European Commission[31]), New Zealand's newly adopted model contract clauses (Office of the Privacy Commissioner[32]), Argentina's data protection contractual clauses (Ministry of Justice and Human Rights, Argentina[33]), the standard data protection clauses recently adopted by the Dubai International Financial Centre (Dubai International Financial Centre[34]), or the ASEAN Model Contractual Clauses for Cross-Border Data Transfers that were recently published (see above for more information) (ASEAN, 2021[23]). Model contract clauses are also a recognised instrument under the Council of Europe Convention 108 (see Article 14(3)(b) of the modernised Convention (Council of Europe, 2018[35])). In October 2021, the Ibero-American Data Protection Network adopted a resolution recognising the importance of MCCs as a transfer tool and triggering the adoption procedure for MCCs (RIPD, 2021[36]).

[20] For instance, MCCs represent an important transfer instrument for data transfers from the EU to third countries. See IAPP-EY Annual Privacy Governance Report 2019 ("88% of respondents [most of whom being from the US and the EU] in this year's survey reported MCCs as their top method for extraterritorial data transfers, followed by compliance with the EU-US Privacy Shield arrangement (60%). For respondents transferring data from the EU to the UK (52%), 91% report they intend to use MCCs for data-transfer compliance after Brexit"). See also Asian Business Law Institute (2020[11]) which notes "Contracts are the most promising avenue of cooperation for increasing the compatibility of Asian data transfer regimes".

Binding Corporate Rules

Binding corporate rules (BCRs), sometimes referred to as intra-group rules, are data protection policies adhered to by companies for cross-border transfers of personal data within a group of undertakings or enterprises. They can be particularly beneficial for companies that need to transfer data globally within their own group.

BCRs are often standardised, establishing uniform binding rules applicable to all relevant entities across the group, so that adequate protection for data transferred across borders and compliance with local law can be ensured. In general, BCRs address the application of data protection principles, types of data transfers, rights of data subjects, complaint handling procedures, the role of data protection officers (DPOs), the mechanisms within the group to verify compliance, methods of reporting to supervisory authorities, and training. BCRs sometimes require approval by a supervisory authority. For example, in the EU, BCRs require approval by the competent supervisory authority in the EU (EU GDPR Article 47) [21].

BCRs have been developed in the EU as a cross-border transfer mechanism consistent with the transfer requirements in the EU GDPR[22]. In addition, several Asia-Pacific countries' laws allow cross-border transfers based on 'internal rules' or BCRs, among other data transfer mechanisms. Such rules are explicitly recognised as a valid data transfer mechanism in the laws of, or regulatory guidance issued in, several jurisdictions (Australia, Hong Kong SAR, Japan, New Zealand, and Singapore), as well as in the data protection bills of Thailand (Personal Data Protection Act) and India (Data Protection Bill) (Asian Business Law Institute, 2020[11]).

CBPR System

The CBPR System, developed by all 21 APEC economies, and endorsed by APEC leaders in 2011, provides an example of interoperability in practice. The APEC Privacy Framework (itself modelled after the OECD Privacy Guidelines), which provides that APEC member economies should take all reasonable and appropriate measures to remove unnecessary barriers to data flows and avoid the creation of such barriers, provides the basis for the CBPR system.

This mechanism recognises the differences amongst the legal systems in the APEC region, and establishes a baseline protection whilst also allowing each economy to choose implementation methods. Under this system, companies are certified for their compliance with the APEC Privacy Framework as it relates to requirements for the protection of personal data, demonstrating their compliance with

[21] BCRs require to be approved in accordance with the so-called consistency mechanism if the approval process involves supervisory authorities from more than one Member State (EU GDPR Art 63).

[22] The list of approved BCRs under the GDPR can be found at: *https://edpb.europa.eu/our-work-tools/accountability-tools/bcr_de*.

internationally recognised data privacy protections and therefore able to transfer data within APEC economies. Additionally, a regulatory cooperative arrangement (the CPEA[23]) acts to facilitate co-operation of privacy enforcement authorities of participating APEC economies in enforcing the CBPR.

The CBPR System is only accessible to those APEC economies which can demonstrate compliance with its requirements. Currently, there are nine participating APEC CBPR system economies: Australia, Canada, Chinese Taipei, Japan, Mexico, the Philippines, Korea, Singapore, and the USA, and 42 CBPR certified companies (36 in the USA, 2 in Japan and 4 in Singapore) as of July 2021[24]. Significantly, the CBPR System was recognised in the 2018 trade agreement among Canada, Mexico and the United States as demonstrating the trade benefits of cooperating on these issues[25], and Japan and Singapore have recognised the CBPR System's capacity to enable cross-border data transfers in compliance with domestic law. APEC economies make efforts to promote the system, publicising the practical benefits for companies of joining the CBPR (APEC, 2019[37]).

Through the CBPR System, once companies are certified for their compliance through an APEC recognised Accountability Agent[26], they are able to transfer data to other CBPR-certified companies to the extent the domestic law applicable to them allows this, and will be subject to enforcement of the program requirement by both the Accountability Agent and also the PEA in the relevant APEC economies. In this way, certified companies and governments work together to ensure that when personal information moves across borders, it is protected in accordance with prescribed privacy standards, and those standards are enforceable across participating jurisdictions.

[23] This mechanism aims to: 1) Facilitate information sharing among Privacy Enforcement Authorities (PE Authorities) in APEC Economies (which may include Privacy Commissioners' Offices, Data Protection Authorities or Consumer Protection Authorities that enforce Privacy Laws); 2) Provide mechanisms to promote effective cross-border cooperation between authorities in the enforcement of CBPR program requirements and privacy laws generally, including through referrals of matters, parallel or joint investigations, or enforcement actions; and 3) Encourage information sharing and cooperation on privacy investigation and enforcement with PEAs outside APEC.

[24] APEC Economies establish a publicly accessible directory of organisations that have been certified by Accountability Agents as compliant with the CBPR System, which includes relevant details of each certification.

[25] This reflects observations recently made by the OECD that the number of trade agreements with data flow provisions are growing. (See, *Mapping Commonalities in Regulatory Approaches to Cross-border Data Transfers* (OECD, 2021[10])at p26ff).

[26] To become an APEC-recognized Accountability Agent, an Accountability Agent should meet the established recognition criteria to the satisfaction of APEC Economies (see para 33, of the APEC CBPR System Policies, Rules and Guidelines, available at: *http://cbprs.org/wp-content/uploads/2019/11/4.-CBPR-Policies-Rules-and-Guidelines-Revised-For-Posting-3-16-updated-1709-2019.pdf*).

A key aspect of the CBPR System is that it is not intended to displace or change an APEC economy's domestic laws and regulations, and where there are no applicable domestic privacy protection requirements in an APEC economy, the CBPR System is intended to provide a minimum level of protection.[27] Nonetheless, when considering whether to participate in the CBPR System, economies may need to make changes to domestic laws and regulations to ensure the necessary elements of the CBPR. To this end, several measures are available – for example, identifying an appropriate regulatory authority to act as the privacy enforcement authority in the CBPR System.

BCR/CBPR Referential

An initiative between the CBPR System and the EU data transfer mechanisms, building on the "Referential" (EU WP29 [former Article 29 Data Protection Working Party of the European Union], 2014[38]) was developed in 2014 to reflect the respective requirements of the CBPR System and the Binding Corporate Rules ("BCR") of the EU.[28]

The Referential aims to serve as an informal, pragmatic checklist for organisations applying for authorisation of the BCR and/or certification of the CBPR System, thereby facilitating the design and adoption of personal data protection policies compliant with each of the systems. Although it does not aim at achieving mutual recognition of both systems, it could serve as a basis for double certification. For each of the essential principles and requirements of the systems, the Referential comprises: a "common block" describing the main elements which are common or similar to the BCR and the CBPR, and "additional blocks" presenting their main differences and the additional elements specific to the BCR or to the CBPR System.

Codes of Conduct

Codes of Conduct ('codes') are voluntary instruments adopted by organisations to help them apply general data protection provisions, including for the cross-border transfer of personal data. These codes can be tailored to specific sectors, and the specific needs of the organisation itself.

Codes are drawn up by the organisation itself, representative bodies such as industry associations, government or data protection authorities. Codes sometimes

[27] See Paragraph 43 and 44 of the Policies, Rules and Guidelines.

[28] It is noted that this initiative was developed under the former Data Protection Law (Directive 95/46/EC), and is not established under the GDPR. In the context of that "Referential", the OECD's Working Party on Security and Privacy in the Digital Economy (now replaced by the Working Party on Data Governance and Privacy and the Working Party on Security in the Digital Economy) held a roundtable on "Opportunities and Challenges for Advancing Global Interoperability" at its 36th meeting (June 2014). The June 2014 Roundtable underlined the importance of providing global operators with tools to meet their privacy obligations and stressed the desirability of moving beyond a regional approach to a more global one together with stronger international enforcement co-operation.

require approval by a competent supervisory authority. The association or industry body creating such codes conducts reviews of any applicant seeking membership and ensures compliance with the codes of conduct by adhering organisations. Codes are deemed useful for SMEs as they can rely on the association to ensure compliance.

Recognition of codes of conduct as a cross-border transfer mechanism exists in the EU GDPR, which provides that adherence to codes, together with binding and enforceable commitments (to comply with the safeguards contained in the code), can demonstrate that data importers located outside the EU have implemented adequate safeguards in order to permit transfers under Article 46(e) GDPR. In Australia, the Information Commissioner can approve and register enforceable codes which are developed by entities on their own initiative or on request from the Information Commissioner, or developed by the Information Commissioner directly. In New Zealand, the Privacy Commissioner has issued several Codes of Practice under the Privacy Act, which have become part of the law and which modify the privacy principles in relation to specific industries[29] (Asian Business Law Institute, 2020[11]).

Private Sector Initiatives

A number of different private sector initiatives are worth highlighting. For example, the International Organization for Standardization (ISO), an international standard-setting body composed of representatives from various national standards organisations, has developed a privacy protection ISO (ISO/IEC 27701:2019; (ISO, 2019[39])), which specifies requirements and provides guidance for establishing, implementing, maintaining and continually improving a Privacy Information Management System.

Industry associations also play a role in this area. For instance, the Business Software Alliance has developed a Privacy Framework (BSA, 2018[40]) as a guide for policymakers to draft privacy legislation, which includes a recommendation that governments create tools to bridge gaps among different domestic privacy regimes in ways that both protect privacy and facilitate the free flow of data.

Privacy "trust marks" are another private sector initiative, sometimes involving the public sector. Although there is no common definition, a privacy trust mark or seal is often designed to help organisations demonstrate that their privacy/data protection practices are compliant with international standards, and help consumers recognise their privacy safety. Granted to companies or their products/services by private certification agencies or privacy enforcement authorities, privacy trust marks can help increase international interoperability at an organisation and product/service level. While further work is needed to analyse these and other

[29] Health Information Privacy Code (1994), Credit Reporting Privacy Code (2004), Telecommunications Information Privacy Code (2003).

private sector initiatives, standard setting by private sectors could promote cross-border data flows with trust that is built upon compliance with those standards.

Privacy enhancing policy measures and cross-border enforcement co-operation

Complementary policy measures

The recent review of the OECD Privacy Guidelines and the Privacy Guidelines Questionnaire shed light on a range of policy measures that governments or PEAs take to promote transborder data flows, international privacy enforcement co-operation, and privacy interoperability (OECD, 2021[3]). The need for complementary policy measures is mentioned in Part 5 of the OECD Privacy Guidelines as a means for national implementation of the Guidelines [paragraph 19(g)].

Such measures include stakeholder consultations, workshops, advisory guidelines and participation in international fora. The Privacy Guidelines Questionnaire found that enhancing privacy awareness through guidance and education was the most frequently adopted policy measure, in particular by PEAs (OECD, 2021[3]).

As an illustration, the Australian Information Commissioner (OAIC), together with other Asia Pacific Privacy Authorities (APPA), organises an annual Privacy Awareness Week. As will be discussed in the next section, regional and international fora are also a means to promote interoperability through cross-border enforcement co-operation.

Cross-border enforcement co-operation

Interoperability can facilitate cross-border enforcement co-operation, and, in turn, effective cross-border enforcement is a critical feature of the design of privacy interoperability mechanisms.

The role of cross-border enforcement for interoperability is reflected in Part Six of the OECD Privacy Guidelines, which emphasises both "International Co-operation and Interoperability" (as highlighted in the introduction to this Toolkit Note), and at paragraph 20 asks adhering countries to "take appropriate measures to facilitate cross-border privacy law enforcement co-operation, including by sharing relevant information among [PEAs]"[30]. In practice, 'sharing relevant information' can take many forms, such as simply sharing information and evidence, formal or informal consultations, joint investigations, or establishing frameworks detailing the

[30] The role of cross-border enforcement for interoperability was already acknowledged in the Explanatory Memorandum for the 1980 Privacy Guidelines which foresaw that international data networks and the complications associated with them would become more numerous, and explained that provisions on mutual assistance were drafted to alleviate some of these complications (OECD, 2013[2]).

conditions for such sharing through Memorandums of Understanding between two or more countries, depending on the needs, purposes and tools available.

The 2021 review of the OECD Privacy Guidelines revealed that approximately two-thirds of countries which responded to the OECD Privacy Guidelines Questionnaire said that their PEA had sought assistance from, or referred a privacy violation complaint to, a PEA in another country and/or vice versa[31] (OECD, 2021[3]). Of note:

- Australia and Canada reported engaging in a joint cross-border investigation regarding a data hack that threatened exposure of the accounts of approximately 36 million adult-dating user accounts (Australian Government, Office of the Australian Information Commissioner, 2016[41]);
- Israel reported co-operation with PEAs in the EU regarding a company then registered in Israel, which was allegedly violating EU privacy legislation; and
- Korea reported requesting information sharing from the UK Information Commissioner's Office, in relation to an investigation concerning Facebook.

Additionally, countries responding to the questionnaire reported their participation in a range of international fora 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 popular (18 responding countries), followed by the ICDPPC[32] Enforcement Cooperation Arrangement (11 responding countries) and the APEC Cross-border Privacy Enforcement Arrangement (CPEA) (8 responding countries) (although the total number of participants in both initiatives which extend beyond the OECD area is much higher). Also of note is the binding enforcement co-operation mechanism under Convention 108 / Convention 108+ of Council of Europe. This convention requires co-operation between the supervisory authorities of Parties to the Convention, including through mutual assistance, information sharing and co-ordinated investigations.

The European Data Protection Board (EDPB) was often mentioned by respondents within the EU as a body established for regulatory co-operation and as a means to promote privacy consistency. The EDPB is an EU body tasked with ensuring the consistent application of EU legislation in the field of data protection. Within the Union, where integration is very advanced, co-operation has been made compulsory, under the aegis of the EDPB (Chapter 7 of the GDPR).

Regional networks of data protection authorities from countries that share similar aspects in terms of language and culture are also beneficial for facilitating and promoting cross-border enforcement co-operation and capacity building through the sharing of knowledge and best practices for data protection. Such networks

[31] 23 responding countries said their PEA sought assistance from/referred a violation to another country and 22 responding countries said another PEA sought assistance from/referred to them.

[32] Now the Global Privacy Assembly.

include the Asia Pacific Privacy Authorities (APPA) Forum for Asia-Pacific countries, the Common Thread Network (CTN) for Commonwealth countries, l'Association Francophone des Autorités de Protection des Données Personnelles (AFAPDP) 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.

Discussions on emerging enforcement challenges among experts emphasised the importance of cross-border international collaboration, particularly in order to facilitate the free flow of data with trust (OECD, 2021[3]). Many of the aforementioned collaboration and co-operation mechanisms were proposed as good practices, including information sharing, joint investigations and conducting co-ordinated compliance actions. Experts suggested that effective international collaboration can allow PEAs to overcome the challenges of regulating in an environment involving rapid innovation.

Lastly, the 2007 OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy (OECD, 2007[42])should be highlighted in this regard. This Recommendation, which is grounded in the OECD Privacy Guidelines, 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 to one another in the enforcement of privacy laws. The importance of this Recommendation in facilitating interoperability was clearly recognised in the report on the implementation of the OECD Privacy Guidelines, with a number of countries recommending that its implementation be reviewed (OECD, 2021[3]).

National privacy strategies

Paragraph 19.a) of the OECD Privacy Guidelines asks Member Countries to "develop national privacy strategies (NPS) that reflect a co-ordinated approach across governmental bodies". The prevalence of NPS and their components were explored in the report on the implementation of the OECD Privacy Guidelines (OECD, 2021[3]). The analysis based primarily on the replies to the privacy questionnaire for the 2017 edition of the Digital Economy Outlook (DEO) (OECD, 2017[43]) and the May 2018 Roundtable identified five key features[33] of the process to develop a NPS, with one such feature being "*The enhancement of international co-operation to foster*

[33] These being: 1) A definition of privacy and data protection policy objectives at the highest level of government and their alignment with other important strategic national objectives; 2) The adoption of a whole-of-society (holistic) approach that involves all relevant stakeholders to enhance privacy protection while providing the flexibility needed for all to benefit from digital innovation; 3) Assurance of coherence of policy and regulatory measures to protect privacy by improvement of intra-governmental and public-private co-ordination; 4)The enhancement of international co-operation to foster interoperability of privacy protection frameworks and lessen uncertainties in transborder data flows; and 5) The measurement of the implementation and impact of NPS to monitor their effectiveness.

interoperability of privacy protection frameworks and lessen uncertainties in transborder data flows".

Amongst other benefits, NPSs can play a significant role in promoting privacy interoperability, through addressing privacy and data protection in a comprehensive and coherent manner, and by incorporating a whole-of-society perspective on how to protect privacy more effectively, while enabling innovation and transborder data flows. Ideally, a NPS could provide an outline for international cooperation that addresses international privacy issues and existing restrictions on international data sharing, as well as risks associated with incompatibilities of legal regimes. NPSs should further strive to provide clarity with regard to existing legal requirements around data protection and privacy.

It is apparent that there remains work to be done to ensure a shared understanding of NPS, as well as wider adoption. The findings from the review suggest that just under half of the respondents have in place a national privacy strategy or whole-of-government approach to privacy, with only seven responding countries positively stating they have a national privacy strategy. A number of countries reported nonetheless alternative means of whole-of-government co-ordination, such as through legislation, the PEA or other dedicated entities or fora.

Nonetheless, the privacy questionnaire carried out for the 2017 edition of the DEO concluded that most countries did have in place some of the basic elements of a NPS, albeit as part of other strategic documents (OECD, 2017[43]).For example, actions to enhance international co-operation and the importance of participation in international privacy initiatives is recognised in many national strategic policy documents[34]. Additionally, international co-operation and the need for better alliances and partnerships with like-minded countries or allies, including facilitating capacity building of less developed countries, are shared as key objectives by most national digital security strategies (OECD, 2013[2]).

Conclusion

This paper has stressed the importance of privacy interoperability (as well as international co-operation) in light of the growth in volume and importance of transborder flows of personal data, and the multiplicity of applicable privacy regimes (which have the potential to create uncertainty for governments, businesses and individuals). The paper has also sought to contribute to a shared understanding of the concept 'privacy interoperability' and has considered the

[34] For example in Korea's Personal Data Protection National Basic Plan 2018-2020 ("Rationalizing regulations and reinforcing global cooperation"); the United Kingdom's Information Commissioner's Office International Strategy 2017-2021 (see Annex); the Office of the Australian Information Commissioner's International Strategy 2020-2021 (see Annex); and Japan's National Data Strategy (a Cabinet Decision in 2021).

different measures which exist to foster and promote the interoperability of privacy and data protection frameworks.

With the aim of progressing towards a shared definition, and in connection with future work on the Privacy Guidelines and its Supplementary Explanatory Memorandum, the report suggests that interoperability, in the context of privacy and data protection, is best understood 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 the different approaches and systems of privacy and personal data protection to facilitate transborder flows of personal data. Several different measures are identified which can foster and promote privacy interoperability. Different international and regional instruments (both binding and non-binding) encourage countries to adopt privacy and data protection principles and promote interoperability between privacy protection regimes in order for data to be transferred between them seamlessly. For example, in line with the OECD Privacy Guidelines, Convention 108, or through the APEC and ASEAN Privacy Frameworks.

Other measures to foster and promote interoperability include binding arrangements such as those under the GDPR, or Japan's APPI, which provide for mutual recognition of privacy regimes, allowing for personal data to flow freely between the concerned jurisdictions on the basis of an adequacy or equivalency determination. Additionally, this paper identified a number of initiatives, which involve the private sector to different degrees (often entailing some form of pre-approval by domestic regulatory authorities), such as certification schemes, model contract clauses, binding corporate rules, and codes of conduct.

Lastly, this note identifies that the adoption of complementary policy measures as well as national privacy strategies can act to further privacy interoperability, and it is seen that countries participate in a variety of regional and international fora to promote privacy interoperability, as well as co-operating and sharing information on privacy enforcement (particularly in terms of seeking assistance with privacy violations).

Annex. A selection of instruments, approaches and initiatives to foster privacy interoperability

Bilateral and multilateral approaches

OECD Privacy Guidelines

Responsible entity: OECD

Description: The Recommendation concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (the "OECD Privacy Guidelines") was adopted by the OECD Council in 1980. The Privacy Guidelines were the first internationally agreed set of privacy principles applicable to the protection of personal data, whether in the public or private sectors. The Privacy Guidelines were revised in 2013, introducing a number of new concepts including global interoperability. Paragraph 21 of the revised Privacy Guidelines expresses the general objective of Member countries to improve global interoperability of privacy frameworks through the promotion of policy and international arrangements that give practical effect to the Privacy Guidelines. To date, 37 OECD Member countries adhere to the Recommendation.

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

APEC Privacy Framework

Responsible entity: APEC

Description: The APEC Privacy Framework (originally developed in 2005 and modelled upon the OECD Privacy Guidelines) sets out the APEC information privacy principles, as well as providing guidance for domestic and international implementation. It forms the basis for the APEC Cross-border Privacy Enforcement Arrangement (CPEA) and the APEC Cross-Border Privacy Rules (CBPR) System. Updated in 2015 to reflect the 2013 revisions to the OECD Privacy Guidelines, the APEC Privacy Framework calls on member economies to encourage and support the development of international arrangements that promote interoperability amongst privacy instruments and which can give practical effect to the Framework.

Read more: *https://www.apec.org/Publications/2017/08/APEC-Privacy-Framework-(2015).*

ASEAN PDP Framework

Responsible entity: ASEAN

Description: The ASEAN 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 intend to create legally binding domestic or international obligations, but encourages the

participants to endeavour to cooperate, promote and implement the privacy principles set out in the Framework in their domestic laws and regulations, while continuing to ensure and facilitate the free flow of information among ASEAN Member States.

Read more: *https://asean.org/storage/2012/05/10-ASEAN-Framework-on-PDP.pdf.*

Convention 108 / Convention 108+

Responsible entity: Council of Europe

Description: The Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (commonly referred to as Convention 108) is a binding treaty protecting the right to privacy of individuals with respect to the automatic processing of personal data. The ratification process requires States to implement the Convention into their domestic law. To date, fifty-five States have ratified Convention 108. In October 2018, a Protocol to modernise Convention 108 to ensure its applicability to new information and communication technologies, and to strengthen its effective implementation, was opened for signature. The Convention as amended by the Protocol is referred to as "Convention 108+". Convention 108+ is yet to come into force, and will do so either once all signatories to Convention 108 have ratified, or on 11 October 2023 if there are 38 parties to the Convention on that date. The implementation of Convention 108+ is monitored by the Council of Europe's Convention 108 Committee.

Read more: *https://www.coe.int/en/web/data-protection/convention108/modernised.*

Mutual Adequacy Decisions

Responsible entity: EU, Japan

Description: Mutual adequacy decisions exist between EU and Japan. Article 45 of the EU's General Data Protection Regulation [Regulation (EU) 2016/679, "GDPR"] permits transfer of personal data to a third country where the European Commission has decided that third country ensures an adequate level of protection without any further safeguards being necessary. Likewise, the Japanese privacy authority, the Personal Information Protection Commission (PPC) can 'whitelist' a foreign country with standards equivalent to those which serve to protect an individual's rights and interests in Japan, pursuant to Article 24 of the Act on the Protection of Personal Information. In January 2019, the European Commission adopted its adequacy decision on Japan and the PPC issued an equivalent decision on EEA countries, allowing free flow of personal data between the two economies.

Read more:
https://ec.europa.eu/commission/presscorner/detail/en/IP_19_421.
https://www.ppc.go.jp/en/aboutus/roles/international/cooperation/20190123/.

APEC CBPR system

Responsible entity: APEC

Description: The APEC Cross-Border Privacy Rules (CBPR) System, endorsed by APEC leaders in 2011, is a data privacy certification system that facilitates cross-border transfer of personal data amongst APEC economies while ensuring data protection. Companies that choose to participate in the CBPR System should implement data privacy policies and practices consistently with the CBPR program requirements based on the APEC Privacy Framework. These policies and practices must be assessed as compliant with the CBPR program requirements by an APEC-recognised Accountability Agent and be enforceable by law. Currently, there are nine participating APEC CBPR system economies (USA, Mexico, Japan, Canada, Singapore, the Republic of Korea, Australia, Chinese Taipei and the Philippines) and 42 CBPR certified companies (36 in the USA, 2 in Japan and 4 in Singapore).

Read more: *http://cbprs.org/.*

Private sector / Non-governmental initiatives

ISO/IEC 27701: 2019

Responsible entity: International Organization for Standardization (ISO)

Description: ISO/IEC 27701:2019 is an international standard related to privacy and data protection, developed by the ISO, an independent non-governmental international organization with a membership of 165 national standard-setting bodies. It was developed as an extension to the existing ISO standards on information security, and specifies requirements and provides guidance for establishing, implementing, maintaining and continually improving a Privacy Information Management System (PIMS) for Personally Identifiable Information (PII) controllers and processors for all types, whether public or private. It includes a mapping of other privacy frameworks, including the GDPR, to indicate how compliance to ISO/IEC 27701:2019 can be relevant to fulfil obligations to those privacy frameworks. Generally, organisations may be certified compliant with ISO/IEC standards by accredited registrars worldwide.

Read more: *https://www.iso.org/standard/71670.html.*

"Trust marks"

Responsible entity: TrustArc

Description: The US's TrustArc offers a set of privacy assurance programs that are developed based on globally recognized laws and standards such as GDPR, ISO 27001, US HIPPA, OECD Privacy Guidelines and APEC Privacy Framework. Certified companies can display a "TRUSTe Verified Privacy seal" on applicable digital properties.

Read more: *https://trustarc.com/consumer-info/privacy-certification-standards/.*

Responsible entity: The Office of the Privacy Commissioner, New Zealand

Description: Initiated in 2018, the Privacy Trust Mark applies to products and services (not companies) that the Privacy Commissioner considers to be outstanding in the way companies manage personal information in the design of their product or service. The Privacy Trust Mark is designed to help consumers have trust and confidence that their information will be safeguarded. It will also make it easier for people to choose privacy-friendly goods and services.

Read more: *https://www.privacy.org.nz/assets/Uploads/2018-05-09-Privacy-Trust-Mark-FAQs-A562602.pdf.*

Responsible entity: The Info-communications Media Development Authority (IMDA), Singapore

Description: Singapore's Data Protection Trustmark is a voluntary enterprise-wide certification for organisations to demonstrate accountable data protection practices. The certification scheme is administered by the Info-communications Media Development Authority (IMDA). The IMDA indicates that organisations with ISO/IEC 27001 and 27701 may find it easier to attain certification as they have demonstrated good information security and privacy information management standards.

Read more: *https://www.imda.gov.sg/programme-listing/data-protection-trustmark-certification.*

Responsible entity: Japan Information Processing Developing Centre (JIPDEC)

Description: Japan's PrivacyMark, administered by JIPDEC since 1998, assesses whether private enterprises take appropriate measures to protect personal information. The PrivacyMark system has adopted JIS Q 15001 (a Japanese Industrial Standard concerning personal information protection management systems) as its assessment criterion since 1999 (when the first edition was developed), encompassing the 8 principles of the OECD Privacy Guidelines and most of the concepts of the EU Directive (95/46/EC). Certified enterprises are granted the right to display "PrivacyMark" in the course of their business activities. Currently, more than 16 000 enterprises have been certified.

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

National privacy strategies

International Strategy 2017-2021

Responsible entity: Information Commissioner's Office (UK)

Description: The International Strategy 2017-2021 sets out key policy priorities to enhance privacy protection for the UK public. Recognising the importance of global data flows and effective safeguards for international data transfer, the Strategy

states that the ICO seeks to explore the concept of the UK as a 'global data protection gateway' – a country with a high standard of data protection law which is effectively interoperable with different legal systems that protect international flows of personal data. Additionally, it indicates its supports for the development of mechanisms to support better interoperability between the UK's data protection laws and other systems such as the APEC CBPR.

Read more: *https://ico.org.uk/media/about-the-ico/documents/2014356/international-strategy-03.pdf.*

OAIC International Strategy 2020–2021

Responsible entity: Office of the Australian Information Commissioner

Description: OAIC's International Strategy (2020-2021) provides a roadmap for how Australia will engage, cooperate and act within the domestic and international communities to ensure that the privacy and information access rights of the Australian community are promoted and protected both domestically and at the global level. It highlights the importance of Australia's domestic frameworks remaining interoperable, so that data can flow across borders whilst also protecting personal information. It notes that such interoperability will enable the OAIC to continue to co-operate with privacy regulators across borders, in order to: promote a consistent regulatory approach; minimise compliance burden; and help secure Australia's place in the digital economy.

Read more: *https://www.oaic.gov.au/about-us/our-corporate-information/oaic-international-strategy-2020-2021/.*

Cross-border enforcement co-operation

GPEN

Responsible entity: Global Privacy Enforcement Network (GPEN)

Description: The GPEN, launched in 2010, is an informal network, open to public privacy enforcement authorities that are responsible for enforcing privacy laws or regulations. GPEN focusses on the practical aspects of privacy enforcement co-operation. In line with the 2007 OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy, its mission is to promote cooperation by exchanging information about relevant issues, trends and experiences; encouraging training opportunities and sharing of enforcement know-how, expertise and good practice; promoting dialogue with organisations having a role in privacy enforcement; creating, maintaining and supporting processes or mechanisms useful to bilateral or multilateral cooperation; and undertaking or supporting specific activities. As of 2021, GPEN is comprised of 71 authorities of 52 jurisdictions from different geographic regions of the world.

Read more: *https://www.privacyenforcement.net/.*

GPA

Responsible entity: Global Privacy Assembly (GPA)

Description: The GPA (the former International Conference of Data Protection and Privacy Commissioners: ICDPPC) is the global forum for data protection authorities, joined by more than 130 authorities across the globe. The GPA recognises enforcement co-operation as one of the three key pillars in its Policy Strategy, which resulted in the permanent establishment of the International Enforcement Cooperation Working Group (IEWG), with the membership of over 20 authorities. The recent initiatives include updating the "Enforcement Cooperation Handbook", which intends to assist authorities with practical guidance such as potential models, approaches and solutions that authorities can consider to address particular issues, and managing the "Enforcement Cooperation Repository", which is a platform to share links to publicly available information useful for enforcement co-operation.

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

EDPB

Responsible entity: The European Data Protection Board (EDPB)

Description: The EDPB is an EU body, tasked with providing general guidance to clarify the law and to promote a common understanding or EU data protection laws; adopting opinions addressed to the European Commission or to the national supervisory authorities of the Member States; adopting binding decisions addressed to the national supervisory authorities and aiming to settle disputes arising between them when they cooperate to enforce the GDPR, with the purpose of ensuring the correct and consistent application of the GDPR in individual cases; and promoting and supporting the cooperation among national supervisory authorities.

Read more: *https://edpb.europa.eu/edpb_en.*

Convention 108 / Convention 108+

Responsible entity: Council of Europe

Description: The Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (commonly referred to as "Convention 108", and "Convention 108+" as amended by a Protocol to amend Convention 108) provides, among others, for the enforcement co-operation mechanism between the supervisory authorities of Parities to the Convention, including through mutual assistance, information sharing and co-ordinated investigations.

Read more: *https://www.coe.int/en/web/data-protection/convention108/modernised.*

APEC Cross-border Privacy Enforcement Arrangement (CPEA)

Responsible entity: APEC

Description: The APEC Cross-border Privacy Enforcement Arrangement (CPEA) is a framework for regional cooperation in the enforcement of privacy laws, in which any privacy enforcement authority (PEA) in an APEC economy may participate. CPEA aims to: i) facilitate information sharing among PEAs in APEC Economies; ii) provide mechanisms to promote effective cross-border cooperation between authorities in the enforcement of CBPR program requirements and privacy laws generally, including through referrals of matters and through parallel or joint investigations or enforcement actions; and iii) encourage information-sharing and cooperation on privacy investigation and enforcement with PEAs outside APEC. AS of 2021, 26 authorities are members to CPEA.

Read more: *https://www.apec.org/Groups/Committee-on-Trade-and-Investment/Digital-Economy-Steering-Group/Cross-border-Privacy-Enforcement-Arrangement.*

Common Thread Network (CTN)

Responsible entity: Common Thread Network

Description: The Common Thread Network (CTN) is a forum for data protection and privacy authorities of Commonwealth countries, with representation from Europe, Africa, Asia, the Pacific, the Americas and the Caribbean. The CTN focuses on promoting cross-border cooperation and building capacity by sharing knowledge on emerging trends, regulatory changes and best practices for effective data protection.

Read more: *https://www.commonthreadnetwork.org/.*

L'Association Francophone des Autorités de Protection des Données Personnelles (AFAPDP)

Responsible entity: AFAPDP

Description: L'Association Francophone des Autorités de Protection des Données Personnelles (AFAPDP) is a network for data protection authorities of French-speaking countries and the international organisation of La Francophonie. Its goals include strengthening the effectiveness of the members of the association in the promotion and application of the right to the protection of personal data, as well as encouraging research and the sharing of good practices. The association organises an annual conference and a general assembly.

Read more: *https://www.afapdp.org/lafapdp.*

References

African Union (2020), "List of countries which have signed, ratified/acceded to the African Union Convention on Cyber Security and Personal Data Protection", https://au.int/sites/default/files/treaties/29560-sl-AFRICAN%20UNION%20CONVENTION%20ON%20CYBER%20SECURITY%20AND%20PERSONAL%20DATA%20PROTECTION.pdf (accessed on 20 December 2021). [51]

African Union (2014), "African Union Convention on Cyber Security and Personal Data Protection", https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf (accessed on 20 December 2021). [25]

APEC (2019), *APEC Steps Up Promotion of Cross-Border Privacy Rules*, https://www.apec.org/Press/News-Releases/2019/0912_CBPR (accessed on 20 December 2021). [37]

ASEAN (2021), "ASEAN Data Management Framework", https://asean.org/wp-content/uploads/2021/08/ASEAN-Data-Management-Framework.pdf (accessed on 20 December 2021). [24]

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 (accessed on 20 December 2021). [23]

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 (accessed on 20 December 2021). [22]

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 (accessed on 20 December 2021). [21]

ASEAN (2016), "ASEAN Framework on Personal Data Protection", https://asean.org/wp-content/uploads/2012/05/10-ASEAN-Framework-on-PDP.pdf (accessed on 20 December 2021). [20]

Asian Business Law Institute (2020), "Transferring Personal Data in Asia: A path to legal certainty and regional convergence", https://www.abli.asia/NEWS-EVENTS/Whats-New/ID/134 (accessed on 20 December 2021). [11]

Australian Government, Office of the Australian Information Commissioner (2016), *Ashley Madison joint investigaiton*, https://www.oaic.gov.au/privacy/privacy-decisions/investigation-reports/ashley-madison-joint-investigation (accessed on 20 December 2021). [41]

BSA (2018), "BSA Privacy Framework", https://www.bsa.org/files/policy-filings/BSA_2018_PrivacyFramework.pdf (accessed on 20 December 2021). [40]

Casalini, F. (2019), "Trade and cross-border data flows", *OECD Trade Policy Papers* No. 220, http://dx.doi.org/10.1787/b2023a47-en. [17]

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 (accessed on 20 December 2021). [35]

Dubai International Financial Centre (2021), "Model Clauses for Data Export to Non-adequate jurisdictions", https://www.difc.ae/business/operating/data-protection/data-export-and-sharing/ (accessed on 20 December 2021). [34]

EU WP29 [former Article 29 Data Protection Working Party of the European Union] (2014), *Opinion 02/2014 on a referential for requirements for Binding Corporate Rules submitted to national Data Protection Authorities in the EU and Cross Border Privacy Rules submitted to APEC CBPR Accountability Agents*, EU WP29 [former Article 29 Data Protection Working Party of the European Union], https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp212_en.pdf (accessed on 20 December 2021). [38]

European Commission (2021), *Data protection: Commission adopts adequacy decisions for the UK*, https://ec.europa.eu/commission/presscorner/detail/en/ip_21_3183 (accessed on 20 December 2021). [27]

European Commission (2017), "Exchanging and Protecting Personal Data in a Globalised World", *COM/2017/07 final*, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2017%3A7%3AFIN (accessed on 20 December 2021). [15]

European Commission (2021), *Adequacy decisions*, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (accessed on 20 December 2021). [26]

European Commission (2021), "Standard contractual clauses for international transfers", https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_en (accessed on 20 December 2021). [31]

European Union (2019), *Commission Implementing Decision (EU) 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan […]*, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019D0419&from=EN (accessed on 20 December 2021). [46]

G20 (2020), *G20 Digital Economy Ministers Meeting: Ministerial Declaration*, https://www.my.gov.sa/wps/portal/snp/content/news/newsDetails/CONT-news-230720201 (accessed on 20 December 2021). [8]

G20 (2019), *G20 Ministerial Statement on Trade and Digital Economy*, http://www.meti.go.jp/press/2019/06/20190610010/20190610010-1.pdf (accessed on 20 December 2021). [7]

G20 (2017), *G20 Digital Economy Ministerial Declaration: Shaping Digitalisation for an Interconnected World*, https://www.bmwi.de/Redaktion/DE/Downloads/G/g20-digital-economy-ministerial-declaration-english-version.html (accessed on 20 December 2021). [6]

G7 (2021), *G7 Digital and Technology Ministers Declaration*, https://www.gov.uk/government/publications/g7-digital-and-technology-ministerial-declaration (accessed on 20 December 2021). [9]

GSM Association (2018), "Regional Privacy Frameworks and Cross-Border Data Flows", https://www.gsma.com/publicpolicy/wp-content/uploads/2018/09/GSMA-Regional-Privacy-Frameworks-and-Cross-Border-Data-Flows_Full-Report_Sept-2018.pdf (accessed on 20 December 2021). [12]

ISO (2019), "ISO/IEC 27701:2019, Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines", https://www.iso.org/standard/71670.html (accessed on 20 December 2021). [39]

Ministry of Justice and Human Rights, Argentina (2016), "Dirección Nacional de Protección de Datos Personales", http://servicios.infoleg.gob.ar/infolegInternet/anexos/265000-269999/267922/norma.htm (accessed on 20 December 2021). [33]

OECD (2021), "Mapping commonalities in regulatory approaches to cross-border data transfers", *OECD Trade Policy Papers* No. 248, https://doi.org/10.1787/ca9f974e-en. [10]

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", *C(2021)42*, https://one.oecd.org/document/C(2021)42/en/pdf. [3]

OECD (2020), *OECD Digital Economy Outlook 2020*, https://doi.org/10.1787/bb167041-en. [14]

OECD (2017), *OECD Digital Economy Outlook 2017*, http://dx.doi.org/10.1787/9789264276284-en. [43]

OECD (2016), *Declaration on the Digital Economy: Innovation, Growth and Social Prosperity (Cancún Declaration)*, https://www.oecd.org/digital/Digital-Economy-Ministerial-Declaration-2016.pdf. [5]

OECD (2015), *Data-Driven Innovation: Big Data for Growth and Well-Being*, OECD Publishing, Paris, http://dx.doi.org/10.1787/9789264229358-en. [13]

OECD (2013), *The evolving privacy landscape: 30 years after the OECD Privacy Guidelines*, OECD Publishing, https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf. [2]

OECD (2007), *OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy*, https://www.oecd.org/sti/ieconomy/38770483.pdf. [42]

OECD (1980), "Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data", https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188. [1]

Office of the Privacy Commissioner (2020), "Model contract clauses for sending personal information overseas", https://privacy.org.nz/blog/model-contract-clauses-for-sending-personal-information-overseas/ (accessed on 20 December 2021). [32]

Organization of American States (2021), "Updated Principles on Privacy and Personal Data Protection", https://www.oas.org/en/sla/iajc/docs/Publication_Updated_Principles_on_Privacy_and_Protection_of_Personal_Data_2021.pdf (accessed on 20 December 2021). [19]

Personal Information Protection Commission, Government of Japan (2019), *The framework for mutual and smooth transfer of personal data between Japan and the European Union has come into force*, https://www.ppc.go.jp/en/aboutus/roles/international/cooperation/20190123/ (accessed on 20 December 2021). [30]

Personal Information Protection Commission, Government of Japan (2016), "Amended Act on the Protection of Personal Information (Tentative Translation)", *https://www.ppc.go.jp/files/pdf/Act_on_the_Protection_of_Personal_Information.pdf* (accessed on 20 December 2021). [29]

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* (accessed on 20 December 2021). [36]

RIPD (2017), "Estándares de Protección de Datos Personales para los Estados Iberoamericanos 2017", *https://www.redipd.org/es/documentos/estandares-iberoamericanos* (accessed on 20 December 2021). [18]

The Economist (2017), "The world's most valuable resource is no longer oil, but data", *https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data* (accessed on 20 December 2021). [47]

UNCTAD (2020), *Data Protection and Privacy Legislation Worldwide*, *https://unctad.org/page/data-protection-and-privacy-legislation-worldwide* (accessed on 20 December 2021). [4]

United Kingdom Government (2021), *UK government welcomes the European Commission's draft data adequacy decisions*, *https://www.gov.uk/government/news/uk-government-welcomes-the-european-commissions-draft-data-adequacy-decisions* (accessed on 20 December 2021). [28]

US Department of Commerce (2016), *Measuring the Value of Cross-Border Data Flows*, *https://www.commerce.gov/data-and-reports/reports/2016/09/measuring-value-cross-border-data-flows?q=%2Fdata-and-reports%2Freports%2F2016%2F09%2Fmeasuring-value-cross-border-data-flows* (accessed on 20 December 2021). [16]