Global Data Alliance Comments on
An International Arrangement for Partnership on
Data Free Flow with Trust

The Global Data Alliance (GDA) – representing companies based in Australia, Brazil, Canada, Denmark, Finland, France, Germany, Hungary, Ireland, Japan, Korea, Sweden, Switzerland, South Africa, the UK, and the US, and active across more than 15 sectors and 150 countries – urges the Group of Seven (G7) governments to advance a vision of *Data Free Flow with Trust* that supports the ability to transfer data across transnational digital networks while building digital trust.

The 2019 G20 Osaka Leaders Declaration urged countries to "work together to foster global economic growth, while harnessing the power of technological innovation, in particular digitalization, and its application for the benefit of all"; to "facilitate data free flow and strengthen consumer and business trust"; and to "cooperate to encourage the interoperability of different frameworks."[1] This Declaration was built in part on the vision of former Prime Minister Shinzo Abe, who spoke to the imperative of enabling the free flow of data – including medical, industrial, traffic, and other data – "to see no borders."

Consistent with the Global Industry Call on Data Free Flow with Trust recently issued by 35 associations from Canada, Japan, the EU, UK and US,[2] we support efforts by the G7 to operationalize this vision. To that end, this submission addresses:

(1) Benefits of cross-border data transfers;
(2) The challenge of increasing cross-border data restrictiveness;
(3) Definitional characteristics of cross-border data restrictions;
(4) Emerging challenges to digital trust; and
(5) Recommendations re the operationalization of "Data Free Flow with Trust."

I. Cross-Border Data Transfers Offer Many Benefits

We observe that the ability to access and transmit information across transnational digital networks supports not only broad economic, scientific, and societal benefits, but also governmental policy objectives, including those relating to:

1. Cybersecurity, including through an enhanced ability to detect and respond to cybersecurity threats, and to recover from cybersecurity incidents, through real-time cross-border data visibility into cyber-risk and international cyber-risk management;
2. Digital transformation of both governmental services (e.g., in relation to education, health, and safety) and non-governmental services, through the adaption of digital technologies across all sectors of the economy;
3. Environmental sustainability, including through improved cross-border carbon emissions tracking and predictive climate modeling based on multi-regional data sets that can help communities to prepare for climate-related risks and identify mitigation and remediation strategies;
4. Financial inclusion, including for those lacking access to banking resources, as well as fraud prevention, anti-money laundering, anti-corruption, and other financial transparency objectives;
5. Health, including through international research and development (R&D) to meet the challenges of pandemics and other health emergencies; cross-border healthcare regulatory collaboration;

and global medical humanitarian assistance and healthcare delivery;

6. Human-centric and trustworthy artificial intelligence, including through cross-border data analytics to help shared global challenges;
7. Innovation and scientific progress, including through cross-border access to knowledge and information needed to develop technological solutions to meet global challenges, as well as cross-border acquisition, maintenance, and protection of intellectual property (IP);
8. Privacy and personal data protection, including through commitments to protect personal data as it travels across digital networks, and through mechanisms that promote interoperability among personal data protection frameworks in different jurisdictions; and
9. Sustainable economic development and shared economic prosperity, including through greater cross-border connectivity and the enabling of flexible working arrangements, including for Micro-, Small-, and Medium-Sized Enterprises, underrepresented segments of the population and those based outside of major urban centers.

Cross-border data transfers are necessary and beneficial to many national and international policy objectives, as summarized above.[3]

II. Increasing Cross-Border Data Restrictiveness Threatens Many Global Priorities

The OECD has calculated an 800% increase in policies that undermine the ability to transfer data across transnational digital networks (*hereinafter* "restrictive cross-border data policies"). The OECD's 2023 Services Digital Restrictiveness Index explains that, across all major services sectors, the average cumulative increase in such policies was five times higher in 2022 than in 2021, and that barriers to cross-border data transfers topped the list of restrictions, with dozens of countries maintaining such restrictions.

This increase in cross-border data restrictiveness is not simply unsustainable; it is irreconcilable with shared global goals to address climate change, organized crime, terrorist financing, cybersecurity risks, public health and safety, and many other cross-border challenges. If the global community wishes to solve global problems together, its members must commit not to block the cross-border communication and exchange of information necessary to do so. Without this cross-border exchange, our collective ability to protect ourselves from a wide array of environmental, economic, health, safety, and security threats will be greatly diminished.

III. Characteristics of Cross-Border Data Restrictions

Today, cross-border data restrictions exhibit a wide range of characteristics. These restrictions may include: (a) policies that expressly require data to stay in-country; (b) policies that impose unreasonable conditions on transferring data abroad; (c) policies that prohibit the transfer of data abroad; (d) policies that require the use of domestic data centers or other equipment; (e) policies that require data centers to be owned or operated by nationals; (f) policies that impose minimum shareholding requirements for nationals or maximum shareholding limits for non-nationals; (g) policies that prohibit the application of non-national laws to digital infrastructure or data; and (h) policies that impose import or export duties or other restraints on data transfers as they traverse digital networks.

Whatever their differences, these restrictions frequently share the following characteristics: First, their design or application departs from the stated policy purpose because the restrictions are not necessary to achieve that stated purpose. Second, they are developed with minimal – if any – consideration of potential economic impacts or input from affected stakeholders or the public. Third, they often rely on inaccurate or

overstated claims of the benefits of restricting cross-border access to knowledge, know-how, and information.

IV. Emerging Challenges to Digital Trust

The aforementioned features of many cross-border restrictions – especially inaccurate claims of their beneficial impact coupled with a lack of governmental accountability in their adoption – are a primary challenge to digital trust today. This includes scenarios in which citizens and enterprises cannot trust that they will be able to transfer data for educational, health, research, or commercial purposes in the future, especially as governments increasingly interfere with data transfers, or declare data transfers to be illegal, on the basis of vague and/or previously unknown grounds.

To establish and strengthen digital trust, both governments and the private sector must play their part. First, governments should support digital trust by behaving in a manner that is transparent, democratically accountable, and consistent with good regulatory practices – particularly in view of the complexity and unintended consequences that may flow from restricting a person's ability to access, exchange, or transfer data vis-à-vis another person over a digital networks.[4] Governments should also support digital trust by refraining from imposing restrictions that undermine the core policy priorities outlined above, that are more onerous than necessary, or that serve discriminatory or other improper purposes.

Second, private entities should support digital trust by adhering to high standards of digital responsibility,[5] including through the adoption of strong internal controls in relation to cybersecurity, data security, financial transparency, and other regulatory compliance objectives. In connection with personal data protection, private entities should adhere to the so-called "accountability principle," which reflects the prevailing international legal norm relating to the cross-border movement of data.[6] Under this principle, organizations that transfer data globally should implement procedures to ensure that data will continue to be protected, even if it is transferred to countries other than where it was first collected. The accountability principle was first developed by the OECD,[7] and was subsequently endorsed and has been integrated in many legal systems including the EU's Global Data Protection Regulation (GDPR)[8] and the privacy frameworks of Japan,[9] New Zealand,[10] Singapore,[11] Canada,[12] and the United Kingdom. This principle is also a significant feature of the APEC Privacy Framework,[13] the APEC Privacy Recognition for Processors (PRP) system, the Global Cross Border Privacy Rules (CBPR) system,[14] and the ASEAN Model Contractual Clauses.[15] Reliance on the international accountability principle means that data should flow freely and with trust, provided that contractual commitments re personal data transfers (e.g., in standard contracts or other legal transfer mechanisms) are respected and enforced in a destination country with a strong rule of law and adherence to norms like the OECD Declaration on Government Access to Privately Held Data.

In sum, to build digital trust, we urge G7 Parties to: (a) reject any unfounded assumption that data transfer restrictions promote trust; (b) minimize and remove such restrictions; (c) renounce digital discrimination against non-nationals; (d) support data transfers on the basis of OECD and other international legal norms of accountability; and (e) focus on growing trust in government through greater democratic accountability when new cross-border data policies are being considered, duly respecting an evidence-based approach, good regulatory practices, and private sector best practices.

V. Recommendations re the Operationalization of "Data Free Flow with Trust"

Below, we outline general and specific recommendations re the operationalization of "Data Free Flow with Trust."

A. DFFT Institutional Arrangement for Partnership: General Recommendations

We welcome efforts by the G7 Japan Presidency to operationalize "Data Free Flow with Trust" ("DFFT") in 2023, particularly as the ability of governments and private entities to work together to solve collective challenges is impaired when countries isolate themselves and seek to hoard knowledge and information to the exclusion of others. Against this backdrop, the vision of DFFT has gained increasing importance.

The Global Data Alliance supports the concept of an "Institutional Arrangement for Partnership." (*hereinafter* "IAP"). The IAP should be carefully crafted to advance – and not undermine – DFFT. To that end, we recommend that all participating members reflect a shared commitment to core principles that:

1. Favor the seamless and responsible international movement of data; and

2. With respect to any measures that may impact the international movement of data, all members shall ensure that they are:

    a. Developed in a transparent and accountable manner;
    b. Non-discriminatory;
    c. Necessary to achieve a legitimate objective;
    d. Consistent with relevant international standards; and
    e. Interoperable with other countries' legal frameworks.

3. Avoid specific technology mandates, particularly if a rigorous cost-benefit analysis has not been undertaken and if such mandates are not based on international standards and may distort marketplace conditions.

B. DFFT Base Registry of Cross-Border Data Restrictions: General Recommendations

We could potentially support an international Base Registry of restrictive cross-border data policies, but also urge the G7 economies to be thoughtful and deliberate in designing such a registry. It is critical that the Registry not be misconstrued or misused to offer tacit endorsement or acceptance of improper cross-border restrictions or to promote the dissemination of such restrictions to more jurisdictions. The Base Registry should not overlook that impediments to data transfers and a lack of governmental accountability undermine legal certainty and digital trust.

Before agreeing to any public launch of such a Registry, we urge the G7 economies to carefully consider these implications – and to ensure that any Registry designed to be neutral, impartial, and supportive of DFFT.[16] We illustrate this point in two ways below.

First, developments since the 2019 Osaka Leaders' Statement have highlighted that some economies have invoked security or privacy as a pretense to impose cross-border data restrictions that have little relationship to security or privacy, and that may instead be designed to increase unconstrained and authoritarian governmental control over information. The Base Registry should avoid an uncritical assumption that all cross-border data restrictions premised on "cybersecurity" or "privacy" laws actually support digital trust.

Second, the Base Registry should also be carefully designed in relation to well-established measures, such as the GDPR. For example, the Registry could be subject to protectionist abuse by third countries if it contained elements implying that data transfers are "safest" when made to the EU and the roughly 15 jurisdictions deemed "adequate" under the GDPR. Including such elements in the Base Registry could unjustifiably deter data transfers to dozens of other countries around the world. Clearly, the Base Registry would not further "Data Free Flow with Trust" if it improperly implied that it is relatively "unsafe" to

transfer data to 80 percent of the countries in the world.

C. DFFT Institutional Arrangement for Partnership: Specific Recommendations

With the foregoing comments in mind, we respectfully and humbly offer the following concrete recommendations for the operationalization of the DFFT:

1. Structure and Organization: The IAP should develop as a knowledge and expert center on international data transfers. To that end, the IAP could include: (1) a government-to-government consultative body; (2) a private sector advisory body involving policy experts; and possibly (3) a permanent secretariat. First, establishing a purely government-to-government consultative body is important to allow government representatives to consult directly and freely with one another. It is important that governments retain a forum that is – for at least some purposes – reserved exclusively for participation by governmental representatives and free of outside interference. Second, developing a private sector advisory body with specific and demonstrated expertise in matters of cross-border data policy and digital trust is important to ensure that the government-to-government consultative body receives specific, constructive, and expert-level guidance. There should also be specific opportunities for the private sector body to communicate with governmental representatives.

2. Authority to Develop Economic, Sectoral, and Issue Reports: The IAP should have the authority to develop economic, sectoral, and issue-related reports regarding the benefits of DFFT across a variety of contexts. For example, the IAP could draft or commission in-depth analyses of the role of data transfers – and the costs of data transfer restrictions – in key sectors.[17] (The GDA has developed brief sector reports exploring the role of data transfers in the agriculture,[18] automotive,[19] clean energy, [20] finance, [21] healthcare, [22] logistics, [23] media, [24] medical technology, [25] pharmaceutical, [26] and telecommunications [27] sectors.) Similarly, the IAP could draft or commission in-depth analyses exploring the intersection of cross-border data policies with other governmental policy objectives. (The GDA has developed a series of issue reports that highlight the extent to which data transfers promote cybersecurity, [28] data analytics, [29] economic development,[30] environmental sustainability,[31] innovation/intellectual property,[32] privacy/personal data protection,[33] regulatory compliance,[34] and small business promotion.[35])

3. Authority to Undertake Pilot Projects: The IAP could also productively consider the development of pilot projects to build digital trust while supporting data transfers. Potential pilot projects include:

    a. Mapping national legal systems frameworks to promote implementation of the OECD Declaration on Government Access to Personal Data Held by Private Sector Entities. IAP participants could commit to map their respective legal systems to the OECD Declaration, and then reflect their endorsement of the Declaration. The OECD Declaration describes common values and practices of OECD member countries, distinguishing them from countries that lack the same commitment to digital trust, governmental accountability, and the rule of law. IAP participants could map their domestic legal systems to the seven principles underlying the OECD Declaration, namely:

        i. Legal basis (government access only permitted where a valid legal basis exists);
        ii. Legitimate aims (government access must support the pursuit of specified and legitimate aims, and not disproportionate);
        iii. Approvals (prior approval requirements for government access must be established and implemented per applicable standards, rules, and processes);
        iv. Data handling (data collected via government access must be handled only by

authorized personnel and subject to internal controls);

v. Transparency (legal frameworks for government access must be clear and easily accessible to the public, include public reporting by oversight bodies, and individual notification where applicable, etc.);
vi. Oversight (mechanisms for effective and impartial oversight must be in place); and
vii. Redress (individuals must have effective options for judicial and non-judicial redress to identify and remedy violations, which may include terminating access, data deletion, restoring data integrity, cessation of unlawful processing, etc.)

b. Case studies of restrictive data transfer policies in particular sectors: The IAP could map recent experiences with restrictive data transfer policies in particular sectors. For example, the IAP could examine restrictions imposed on automotive data tranfers. (Such measures have been imposed in several countries). This mapping exercise could include:

i. An inventory of cross-border data restrictions in a particular sector;
ii. A substantive description of those restrictions;
iii. A qualitative analysis of the: (a) nexus between those restrictions and their stated policy bases (e.g., cybersecurity); (b) degree of interoperability with international standards or other countries' laws; (c) potential impacts of the restrictions on the interests of other economies; and (d) due process and regulatory transparency practices adopted in the development of these restrictions.

Such sectoral mapping exercises should have a neutral, impartial, and global remit. They could cover any sectors in which data transfers have been heavily restricted, including automotive data, health data, and financial services data.

c. Performing an economic literature review regarding restrictive data transfer policies: In view of the OECD's estimates that restrictive data transfer policies have increased by 800% and that the rate of increase was five times more severe in 2022 than in 2021, the IAP could benefit from undertaking a detailed overview of this recent increase in cross-border data policy restrictions. This could include an examination of recent studies published by the OECD, universities, think tanks, private economists, or other international organizations (such as the WTO, World Bank, Asian Development Bank, etc.). This work could also summarize regional, sectoral, and substantive trends, and might also include a discussion of how to slow or reverse the threat of increasing cross-border data restrictiveness.

d. Globally developed industry standards for risk management: These can be utilized in order to incorporate industry best practices as well as to ensure a globally interoperable approach that is technology-neutral. Companies can demonstrate compliance with such standards through self-certification requirements. For example, one of the many risk-based approaches that rely on widely utilized international standards (such as ISO 27000 series or the NIST Cybersecurity Framework) can be used as the basis for enterprise risk management programs to demonstrate trust in data flows.

e. Case studies of regulatory best practices re cross-border data policies: In view of rapid increases in restrictive cross-border data policies, it might also be beneficial for the IAP to examine how the adoption of good regulatory practices and due process safeguards can promote better informed, and less disruptive, policymaking by countries around the world. A robust and thorough set of regulatory good practices to evaluate the foregoing factors can help policymakers improve the quality of proposed measures, and eschew unintended consequences that may be particularly pronounced when such measures unnecessarily restrict cross-border data transfers.[36] The IAP could assess cross-border data policymaking

from the perspective of regulatory best practices to:

i. Be transparent;[37]
ii. Draw from the best available evidence re the proposed cross-border data policy;[38]
iii. Analyze that evidence according to sound, objective, and verifiable methods;
iv. Provide opportunity for input from the public, experts, and interested stakeholders relating to the cross-border data policy;[39]
v. Provide a reasoned response to that input, and offer other procedural safeguards and due process.[40]
vi. Assess costs, benefits, and reasonably available alternatives (e.g., via regulatory impact assessments) with respect to proposed cross-border data policy, including:

1. The particular public policy outcome that the proposed measure is intended to achieve;
2. Whether the cross-border data restrictive features of the proposed measure are needed to achieve that outcome;
3. Whether other regulatory or non-regulatory alternatives could feasibly address that need or achieve that outcome with fewer data transfer restrictions;
4. The potential impacts of various alternatives over time (e.g., economic, social, environmental, public health, and safety effects) on the government, enterprises, and other persons who depend upon the ability to access technologies and transfer data across borders;
5. The grounds for concluding that a particular policy alternative is preferable to others.

These elements can help to substantiate and quantify the risks that the proposal purports to address, and analyze whether the proposed measure (and its most restrictive aspects) are necessary and proportionate to address any such risks.[41]

f. Consider development of an objective evaluation process for trusted suppliers: Another aspect of DFFT can involve the development of principles to identify trusted ICT suppliers. For example, under the Prague Proposals, a group of 30 plus countries worked together to increase supply chain trust diversification by focusing on the ability of suppliers to meet certain criteria. Potential considerations to evaluate supply chain trust diversification could include whether an enterprise:

i. Follows appropriate cybersecurity risk management processes;
ii. Adheres to responsible norms of corporate behavior;
iii. Is free from control by a government that has been found to engage in a pattern of digitally authoritarian acts or a pattern of malicious cyber activities against commercial entities, including in relation to the theft of intellectual property for commercial purposes; and
iv. Is based in a jurisdiction that has demonstrated its adherence to the principles underlying the OECD Declaration on Government Access to Personal data Held by the Private Sector.

4. Authority to Review Proposed Policies and Make Comments on New Restrictive Cross-Border Data Policies: The IAP could establish an affirmative and positive agenda to support cross-border data transfers and build digital trust. The IAP could also potentially comment on restrictive cross-border data policies.[42] This could be particularly important in the case of restrictive cross-border

data policies whose underlying justification purports to related to privacy, cybersecurity, or other goals, but whose design or application betrays an alternative purpose.[43] Nevertheless, such an approach would need to duly account for potential jurisdictional overlap with other institutions (such as the World Trade Organization).[44]

5. Foundational Charter: The IAP should be underwritten by a Foundational Charter to reflect:

    a. The IAP's subject matter focus and scope of activities;
    b. Organizational requirements (e.g., budget, method of appointment, required qualifications for permanent secretary and/or members of the private sector advisory body);
    c. Guiding principles (e.g., reflecting a shared commitment to "Data Free Flow with Trust"; expressly acknowledgement of the benefits of cross-border data transfers; reaffirmation of existing international norms that support cross-border data and digital trust;[45] and recognizing the imperative of disciplining restrictive cross-border data policies);
    d. A commitment to transparency by IAP member states;[46] and
    e. A reaffirmation of support for recent OECD initiatives designed to build digital trust and interoperability of national legal frameworks. These OECD initiatives include:
        i. The OECD Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data,[47]
        ii. The OECD Recommendation on Digital Security Risk Management for Economic and Social Prosperity[48] and recent Digital Economy Agreements;
        iii. The OECD Artificial Intelligence Principles;[49] and
        iv. The OECD Declaration on Government Access to Personal Data Held by Private Sector Entities.[50]

6. Analytical Tools: The IAP may wish to explore the development of analytical tools and checklists as a means of advancing its affirmative and positive agenda, including in relation to the evaluation of proposed or adopted measures. The GDA would be pleased to consult with the IAP on this.

7. Avoiding Unnecessary or Distortive Technology Mandates: While the IAP may find it productive or useful to discuss the technological aspects of cross-border data transfers, we urge the IAP not to propose particular technology solutions, particularly those that would potentially interfere with voluntary, industry-led international technical standards or those that could distort conditions of marketplace competition. Similar to cross-border data restrictions, such technological proposals should also not be advanced absent a marketplace cost-benefit analysis.

VI. Conclusion

We thank the G7 economies for the opportunity to share these GDA perspectives regarding the operationalization of DFFT. We welcome any questions or comments that you may have.

About the Global Data Alliance

The GDA is a multi-industry coalition of over 75 companies[51] that depend upon the ability to transfer data across borders and that are committed to high standards of digital responsibility and trust. Alliance members — which include companies based in Australia, Brazil, Denmark, France, Germany, Hungary, Ireland, Japan, Korea, Sweden, Switzerland, South Africa, the UK, and the US — are active across more than 15 sectors and 150 countries worldwide.

---

[1] G20 Osaka Leaders' Declaration (June 29, 2019), available at: http://www.g20.utoronto.ca/2019/2019-g20-osaka-leaders-declaration.html#:~:text=G20%20Osaka%20Leaders%27%20Declaration%20Osaka%2C%20Japan%2C%20June%2029%2C,united%20efforts%20to%20address%20major%20global%20economic%20challenges.

[2] *See* Global Data Alliance, *Global Industry Statement on Data Free Flow with Trust* (2023), at: https://globaldataalliance.org/wp-content/uploads/2023/04/04182023g7dfftglindustry.pdf

[3] In view of the demonstrated benefits of cross-border data transfers to many national and international policy objectives, we do not share the view that data transfers necessarily raise challenges related to privacy, data protection, intellectual property rights, and security.

[4] *See generally,* Global Data Alliance, *Cross-Border Data Policy Principles,* pp. 2-5 (2020), at: https://globaldataalliance.org/wp-content/uploads/2021/07/03022021gdacrossborderdatapolicyprinciples.pdf . G7 governments - and many other governments - have committed under their domestic laws and international agreements to meet good regulatory practice standards. We urge the Institutional Arrangement for Partnership to include mechanisms to examine the extent to which such good regulatory practices are satisfied. Generally speaking, this would require that cross-border data policy proposals: (1) be transparent; (2) draw from the best reasonably available evidence relevant to the proposed cross-border data policy; (3) Analyze that evidence according to sound, objective, and verifiable methods; (4) Provide opportunity for input from the public, experts, and interested stakeholders; and (5) Include other procedural safeguards and due process.

[5] *See generally,* Global Data Alliance, *Cross-Border Data Policy Principles,* pp. 1, 6 (2020),at: https://globaldataalliance.org/wp-content/uploads/2021/07/03022021gdacrossborderdatapolicyprinciples.pdf

[6] The GDA strongly supports the accountability model for international data transfers. This model was, first established by the OECD and subsequently endorsed and integrated in many legal systems and privacy principles. The accountability model provides an approach to cross-border data governance that effectively protects the privacy and consumer rights of individuals and fosters streamlined, robust data flows by that data be protected as required in the country of collection regardless of where it is subsequently transferred.

While governments are rightfully concerned with risks to privacy and data security, these risks are not dependent on the physical location of where data is stored or processed, or the location of the infrastructure supporting it. In fact, the effectiveness of data security and personal information protection is a function of the technologies, systems, and procedures put in place by the companies handling the personal information to protect the data.

To benefit from cross-border data transfers while simultaneously ensuring the responsible processing and protection of data, the focus of privacy policy and regulation needs to be on the quality and effectiveness of the mechanisms and the controls maintained to protect the data in question. The accountability model, therefore, continues to be an important tool in increasing privacy and security by requiring entities to ensure that data will continue to be properly protected, regardless of where the data is located.

Personal data protection and privacy frameworks that are based on a common set of international consensus-based principles facilitate cross border data transfers and drive innovation and business investment in local markets by promoting international interoperable legal frameworks upon which businesses of all sizes can rely. These coordination mechanisms also help to bridge current gaps in international privacy norms while facilitating the safe and secure international transfer of personal information. Such mechanisms may include private codes of conduct, contractual arrangements such as standard contractual clauses, certifications such as the APEC Cross Border Privacy Rules (CBPR), seals or marks, and mutual recognition arrangements such as the adequacy with the European Union General Data Protection Regulation (GDPR).

[7] OECD Privacy Framework 2013 (p15), http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

[8] Directive 95/46/EC (General Data Protection Regulation), https://eur-lex.europa.eu/eli/reg/2016/679/oj

[9] Act on the Protection of Personal Information, https://www.ppc.go.jp/en/legal/

[10] Privacy Act 2020, https://www.legislation.govt.nz/act/public/2020/0031/latest/LMS23223.html

[11] Personal Data Protection Act 2012, https://www.pdpc.gov.sg/Overview-of-PDPA/The-Legislation/Personal-Data-Protection-

Act

[12] Personal Information Protection and Electronic Documents Act fair information principles, https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/

[13] APEC Privacy Framework, https://www.apec.org/Publications/2017/08/APEC-Privacy-Framework-(2015)

[14] APEC Cross Border Privacy Rules system, https://www.apec.org/About-Us/About-APEC/Fact-Sheets/What-is-the-Cross-Border-Privacy-Rules-System

[15] ASEAN Model Contractual Clauses (2021), at: https://asean.org/wp-content/uploads/3-ASEAN-Model-Contractual-Clauses-for-Cross-Border-Data-Flows_Final.pdf; *See also,* Singapore Personal Data Protection Commission, Guidance for Use of ASEAN Model Contractual Clauses for Cross-Border Data Flows in Singapore (2022), at: https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Singapore-Guidance-for-Use-of-ASEAN-MCCs.pdf?la=en#:~:text=The%20ASEAN%20Model%20Contractual%20Clauses%20%28ASEAN%20MCCs%29%20are,parties%20that%20protects%20the%20data%20of%20data%20subjects.

[16] The Base Registry could also be kept up-to-date by the IAP permanent secretariat. Safeguards should be adopted or maintained to ensure that the design and operation of the Base Registry – and the permanent secretariat – remain accountable to IAP member governments.

[17] For example, one such a study could examine the health-related impacts of restrictive cross-border data policies from the perspective of basic health-related R&D; clinical trials; safety, pharmacovigilance, and adverse event reporting; healthcare delivery; and so forth. This could be a valuable exercise for the IAP: While privacy laws often impose the most stringent cross-border data restrictions on health-related data, health and safety regulations (e.g., relating to pharmaceuticals and medical devices) often mandate the cross-border exchange and sharing of such data, whether for research, clinical trial, and safety/pharmacovigilance purposes.

[18] Global Data Alliance, *Cross-Border Data & Agriculture* (2022), at: https://globaldataalliance.org/sectors/agriculture/

[19] Global Data Alliance, *Cross-Border Data & Automotive Technology* (2022), at: https://globaldataalliance.org/sectors/automotive/

[20] Global Data Alliance, *Cross-Border Data & Energy* (2022), at: https://globaldataalliance.org/sectors/energy/

[21] Global Data Alliance, *Cross-Border Data & Finance* (2022), https://globaldataalliance.org/sectors/finance/

[22] Global Data Alliance, *Cross-Border Data & Healthcare* (2022), https://globaldataalliance.org/sectors/healthcare/

[23] Global Data Alliance, *Cross-Border Data & Supply Chain Logistics* (2022), https://globaldataalliance.org/sectors/supply-chain-logistics/

[24] Global Data Alliance, *Cross-Border Data & Media and Publishing* (2022), https://globaldataalliance.org/sectors/media-publishing/

[25] Global Data Alliance, *Cross-Border Data & Medical Technologies* (2023), https://globaldataalliance.org/sectors/medical-technology/

[26] Global Data Alliance, *Cross-Border Data & Biopharmaceutical R&D* (2022), https://globaldataalliance.org/sectors/biopharmaceutical-rd/

[27] Global Data Alliance, *Cross-Border Data & Telecommunications* (2022), https://globaldataalliance.org/sectors/telecommunications/

[28] Global Data Alliance, *Cross-Border Data & Cybersecurity* (2023), https://globaldataalliance.org/issues/cybersecurity/

[29] Global Data Alliance, *Cross-Border Data & Data Analytics* (2023), https://globaldataalliance.org/issues/data-analytics/

[30] Global Data Alliance, *Cross-Border Data & Economic Development* (2023), https://globaldataalliance.org/issues/economic-development/

[31] Global Data Alliance, *Cross-Border Data & Environmental Sustainability* (2023), https://globaldataalliance.org/issues/environmental-sustainability/

[32] Global Data Alliance, *Cross-Border Data & Innovation* (2023), https://globaldataalliance.org/issues/innovation/

[33] Global Data Alliance, *Cross-Border Data & Privacy* (2023), https://globaldataalliance.org/issues/privacy/

[34] Global Data Alliance, *Cross-Border Data & Regulatory Compliance* (2023), https://globaldataalliance.org/issues/regulatory-compliance/

[35] Global Data Alliance, *Cross-Border Data & Small Business* (2023), https://globaldataalliance.org/issues/small-businesses/

[36] Commentary on good regulatory practices in relation to cross-border data policy includes: OECD, *Trade in the Digital Era* (2019), http://www.oecd.org/going-digital/trade-in-the-digital-era.pdf; World Economic Forum, Data Free Flow with Trust (DFFT): Paths towards Free and Trusted Data Flows, White Paper (2020), p. 18

https://www.jmfrri.gr.jp/content/files/Open/Related%20Information%20/WEF_May2020.pdf ("[P]olicy-makers should ensure that domestic measures affecting data are enacted in a transparent manner that allows opportunities for broad stakeholder input; are evidence-based and consider the technical and economic feasibility of requirements; require the publication of impact assessments to ensure the appropriateness and effectiveness of regulatory approaches; and are targeted and proportionate, and restrict trade as little as possible."); UNCTAD, *Data protection regulations and international data flows: Implications for trade and development* (2016), at: https://unctad.org/system/files/official-document/dtlstict2016d1_summary_en.pdf (recommending that the impact on smaller businesses be assessed with respect to proposed data protection legislation and data flow restrictions); Indian Council for Research on International Economic *Relations, Regulatory Burden on Micro, Small and Medium Businesses Due to Data Localisation Policies*, (Sept. 2019), at http://icrier.org/pdf/Regulatory-Burden.pdf; OECD, *Going Digital: Shaping Policies, Improving Lives* (2019), Molinuevo & Saez, Regulatory Impact Assessment Toolkit, The World Bank (2014), at: https://openknowledge.worldbank.org/bitstream/handle/10986/17255/9781464800573.pdf?sequence=1; ICTSD, Advancing Sustainable Development Through Services Regulation (2017)

[37] For example, governments should adopt pre-publication and final publication processes that specify implementation timelines, how various substantive concerns are addressed, the evaluation of evidence and expert input, and alternatives or other steps taken to mitigate negative impacts of the measure.
[38] For example, governments should seek out the best reasonably obtainable information relevant to the proposed policy, be transparent regarding information sources and any significant assumptions, and use sound statistical methodologies in analyzing that information.

[39] For example, governments should adopt procedural safeguards to ensure that any proposed measure that would impact cross-border data transfers is well-informed through input from experts, interested stakeholders, and the public. Such safeguards include:

- Advance publication, including an explanation of the measure's underlying objectives, the statutory or other legal basis underlying those objectives, and how the measure would achieve those objectives in light of available evidence;
- Opportunities for public comment; and
- Use of expert advisory groups, public-private consultative mechanisms, evaluation of best practices, and other means of protecting the public interest in thoughtful, deliberative policymaking.

[40] For example, governments should offer a retrospective review mechanism that allows for future enhancements or revisions of the measure, including from the perspective of cross-border data policy. The mechanism should permit the government to evaluate:

- How effective the measure has proven in achieving stated objectives;
- Whether changed circumstances or new information would justify a review of some aspects of the measure; and
- Whether there are any new opportunities to eliminate unnecessary regulatory burdens.

[41] *See e.g.,* OECD, *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, Art. 12 (2013), https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf ("Any restrictions to transborder flows of personal data should be proportionate to the risks presented, taking into account the sensitivity of the data, and the purpose and context of the processing.")
[42] We do not currently recommend that the IAP be vested with the authority to impose sanctions or penalties on governments that impose unnecessary or discriminatory cross-border data restrictions. G7 Members may wish to explore whether the IAP – or perhaps just its private sector advisory body – should issue advisory recommendations or comments.

[43] For example, such policies may: (1) reflect a choice of policy tools that are significantly more restrictive of cross-border data transfers than necessary to achieve the stated public policy goal; (2) contain elements that suggest the presence of discrimination vis-à-vis non-nationals or other unjustified or disguised restrictions on cross-border data transfers.

[44] In this regard, it would be important to avoid establishing an institutional arrangement that could lead to inconsistencies or redundancies between the IAP and other relevant international organizations such as relevant World Trade Organization (WTO) committees or the WTO Dispute Settlement Body.

[45] The existing international norms that should be reaffirmed include:

a. To permit the cross-border movement of data and the cross-border supply of services over digital networks, and to refrain from: (a) discrimination against non-national persons, products, services, or technologies; and (b) the imposition of greater restrictions on data flows than necessary or required to achieve a legitimate policy objective, consistent with their respective obligations under the WTO General Agreement on Trade in Services and recent Digital Economy Agreements. Recent Digital Economy Agreements include the Comprehensive and Progressive Trans-Pacific Partnership (Chapter 14), the Canada-US-Mexico Agreement (Chapter 19), and the UK-Singapore Digital Economy Agreement, among others. *See also* WTO General Agreement on Trade in Services, available at: https://www.wto.org/english/docs_e/legal_e/26-gats_01_e.htm

b. To adopt or maintain a legal framework for the protection of personal information or privacy, consistent with recent Digital Economy Agreements and the OECD Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data, at: https://legalinstruments.oecd.org/public/doc/114/114.en.pdf

c. To promote cybersecurity protection through effective cybersecurity risk management and real-time cross-border access to cybersecurity-related technologies and cyber threat indicators, consistent with the OECD Recommendation on Digital Security Risk Management for Economic and Social Prosperity and recent Digital Economy Agreements. OECD Recommendation on Digital Security Risk Management for Economic and Social Prosperity.

d. To promote human-centric development and deployment of Artificial Intelligence (AI), including through the application of AI risk management frameworks, consistent with the OECD Artificial Intelligence Principles, at: https://oecd.ai/en/ai-principles

e. To adhere to procedural safeguards to ensure that protections for privacy and other human rights and freedoms are in place with respect to law enforcement and national security access to personal data held by private sector entities, consistent with the OECD Declaration on Government Access to Personal Data Held by Private Sector Entities, at: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0487

[46] By endeavoring through their domestic procedures to offer ample opportunity for public input, IAP members can help build public awareness, confidence, and trust in the work of the IAP. The public may also be able in this way to supplement the guidance and input provided by the private sector advisory body.

[47] OECD Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data, available at: https://legalinstruments.oecd.org/public/doc/114/114.en.pdf
[48] OECD Recommendation on Digital Security Risk Management for Economic and Social Prosperity, available at: https://www.oecd.org/sti/ieconomy/Digital-Security-Risk-Management.htm#:~:text=The%202015%20OECD%20Recommendation%20on%20Digital%20Security%20Risk,empowerment%3B%20responsibility%3B%20human%20rights%20and%20fundamental%20values%3B%20co-operation
[49] The OECD Artificial Intelligence (AI) Principles, available at: https://oecd.ai/en/ai-principles
[50] Declaration on Government Access to Personal Data Held by Private Sector Entities, available at: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0487
[51] The Global Data Alliance is a cross-industry coalition of companies that are committed to high standards of data responsibility and that rely on the ability to transfer data around the world to innovate and create jobs. BSA | The Software Alliance administers the Global Data Alliance.