Data Beyond Borders 2.0

Laying the foundation for a digital global economy

2021

Contents

1. **Executive Summary** 3
2. **Cross-Border Data Flows Index** 6
   - 2.1 Key Findings 6
   - 2.2 Scores and Rankings 9
   - 2.3 Correlation Analysis 12
3. **Recommendations** 13
4. **Market Highlight: Singapore** 15

Appendix I. **Methodology** 18

Appendix II. **Country Scores** 19

Appendix III. **Statistical Analysis** 21

Appendix IV. **Abbreviations** 23

Appendix V. **References** 24

1. Executive Summary

The Covid-19 pandemic has accelerated the digitisation of the economy, underscoring the importance of data utilisation and data flows to economic recovery and growth. The constant, real-time movement of data across international borders that underpins global economic activity facilitates the movement of goods, services, and finance, and plays an essential role in driving emerging technologies such as artificial intelligence (AI), blockchain and the Internet-of-Things (IoT). As countries implemented physical shutdowns and social distancing measures, the access to digital tools, services, and infrastructure – which rely on the seamless movement of data – were fundamental in helping to sustain social and economic activity.

Data transfers have contributed:

$2.8 trillion
to global Gross Domestic Product (GDP)

growing
45 times
every ten years[1]

60%
of global GDP will be digitised by 2022[2]

Commissioned by Salesforce and prepared by Access Partnership, this report is the second edition of the Cross-Border Data Flows Index (CBDFI) which was first presented in 2019. The Index quantifies and evaluates eight regulatory dimensions that serve to either restrict or enhance the volume and variety of cross-border data flows for G20 economies. For this 2021 edition of the report, Singapore has been added to the original economies covered. It has created a conducive policy and regulatory environment for the development of its digital economy. Experiences from Singapore can be leveraged to enable seamless flow of data across borders.

The report recommends long-term measures to build trust and confidence as well as short-term initiatives that will deliver immediate results in offering clarity on data transfer mechanisms. Overall, the CBDFI finds that:

- Data-related policies and regulations of G20 economies are increasing in restrictiveness, the introduction of the notion of data sovereignty, and there is greater divergence on data transfer requirements. For businesses, these barriers raise regulatory complexity, resulting in more uncertainty, less transparency, and higher costs.
- On-going digitalisation of economies means that cross-border data flows will play a pre-eminent role in restoring economic growth and recovery.
- Approaches that encourage regulatory cooperation and alignment will build trust and confidence in cross-border data transfers.

The emergence of data sovereignty

Data sovereignty refers to the jurisdictional control or legal authority that can be asserted over data because its physical location is within jurisdictional boundaries, unlike data residency, which refers to the physical location of where data is stored.

Data sovereignty provides the government with the means to prevent unvetted access by foreign contractors, and entities to sensitive government data, whereas data residency does not.

The global regime for the regulation of cross-border data flows remains highly fragmented, and there is an increase in data sovereignty requirements. Across the G20, data-related policies of some G20 economies have become more inward-looking, prioritising the retention of data within borders. Recent policies and regulations in G20 economies risk undermining cross-border flows, ranging from highly restrictive data localisation mandates to policy statements about placing limits on the movement of data. At the same time, among G20 economies, the divergence in the requirements for cross-border transfers of personal data appears to be increasing, even as digital consumption has skyrocketed through the pandemic.

Cross-border data flow restrictions, as well as the variance in transfer requirements together can form formidable barriers for businesses.

Cross-border data flows can contribute to economic recovery

The G20 economies account for nearly:

80%
of the world's GDP

75%
of global trade

contracted
4.1%
during the COVID-19 pandemic.[3]

Given the on-going digitalisation of economies, cross-border transfers will play a crucial role in turbo-charging economic recovery.

The correlation analysis between total CBDFI scores and key economic indicators has shown a strong positive association between cross-border data flows, and economic growth, competitiveness, and opportunity. These findings are also supported by other research that shows that the data flows create greater economic growth and opportunity. The World Trade Organisation (WTO) estimates that by 2030, global trade will rise 34 percent through the use of digital technologies.[4] E-commerce platforms involved in cross-border transfers are estimated to have reduced the cost to local firms of distance in trade by 60 percent.[5]

At the country-level, Japan has once again topped the CBDFI with a total score of 38. This highlights that among G20 economies, it provides the strongest policy and regulatory framework for optimising cross-border data flows, while also providing sufficient privacy protections. It is followed by United Kingdom (score of 36), which has adopted an open a forward-looking approach in enabling cross-border flows of data and also protection of personal data. Singapore (34) and European Union (32) follow which has relatively comprehensive data-transfer frameworks in place, but growing emphasis on EU's 'digital sovereignty' has contributed to business uncertainty. At the other end of the CBDFI scorecard are important economies such as India (13), China (9) and Russia (6). Among them, China has implemented the most stringent data transfer restrictions, and India is also expected to pass legislation that could restrict data flows.

Data flows require regulatory cooperation and trust

Given the size and relevance of the G20, global recovery hinges on its ability to revive economic growth, and provide a leadership role in building long-term resilience. Based on the on-going digitalisation of economies, cross-borders transfers will play a crucial role in turbo-charging economic recovery. This makes it imperative and urgent for G20 economies to come together and lead efforts to enable the free flow of data across borders.

The first edition of this report had recommended maintaining multilateral discussions on mechanisms to reduce cross-border data barriers and increase cooperation. This is one area where significant progress has been made. The Joint Statement Initiative (JSI) on Electronic Commerce was launched in 2019 to develop rules on trade-related aspects of e-commerce.[6] Co-convened by Singapore, Australia and Japan, the JSI has 86 World Trade Organisation (WTO) members, representing over 90 percent of global trade. It has had a promising start. In December 2020, it announced the development of a consolidated text to form the basis of negotiations in 2021, and has highlighted that provisions which enable and promote the flow of data are key to a meaningful outcome.[7]

Recommendations

This report goes further to recommend measures that G20 economies can adopt and facilitate in building regulatory cooperation and trust. It outlines long-term approaches that address the drivers of restrictions on cross-border data transfers and seek to encourage innovation, as well as short-to-medium term initiatives that will deliver immediate results in providing clarity on data transfer mechanisms. The key recommendations are to:

Promote convergence and interoperability in privacy laws

Governments should reduce the variance in privacy regulations by basing them on international standards, such as the OECD Privacy Principles and APEC Privacy Framework. Cross-border transfer mechanisms such as certifications and data transfer agreements can deliver immediate results.

Expand bilateral and multilateral agreements to further facilitate data

Bilateral or multilateral agreements with clear rules on how to provide access to information needed for supervision or law enforcement can enhance trust and confidence among countries.

Make trusted data sharing frameworks the default

Embedding trust in international data transfers through robust data protection provisions, cybersecurity and data classification frameworks, will enable secure and seamless data flows.

Encourage innovation through forward-looking policies and regulations

Policy and regulatory landscape must adapt to and encourage rapid technological innovations that are addressing concerns driving data sovereignty, and facilitating cross-border data flows.

Enable digitisation of businesses and government services

Government policies directed at helping digitise public and private sector will further enable their growth, subject to having settings that enable free flow of data in their jurisdiction.

2. Cross-Border Data Flows Index

The Cross-Border Data Flows Index (CBDFI) provides a quantitative measure of G20 economies' approach to cross border data flows, allowing comparisons to be drawn between the effectiveness of their specific strategies. It examines the impact of regulations and provisions governing cross border flows across eight key dimensions:

1. **Data localisation requirements**, which can limit the import and export of foreign-sourced data-processing and data-storage services;
2. **Explicit provisions** allowing for international or extraterritorial transfers of personal data;
3. **Existence of specific mechanisms by which personal data is allowed to be transferred**, subject to conditions;
4. **Presence of a data classification framework** which enables cross-border data flows (distinct from an "official secrets act");
5. **Consent requirements** for the cross-border collection, storage, and dissemination of personal data;
6. **Participation in the EU's General Data Protection Regulation (GDPR)** regime, or meeting GDPR adequacy requirements;
7. **Participation in the APEC Cross-Border Privacy Rules (CBPR)** or similar regional system, promoting an accountability rather than an adequacy system;
8. **Whether a government has offered indications of being favourably or unfavourably positioned** on supporting cross-border data flows.

Appendix I provides details on the scoring mechanism for each of these dimensions.

Restrictions on cross-border data flows are rising

Across the G20, data-related policies are both complex and fragmented. In the two years since the first Data Beyond Borders Report, these policies have in many cases become more inward looking, prioritising issues of data sovereignty and the retention of data within borders.

While data flow restrictions are more pronounced in centrally-controlled markets, they are expanding to market economies as well, such as the EU. Box 1 below gives an overview of some recent policies and regulations in G20 economies ranging from highly restrictive data localisation mandates to policy statements about placing limits on the movement of data.

Restrictions on cross-border flows are still said to be chiefly driven by concerns about the security of data, ostensibly to ensure that its protection is not undermined by transfers to jurisdictions which may not offer the same safeguards, or that may limit timely access to data by law enforcement authorities.

Box 1: Cross-border data flow restrictions in G20 economies (2019-2021)

The European Union (EU) has advanced the idea of 'digital sovereignty', with growing calls across the European Commission (EC) and Member States for data to be stored and processed in the EU. GAIA-X, a federated and secure data infrastructure, is being incubated by the EU, and may accompany stricter localisation and licensing requirements. The Schrems II decision has invalidated the EU-US Privacy Shield, making the US a non-adequate country for transfer and storage of EU personal data. The proposed Data Government Act (DGA) introduces rules for international transfers of protected data held by the public sector.[8]

The United States (US) has a patchwork of state privacy laws, following the introduction of the California Consumer Privacy Act (CCPA). Numerous states have implemented or are implementing similar data privacy and security laws including Virginia, Washington, Texas, Massachusetts, and New York, creating more complexity in rules governing data transfers. Additionally, extensive restrictions on cross-border mergers and acquisitions, as well as procurement of telecommunications equipment and services have created some uncertainty for businesses.

China has announced several laws and policies that could impede the ability of foreign businesses to transfer data into and out of China.[9] The Cybersecurity Law of the People's Republic of China, the September 2020 Guiding Opinions on Implementing the Cybersecurity Classified Protection Scheme (CCPS), and CII Protection Scheme include specific data transfer restrictions. The Personal Information Protection Law similarly restricts the transfer of certain data outside of China. The Data Security Law (DSL) to come into force in September 2021, also has broad extraterritorial powers if data activities of overseas entities harm China's national security or public interests.

India already has sector-specific data localisation requirements in place, and could pass the Personal Data Protection Bill (PDP Bill) in 2021. The Bill includes requirements to localise critical data, maintain copies of sensitive data in India, and is unclear on the scope and definition of critical data and sensitive data.

Indonesia issued GR71 on the Operation of Electronic Systems and Transactions (GR71) in 2019,[10] which restricts storage and processing of public sector data to Indonesia. While it does not place the same restriction on private sector data, it gives sectoral regulators scope to define sector-specific requirements. Bank Indonesia (BI) and Otoritas Jasa Keuangan (OJK), for example, have continued with existing localisation requirements on financial sector data. The e-commerce regulation, GR80, also states that personal data can only be transferred to jurisdictions that offer the same or higher levels of protection as Indonesia, as determined by the Minister of Trade.

Brazil enforced the General Data Protection Law (LGPD) in August 2020, yet the newly established National Data Protection Authority (ANPD) has yet to become operational, creating legal uncertainty about cross-border transfer mechanisms. Another bill proposing data localisation requirements has been introduced in the Brazilian House of Representatives in September 2020.

Diversity in cross-border data flow requirements is increasing

Across the G20, privacy laws[11] have a high degree of variance in the requirements for cross-border transfers of personal data and, as our data demonstrates, this appears to be increasing, even as digital consumption has skyrocketed through the pandemic. This heterogeneity of requirements adds to regulatory complexity and uncertainty, resulting in less transparency, as well as less clarity on rules.

Consent is central to overseas data transfers in the majority of G20 economies. However, there are key differences in how consent requirements work and are implemented across countries. For example, opt-in consent is not required in Australia. Organisations must however, inform the individual that the same degree of protection provided under the Privacy Act will no longer apply after data has been transferred, and advise on the potential consequences of their consent being withdrawn.[12] In South Korea, on the other hand, opt-in consent is required. Organisations must inform the individual of the identity of the recipient, the purpose for which the recipient will use the data, the particulars of the personal data provided, the period for which the recipient will retain and use the personal data, and the fact that the individual is free not to give consent.[13] In other countries, such as China and India, consent alone is not adequate ground for data transfer for certain categories of data, with other conditions (such as approval by public authority) applying as well.[14]

International cooperation on data flows has shown limited progress

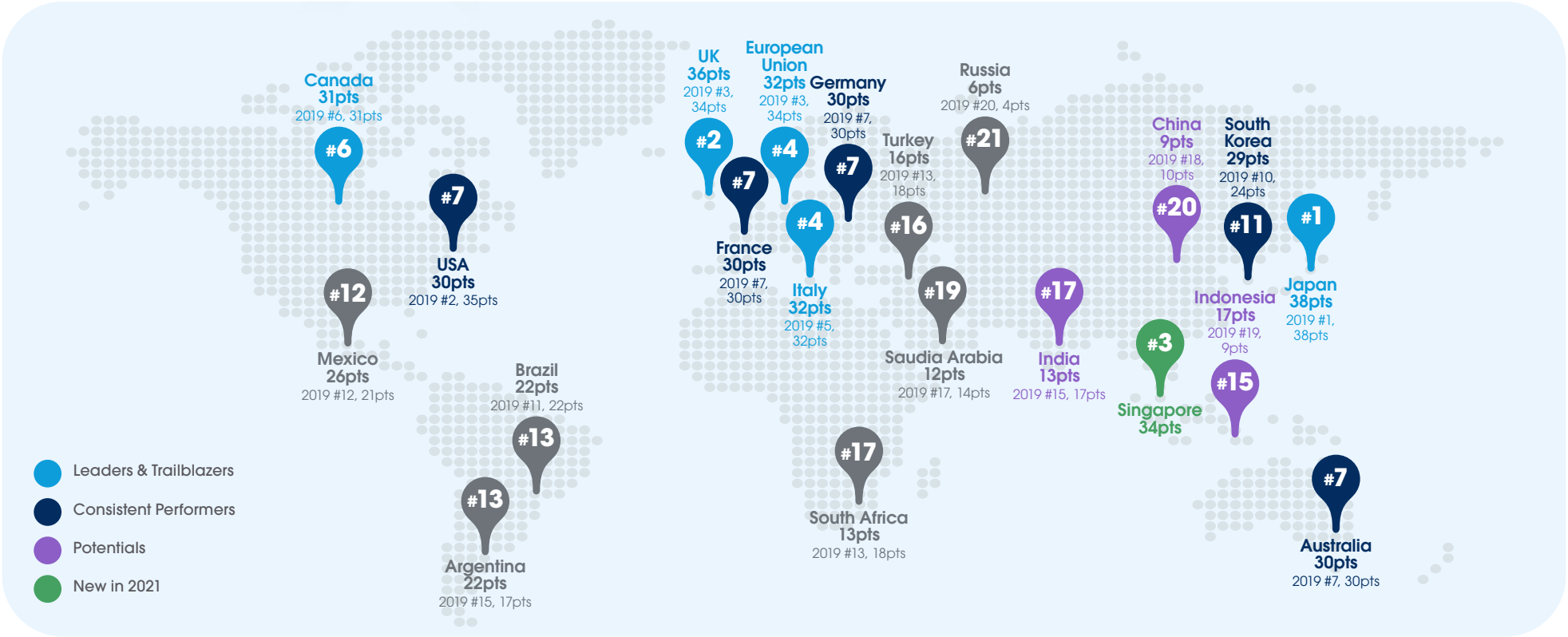
Many G20 economies have made a number of commitments to foster the development of their digital economies, and promote cross-border data flows. At the 2019 G20 Summit, Japan's Prime Minister Shinzo Abe launched the 'Osaka Track'. The initiative aims to enhance cross-border data flows with protections for personal information, intellectual property, and cybersecurity. The Osaka Track follows the concept of 'Data Free Flow with Trust' that calls for the creation of international regulations which will enable the free movement of data across borders. The G20 Digital Economy Ministers Declaration in June 2020 also recognised the importance of 'cross-border flow of data, information, ideas and knowledge for higher productivity, greater innovation, and improved sustainable development', while acknowledging that the protection of privacy and personal data were key concerns.[15]

While these commitments indicate an interest in promoting cross-border flows, there is little tangible progress in either reducing localisation mandates, or aligning regulations to support interoperability.

Commitments towards the free flow of data and prohibition of data localisation made in FTAs show more promise. The Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), United States-Mexico-Canada agreement (USMCA), US-Japan Digital Trade Agreement, Singapore-Chile-NZ Digital Economy Partnership Agreement (DEPA), and Singapore-Australia Digital Economy Agreement (SADEA) all include provisions to not restrict cross-border transfers of information, including personal information, by electronic means. They also prohibit the use or location of computing facilities as a condition for conducting business. Exceptions are however added, whereby parties can place restrictions, to achieve 'legitimate public policy objectives'. The recently signed Regional Comprehensive Economic Partnership (RCEP) also covers commitments on cross-border data flows, but with additional exceptions. For instance, on the location of computing facilities, it adds that the 'necessity behind the implementation of such legitimate public policy shall be decided by the implementing party'.

Across the G20 there is a diversity of policy and regulatory approaches towards cross-border data flows. As shown in Figure 1 below, the average score is 24 but more restrictive laws and policy measures have been introduced (or are forthcoming) since the first CBDFI in 2019. Some economies such as Indonesia and South Korea continue to have restrictions on international data transfers, but have made incremental progress through adoption of data protection good practices, guidelines on interpretation of laws, and international commitments to enhance cooperation with other countries.

Figure 1: Total CBDFI Scores of G20 Economies and Singapore



Leaders and trailblazers – have least restrictions on cross-border transfers

Japan (38) leads the G20 economies in the CBDFI rankings, followed by UK (36), Singapore (34), EU and Italy (tied at 32), and Canada (31). These economies have clear and consistent regulatory frameworks that enable cross-border data flows and offer strong data protection safeguards.

Japan has limited restrictions on cross-border transfers, and the Act on the Protection of Personal Information (APPI) provides clarity on data transfer provisions and mechanisms. In May 2021, it introduced amendments to the APPI to consolidate three laws related to personal data protection that will streamline data sharing between the central and local governments, and private sector. The Personal Information Protection Commission (PPC) has also been elevated to become the sole data protection authority. It is a participant of the APEC CBPR and in 2019, after introducing reforms to the APPI, it was granted an adequacy decision under GDPR for private sector organisations. It also simultaneously granted the EU a whitelist status based on the APPI. With the G20 Presidency in 2019, Japan advocated for cross-border data flows with the concept of 'Data Free Flow with Trust' and launched the Osaka Track, an international framework that promotes inter-government cooperation to enhance openness and trust in cross-border data flows. It has also committed to the free flow of information and prohibition of data localisation in the CPTPP and the US-Japan digital trade agreement.

The EU-UK Trade and Cooperation Agreement (TCA) was applied provisionally from 1st January 2021, and entered into force on 1st May 2021.[16] Apart from commitments in areas such as trade in goods and services, digital trade, intellectual property, and law enforcement it provided a bridging mechanism and allowed cross-border transfers of personal data from the EU to the UK, on the condition that the UK would not change its data protection legislation. On 28th June 2021, the European Commission adopted the adequacy decision for the transfers of personal data to the UK. The adequacy agreement will run for four years after which it will be subject to review and extension if UK maintains comparable privacy standards and level of data protection.[17] The mutual adequacy arrangement with Japan has not been affected by Brexit. In October 2019, it also signed the Bilateral Data Access Agreement with the US to allow law enforcement organisations access to digital evidence held by technology service providers located in their respective countries. This agreement has allowed both countries to bypass existing Mutual Legal Assistance Treaties (MLAT) processes, but agencies are limited to requesting data of only their own residents.

In the EU, the Free Flow of Non-Personal Data Regulation[18] and the European Strategy for Data[19] have been adopted in May 2019 and February 2020, respectively. The EC continues to promote cross-border data flows and prohibits Member States from imposing data localisation restrictions.

Canada's current policy and regulatory frameworks enable cross-border data flows.It has also made commitments in the USMCA to promote the free flow of data, and prohibit localisation mandates. In 2019, however, the Office of the Privacy Commissioner (OPC) reversed its long-standing position regarding cross-border transfers of personal data and launched a consultation proposing that organisations obtain consent when transferring personal information to third parties. Though no amendments were made to the 2009 Guidelines for Processing Personal Data Across Borders, there remains a strong interest in strengthening safeguards for cross-border transfers. The government has also proposed amendments to the Personal Information Protection and Electronic Documents Act (PIPEDA). Canada should ensure that proposed amendments to the legislation do not hamper cross-border flows and increase compliance costs of businesses.

Consistent performers – place certain limitations on cross-border transfers

France, Germany, US and Australia (tied at 30), and South Korea (29) are all in the middle of the pack. They are open to cross-border data flows, but impose certain conditions on cross-border transfers of data.


In France and Germany, there has been growing emphasis on digital sovereignty and "[limiting] dependency on infrastructures and services located outside of Europe"[20] In 2019, the two countries launched the GAIA-X project to link cloud service providers across Europe, followed by a joint statement highlighting the importance of "strengthening Europe's competitiveness in the global digital market".[21] Policy discussions in both countries have increasingly focused on limiting cross-border transfers of EU citizen data, for instance a report commissioned by the French Minister of Economy and Finance has recommended data localisation requirements to be imposed on payments data.[22]

The invalidation of the EU-US Privacy Shield has rendered the US a non-adequate country for transatlantic data transfers. This has had a significant impact on EU-US data transfers as many organisations now need to rely on other transfer mechanisms. In addition, the growing number of state privacy laws are contributing to legal complexity for data transfers. The US is however a participant of the APEC CBPR, and has made strong commitments to international data transfers (including financial information) in the USMCA and the US-Japan digital trade agreements.

In Australia, the Privacy Act details cross-border data transfer provisions and mechanisms. While there are no overarching restrictions, certain sector-specific limitations are placed on data flows. It has also made trade commitments to the free flow of data under the CPTPP, SADEA, and the Indonesia-Australia Comprehensive Economic Partnership Agreement (CEPA). Australian parliament passed the Telecommunications Legislation Amendment (International Production Orders) Bill 2020, to establish a framework for its enforcement agencies to access certain data held by communications providers outside of Australia for law enforcement and national security purposes. The Bill paves the way for a reciprocal cross-border data access regime with the United States under the CLOUD Act and provides an alternative to the MLAT process.[23]

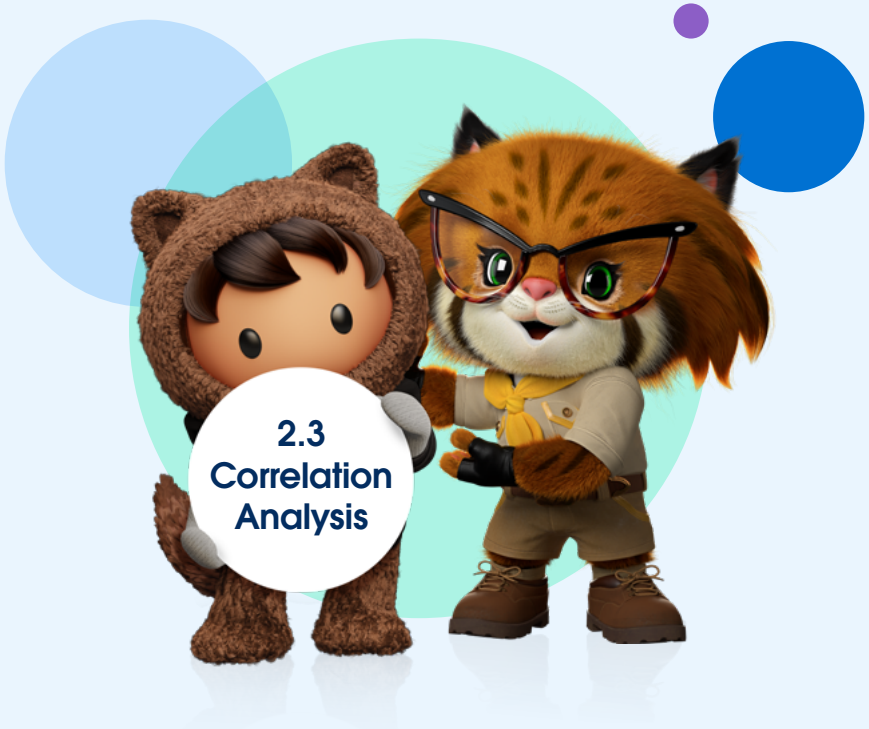
Potentials – have strict restrictions on cross-border transfers

At the lower end are Indonesia (17), India (13) and China (9). They each have strict data localisation requirements, but have the potential to make more gains, given the size of their economies.

Indonesia has shown notable progress in enhancing its privacy regime. With the introduction of GR71, localisation requirements for the private sector were lifted, although public sector data must only be managed, stored, and processed in-country. Even as data flow barriers have been reduced, sectoral regulators have been allowed to maintain data localisation mandates. The draft e-commerce regulation, GR80, also contains provisions that limit cross-border personal data transfer to third countries deemed having the same level of personal data standards and protection as Indonesia, which will be determined by the Ministry of Trade. As part of the Indonesia-Australia CEPA, it has made commitments to enabling cross-border data flows.

India has multiple sector-specific data localisation requirements, and the draft PDP Bill (expected to be passed in Parliament in 2021), also contains restrictions on cross-border transfers. Under the Bill, sensitive personal data may be transferred outside India for the purpose of processing, but will continue to be stored in-country. Critical personal data, which has not been defined, can only be processed in India. In recent years, the government has taken a strong position against cross-border data transfers, and the inadequacy of existing international frameworks in addressing concerns about data access.

In China, the Cybersecurity Law (CSL) requires operators to store personal information and important data generated from critical information infrastructures (CII) within the country. The Data Security Law (DSL) and the Measures for Security Assessment for Cross-Border Personal Data Transfer also contain provisions on data localisation. The Draft Personal Information Protection Law (PIPL) stipulates the conditions under which organisations will be permitted to access and transfer personal data outside of China, it also extends the data localisation obligations from operators of CII to personal information processors who process personal information in a volume that reach the threshold specified by the Cyberspace Administration of China (CAC), by mandating a security assessment. The finalisation of the PIPL will further limit interoperability with other regulatory regimes.



Given the wide ranging impact of cross-border data flows on the growth of various economic sectors including finance, health, e-commerce, and education, it can be challenging to comprehensively assess the economic value generated by global data flows, as well as the cost of imposing restrictions on them.

The European Centre for International Political Economy (ECIPE) has attempted to quantify the losses resulting from data localisation policies in six G20 economies. It estimates that the negative impact on GDP of a country would range from 0.7 percent to 1.1 percent if these requirements were imposed across all sectors of the economy.[24]

On the other hand, econometric modeling conducted by McKinsey has estimated that data flows alone could directly raise world GDP by 3 percent. For G20 economies, the benefits arising from unrestricted data flows could amount to USD2.93 trillion by 2025.[25]

Table 1 below shows a correlation analysis between the overall CBDFI scores and key economic indicators to evaluate the potential economic impact of cross-border data flows on G20 economies. The selected indicators include:

1. GDP per capita;
2. GDP growth;
3. Foreign Direct Investment (FDI), net inflows;
4. The World Bank's Ease of Doing Business Index;
5. Unemployment rates;
6. Employment to total population ratio;
7. AT Kearney's FDI Confidence Index;
8. The World Economic Forum (WEF)'s Global Competitiveness Index (GCI) and
9. Heritage Foundation's Index of Economic Freedom

The results indicate that CBDFI scores are positively correlated with GDP per capita, the Global Competitiveness Index (GCI) and the Index of Economic Freedom (all statistically significant at the 0.01 level). Therefore, there is a positive association between an enabling regulatory environment for cross-border data flows and economic growth, competitiveness, and opportunity.

Table 1: Correlation between CBDFI Scores and selected economic indicators

GDP per capita	GDP growth	FDI, net inflows	Ease of Doing Business Index	Unemployment Rate	Employment Ratio	FDI Confidence Index	Global Competitiveness Index	Economic Freedom Index
Strong	Insignificant	Insignificant	Insignificant	Insignificant	Insignificant	Insignificant	Strong	Strong

3. Recommendations

The CBDFI has shown that lower trust between countries has resulted in stringent data transfer requirements, as well as outright data localisation restrictions. The country-to-country variance in technical requirements for data transfers is adding to the regulatory complexity for businesses.

Given these observations and the current economic climate, we make five recommendations to enable cross-border data flows.

Promote convergence and interoperability in privacy laws

Across the G20, regulatory diversity presents a significant challenge in the effective transfer of data across borders. Governments should aim to reduce the variance in privacy laws, which will support businesses, and foster greater cooperation and trust amongst countries. Regulations based on international standards, such as the OECD Privacy Principles and APEC Privacy Framework can significantly reduce the heterogeneity in data transfer provisions.[26] This is a long-term goal that G20 governments must work towards.

In the short-term, G20 economies must cooperate in establishing mechanisms that imitate this convergence and enable cross-border transfers, without requiring amendments to laws (which is a lengthier process). These include:

i Certifications based on international standards: Businesses can utilise certifications based on standards as mechanisms for cross-border transfers. These may include regional or international standards such as APEC CBPR and ISO/IEC 27000.[27] International standards will be more cost effective as they will offer global coverage and limit the need to get multiple different certifications. National privacy authorities can provide guidance on attaining certifications.

ii Data transfer agreements: Businesses can be guided and supported in establishing data transfer agreements, and what key elements to include in them. Ongoing regional developments such as the ASEAN Model Contractual Clauses on Cross-Border Data Flows (MCC) can be leveraged, as they provide template contractual terms and conditions that can be included in binding legal agreements between businesses engaged in cross-border transfers.

Expand bilateral and multilateral agreements to further facilitate data

Restrictions on cross-border data transfers are driven chiefly by concerns about getting timely access to data for regulatory supervision or law enforcement purposes. G20 economies can address this concern by strengthening trust among regulatory authorities that they will have access to information needed to perform their functions. These could take the form of bilateral or multilateral agreements. With greater trust and confidence, data localisation requirements where access to data is a concern can be minimised.

International agreements to facilitate regulatory access to data across borders already exist. The UK and the US have signed a Bilateral Data Access Agreement to allow law enforcement agencies access to data held by technology service providers located in these countries. Agreements such as this can be used as building blocks for greater cooperation between other G20 economies. Several G20 economies have also made commitments in Free Trade Agreements (FTAs) to promote the free flow of data and limit data localisations measures. Of these, USMCA and the US-Japan Digital Trade Agreement contain explicit provisions for access to financial information.

Financial regulators may also come together through bilateral agreements that commit to financial institutions transferring data across borders. Singapore's Monetary Authority of Singapore (MAS) for instance, jointly issued a statement with the US Treasury in February 2020 to oppose measures that impose data localisation requirements on financial service suppliers.[28] In November 2020, it issued a similar statement with the Central Bank of Philippines (BSP), to promote data connectivity, without restrictions on the location of data storage and processing.[29]

Another example is Singapore led initiatives in the ASEAN Data Management Framework (DMF) and ASEAN Model Contractual Clauses (MCCs) for Cross Border Data Flows, to help with the free flow of data among ASEAN economies.

Make trusted data sharing frameworks the default

G20 governments should prioritise making trusted data sharing frameworks the default. In today's digitally driven global economy, businesses depend on seamless and uninterrupted data flows across national borders. As such, a policy in favour of secure cross-border data sharing should be seen as not only pro-economic growth but pro-innovation, critical in the post-Covid-19 recovery environment.

Trusted data sharing will not increase government or business risks and vulnerabilities if robust provisions and frameworks (both data protection and cybersecurity) are established and aligned across countries. On the contrary, imposing data localisation requirements increases the cost for all stakeholders, especially if the focus is on localisation rather than protection:

- Data localisation requirements also severely compromise the ability of regulatory authorities and businesses to detect and monitor fraud, money laundering, and terrorism financing activities. Limiting the flow of data across borders makes the process of detecting suspicious activities more complex.

An elemental component of establishing data sharing as the default is the use of data classification frameworks. While recognising that many countries in the G20 have yet to institute a risk-based data classification framework and should focus on doing so, governments must aim to go beyond meeting this foundational requirement for domestic purposes such as national security. Governments should review the purpose of their data classification frameworks and ensure that it not only aligns with but is leveraged upon in its larger data privacy regulations and policies to facilitate cross-border data sharing.

Encourage innovation through forward-looking policies and regulations

Digital technologies are constantly transforming. For instance, new and alternative models (such as federated learning and data trusts) that unlock siloed data, data learnings or algorithms across borders have the potential to address concerns driving data sovereignty and facilitate cross-border data flows.[30]

The policy and regulatory landscape of G20 economies must therefore, be agile, to adapt to, as well as encourage these technological innovations. This can be done through sandboxes, and testbeds, as well as self-regulation and co-regulation initiatives that include greater participation of industry stakeholders and citizens. By following such approaches, governments would also be adopting the most sustainable approach, one that will ensure that digital economies (national, regional, and inter-regional) remain robust for the future.

Enable digitisation of businesses and government services

Governments are undertaking digital transformation efforts to streamline internal processes, and broaden and expand the provision of public services. Citizens' expectations of government are also rising – they expect high quality services that are reliable, convenient, and fast, and for governments to protect their privacy. Nearly two-thirds of customers expect digital government services to perform at the standard of leading private companies, if not better.[31] Similarly, businesses are increasing investments in digital technologies and tools that cover all aspects of their business whether it be e-payments; marketplaces; payroll management; e-invoicing; marketing; and Customer Relationship Management (CRM).

The pandemic has accelerated the pace of these digitisation efforts. However, success hinges upon conducive regulatory environments that allow the free flow of data across borders. Digital technologies and tools rely on data that may be stored and processed in different locations around the globe. For businesses, they allow participation in international trade, and being part of global value chains (GVCs). Small and medium-sized (SME) businesses that account for nearly 90 percent of all businesses are then able to access national and international markets.[32]

Government policies to support digital transformation efforts of both the public and private sector must be accompanied by regulations that enable and facilitate international data transfers. Restrictions on the other hand, increase costs in terms of the time and resources spent in navigating rules and ensuring compliance, as well as the missed business opportunities.

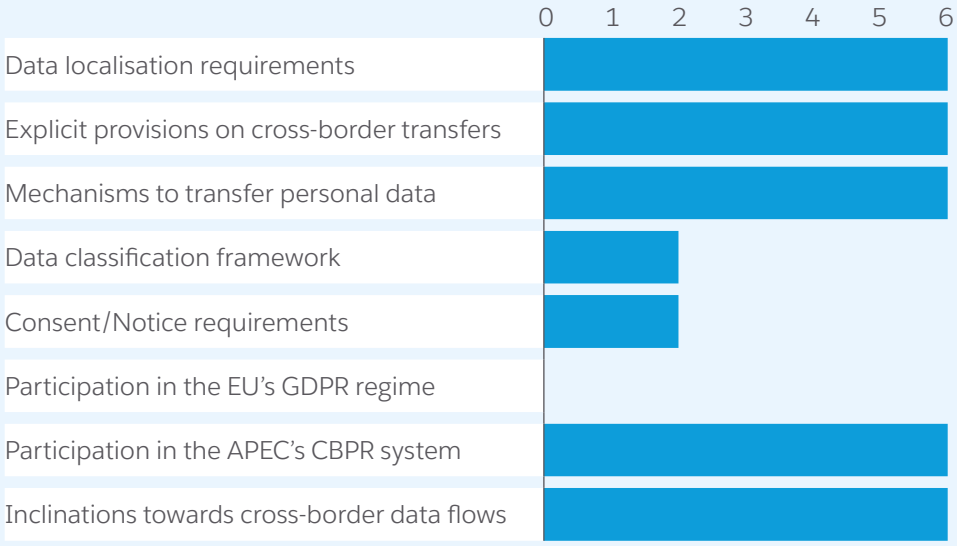
4. Market Highlight: Singapore

Singapore has a stellar track record in creating the right policy and regulatory environment for the development of the digital economy.

Supported by strong data protection regulation and guidelines, the country has taken an open and forward-looking approach in enabling the secure and seamless flow of data across borders.

Measured on each of the eight dimensions of the CBDFI, it receives a score of 34 (Figure 2).

Figure 2: CBDFI Scores for Singapore



The following is a detailed overview of Singapore's approach to cross-border data flows:

Dimension 1: Data Localisation requirements

Singapore's Personal Data Protection Act (PDPA) recognises the importance of cross-border flow of data, and has not imposed any overarching data localisation requirements. There are also no sectoral or targeted localisation requirements impacting data flows.

Dimension 2: Explicit provisions on extraterritorial transfers

The PDPA includes explicit provisions for businesses transferring personal data overseas. These provisions are meant to ensure that a comparable standard of protection is provided to data, and it provides businesses clarity and certainty.

Dimension 3: Mechanisms to transfer personal data across borders

Singapore has in place a clear mechanism that facilitates transfers of data, providing transparent and consistent rules for businesses. According to the PDPA, transferring organisations are required to take appropriate steps to ascertain and ensure that the recipient of the personal data outside Singapore is bound by legally enforceable obligation to provide a comparable standard of protection to the transferred personal data.[33] These obligations include the local law of the country of destination, a contract, binding corporate rules, or any other legally binding instrument. The PDPA has been amended by the PDPC to include certification, including the APEC CBPR and PRP Systems as valid data transfer mechanisms. In addition, Singapore has also encouraged certifications based on international transfers. The 2019 Advisory Guidelines on Cloud Services have noted that organisations processing personal data through CSPs can transfer data to other countries, if the CSPs are certified against relevant international standards.[34]

Singapore has also been a regional leader, initiating the ASEAN Data Management Framework (DMF) and ASEAN Model Contractual Clauses (MCCs) for Cross Border Data Flows. The DMF is a guide for businesses, particularly SMEs to implement a data management system. This includes guidelines for data governance structures and appropriate data protection safeguards depending on the underlying purpose of the dataset of interest throughout its lifecycle. While MCCs are contractual terms and conditions that may be included in the binding legal agreements between businesses when transferring personal data to each other across borders.

Dimension 4: Data classification framework

While Singapore does not have a data classification framework specifically for enabling cross-border data flows, the government introduced an Information Sensitivity Framework (ISF) in 2018 to standardise the protection of sensitive data. Public agencies are then able to apply consistent sensitivity categorisations to data, which aids inter-agency data sharing and data analytics as well.[35]

Dimension 5: Consent/Notice requirements for the international use of data

Consent requirements for transfer of personal data are a central feature of data transfer regimes across the world.

Singapore recognises the full range of transfer mechanisms, ranging from contracts and binding corporate rules to specified certification systems, including consent. Obtaining consent is not necessary when relying on any of the other permitted transfer mechanisms. But businesses that choose to rely on consent for transferring personal data will also need to include a 'reasonable summary in writing of the extent to which the personal data to be transferred to that country or territory will be protected to a standard comparable to the protection under the PDPA'.[36] This requirement is challenging, because in practice, in exception of specifically identified transfers to a particular organisation, it is difficult for businesses to provide such information in detail, given that each recipient will have different ways of implementing the protection of personal data.[37]

Dimension 6: Participation in the EU's GDPR regime

Singapore does not have the GDPR adequacy determination. Singapore's PDPA and the EU's GDPR are comprehensive and contain similarities in personal and extraterritorial scopes. In relation to cross-border transfers of personal data to a third country, they both provide for restrictions and exceptions, and establish legal ground and circumstances for lawful transfers.[38] However, unlike the PDPA, the GDPR provides for cross-border transfers made from a register, and allows transfers carried out under international agreements for judicial cooperation.[39] The legislations will however be more closely aligned in the future. The Personal Data Protection (Amendment) Act which took effect in February 2021, introduced a number of key changes, including mandatory data breach notification[40] and data portability provisions.

Dimension 7: Participation in the APEC's CBPR system

Singapore joined the APEC Cross-Border Privacy Rules (CBPR) System in 2018. It has amended the Personal Data Protection Regulations 2014, to recognise the CBPR certifications as modes of transfers of data overseas.[41]

CBPR is a government-backed data privacy certification that allows businesses to demonstrate compliance with internationally recognised data privacy protections.[42] It bridges gaps between national laws and regulations, and facilitates cross-border transfers. Currently, USA, Mexico, Japan, Canada, Singapore, Korea, Australia, Taiwan, and the Philippines are participating in the CBPR system.

Dimension 8: Inclinations towards allowing cross-border data flows

Singapore is a strong advocate for cross-border data flows. It has negotiated two Digital Economy Agreements (DEAs) – Digital Economy Partnership Agreement (DEPA) – with Chile and New Zealand; and the Singapore-Australia Digital Economy Agreement (SADEA). It has also launched negotiations with Korea on a Singapore-Korea Digital Partnership Agreement (SKDPA).[43] DEAs establish digital economy collaborations and aid countries in developing international frameworks for interoperability of standards and systems. Under the DEAs, Singapore has committed to allowing data to flow freely across borders and prohibit localisation, except for legitimate purposes such as personal data protection. Singapore is also part of the CPTPP that aims to promote the free flow of data across borders, and minimise data localisations requirements.

These agreements are in addition to other digital cooperation initiatives that Singapore is a part of, including as the co-convener at WTO's Joint Statement Initiative on E-commerce (JSI). The JSI has made some progress since launching in 2019, and has developed a consolidated text to form the basis of negotiations in 2021. Provisions that enable and promote the flow of data are central to these negotiations, and Singapore and Japan have also held information sessions for negotiators and the private sector on data flows and localisation rules in November 2020.[44]

Within the financial sector, the Monetary Authority of Singapore (MAS) has adopted supportive measures that include bilateral agreements that seek to ensure that financial services institutions can transfer data, including personal data, across borders. The February 2020 US-Singapore joint statement on Financial Services Data Connectivity, for example, opposes measures that impose data localisation requirements on financial service suppliers.[45] In November 2020, it issued a similar statement with the Central Bank of Philippines (BSP), underscoring the importance of data connectivity, without restricting the location of data storage and processing.[46]

Appendix I. Methodology

The Cross-Border Data Flows Index (CBDFI) provides a quantitative measure of G20 economies' policy and regulatory approach to cross-border data flows.

Each of the G20 economies is scored on a scale from 0 to 6 for a total score of 48. Table 2 below provides details on the scoring mechanisms, as well as on the assumptions that guided the scoring process.

The total economy score (with 48 being the maximum attainable score) is a comparable indication of where G20 economies stand relative to one another.

A higher score indicates a more conducive environment for cross-border data flows. Businesses relying on data transfers in these jurisdictions will encounter fewer barriers, lower compliance costs and high degree of legal stability and certainty. On the contrary, a lower score indicates the existence of restrictive and complex requirements that place increased costs and complexity for businesses transferring data across borders.

Table 2: Scoring mechanisms for regulations impacting data flows

Questions on regulations impacting data flows	Scoring mechanisms
1 Is there a data localisation requirement?	No (except for "official secrets act" or similar) = 6 No overarching data local requirement, but certain sector-specific limitations = 4 Some strong sector-specific requirements that increase uncertainty = 2 Forthcoming (or rumoured / likely) = 1 Yes = 0
2 Are there explicit provisions allowing for international or extraterritorial transfers of personal data / personally-identifiable data?	Yes (clearly enabling, and limited to no ambiguity) = 6 Yes, but some lack of clarity on certain types of personal data or some types of conditions = 4 Data residency requirements clearly or ambiguously appearing at times = 2 No (data residency is the clear default) = 0
3 Does the data protection law include a specific mechanism to transfer personal data across borders subject to certain protections?	Yes = 6 Upcoming = 3 Limited = 2 No = 0
4 Is there a data classification framework in use for enabling cross-border data flows (which is distinct from an "official secrets act" or similar)?	Explicit, clear, and published = 6 In use as part of a cloud first or similar framework = 4 In use by key government agencies and certain companies (but not published and perhaps not consistent) = 2 No = 0
5 Is there a consent or notice requirement for the collection, storage, or dissemination of personal data internationally or extraterritorially?	Written (or equivalent) consent is required = 0 Yes, express consent requirements (freely given, specific, informed, and unambiguous) = 2 No consent requirements but notice needs to be given to data subjects = 4 No consent or notice requirements = 6
6 Is the country a participant of the EU's GDPR regime or meets GDPR adequacy requirements?	No = 0 Partial = 3 Yes = 6
7 Is the country a participant of the APEC's CBPR or similar regional system (promoting an accountability rather than an adequacy system)?	Yes = 6 In application or in process = 4 Contemplated = 2 No = 0
8 Are there public record indicators that the government is actively promoting cross-border data flows beyond a clearly articulated data protection and data classification framework (e.g., proactive use of MLATs, international data flow network sharing participation, or clear and supportive policy statements from government leadership)?	Clear and binding legal or regulatory enablers = 6 Active use of existing frameworks such as MLATs = 4 Clear and supportive policy statement from very senior government representative (e.g., President, Central Bank Governor) = 2 No = 0

Source: Access Partnership Research

Appendix II. Country Scores

Table 3: Detailed CBDFI Scores for G20 Economies (out of 48)

	Data Regulations / Requirements	Argentina	Australia	Brazil	Canada	China	European Union	France	Germany	India	Indonesia
	Rank	13	7	13	6	20	4	7	7	17	15
1	Is there a data localisation requirement?	4	4	4	4	0	4	2	2	0	2
2	Are there explicit provisions allowing for international or extraterritorial transfers of personal data / personally identifiable data?	4	6	4	4	4	6	6	6	4	4
3	Does the data protection law include a specific mechanism to transfer personal data across borders subject to certain protections?	2	2	2	0	3	6	6	6	3	3
4	Is there a data classification framework in use for enabling cross-border data flows (which is distinct from an "official secrets act" or similar)?	2	2	6	6	2	4	4	4	0	2
5	Is there a consent or notice requirement for the collection, storage, or dissemination of personal data internationally or extraterritorially?	0	4	2	2	0	2	2	2	2	2
6	Is the country a participant of the EU's GDPR regime or meets GDPR adequacy requirements?	6	0	0	3	0	6	6	6	0	0
7	Is the country a participant of the APEC's CBPR or similar regional system (promoting an accountability rather than an adequacy system)?	0	6	0	6	0	0	0	0	2	0
8	Are there public record indicators that the government is actively promoting cross-border data flows beyond a clearly articulated data protection and data classification framework (e.g., proactive use of MLATs, international data flow network sharing participation, or clear and supportive policy statements from government leadership)?	4	6	4	6	0	4	4	4	2	4
	Total	22	30	22	31	9	32	30	30	13	17

Table 3: Detailed CBDFI Scores for G20 Economies (out of 48) cont.

	Data Regulations / Requirements	Italy	Japan	Mexico	Russia	Saudia Arabia	Singapore	South Africa	South Korea	Turkey	UK	USA
	Rank	4	1	12	21	19	3	17	11	16	2	7
1	Is there a data localisation requirement?	4	6	4	0	2	6	1	2	2	4	4
2	Are there explicit provisions allowing for international or extraterritorial transfers of personal data / personally identifiable data?	6	6	4	2	2	6	6	4	4	6	4
3	Does the data protection law include a specific mechanism to transfer personal data across borders subject to certain protections?	6	6	2	0	0	6	2	3	6	6	2
4	Is there a data classification framework in use for enabling cross-border data flows (which is distinct from an “official secrets act” or similar)?	4	0	2	2	4	2	0	2	0	6	6
5	Is there a consent or notice requirement for the collection, storage, or dissemination of personal data internationally or extraterritorially?	2	2	2	0	0	2	2	2	2	2	2
6	Is the country a participant of the EU’s GDPR regime or meets GDPR adequacy requirements?	6	6	0	0	0	0	0	6	0	6	0
7	Is the country a participant of the APEC’s CBPR or similar regional system (promoting an accountability rather than an adequacy system)?	0	6	6	0	2	6	0	6	0	0	6
8	Are there public record indicators that the government is actively promoting cross-border data flows beyond a clearly articulated data protection and data classification framework (e.g., proactive use of MLATs, international data flow network sharing participation, or clear and supportive policy statements from government leadership)?	4	6	6	2	2	6	2	4	2	6	6
	Total	32	38	26	6	12	34	13	29	16	36	30

Appendix III. Statistical Analysis

Table 4 below provides a detailed breakdown of the calculations used to determine the impact of cross-border data flows on economic performance.

Table 4: Correlations between CBDFI and Selected Economic Indicators

		GDP per capita	GDP growth	FDI net inflow	Ease of Doing Business Index	Unemployment Rate	Employment Ratio	FDI confidence	Global Competitiveness Index	Index of Economic Freedom
CBDFI	Pearson Corr.	.766**	-.297	.234	.424	-.339	.250	.335	.678**	.698**
	Sig. (2-tailed)	.000	.192	.308	.055	.133	.274	.288	.001	.000
	N	21	21	21	21	21	21	12	21	21

Note: **: Correlation is significant at the 0.01 level (2-tailed)
N: G20 Economies, and Singapore

Table 5 compiles the eight indicators of economic growth, competitiveness and opportunity that were used to calculate the correlations.

Table 5: Selected Indicators used for Correlation Analysis

	GDP per capita (current US$), 2019	GDP annual growth rate, 2019	Foreign direct investment, net inflows (% of GDP)	Ease of Doing Business Index (score)	Unemployment, total (% of total labour force)	Employment to population ratio	FDI confidence index	Global Competitiveness Index	Index of Economic Freedom	CBDFI score
Argentina	9,912.30	-2.1	1.5	59	9.8	54.4	--	57	53.1	22
Australia	55,060.30	2.2	2.9	81.2	5.2	62.6	1.98	79	82.6	28
Brazil	8,717.20	1.1	4	59.1	11.9	55.1	1.65	61	53.7	22
Canada	46,194.70	1.7	2.8	79.6	5.7	62	2.2	80	78.2	31
China	10,261.70	6.1	1.1	77.9	5.2	67.3	1.95	74	59.5	9
European Union	34918.5	1.6	1.6	76.2	6.7	53.7	--	72	70.9	32
France	40,493.90	1.5	1.9	76.8	8.4	50.7	2.09	79	66	30
Germany	46,445.20	0.6	1.9	79.7	3.1	60	2.15	82	73.5	30
India	2,099.60	4.2	1.8	71	5.3	45.4	--	61	56.5	13
Indonesia	4,135.60	5	2.2	69.6	3.6	65.7	--	65	67.2	17
Italy	33,228.20	0.3	1.5	72.9	10	44.9	1.94	72	63.8	32
Japan	40,246.90	0.7	0.7	78	2.4	60.6	2.14	82	73.3	38
Mexico	9,946.00	-0.1	2.3	72.4	3.5	58	--	65	66	26
Russia	11,585.00	1.3	1.9	78.2	4.5	59.4	--	67	61	6
Saudi Arabia	23,139.80	0.3	0.6	71.6	6	52.5	--	70	62.4	12
Singapore	65,233.30	0.7	28.3	86.2	3.1	65.2	1.87	85	89.4	34
South Africa	6,001.40	0.2	1.3	67	28.5	39.5	--	62	58.8	16
South Korea	31,846.20	2	0.6	84	3.7	61.2	1.72	80	74	29
Turkey	9,126.60	0.9	1.2	76.8	13.7	45.7	--	62	64.4	16
United Kingdom	42,330.10	1.5	0.7	83.5	3.7	60.9	2.06	81	79.3	33
United States	65,297.50	2.2	1.6	84	3.7	60.8	2.26	84	76.6	30

Sources:
GDP per capita (current US$), 2019, World Bank, https://data.worldbank.org/indicator/NY.GDP.PCAP.CD
GDP annual growth rate, 2019, World Bank, https://data.worldbank.org/indicator/NY.GDP.MKTP.KD.ZG
Foreign direct investment, net inflows (% of GDP), 2019, World Bank, https://data.worldbank.org/indicator/bx.klt.dinv.wd.gd.zs
Ease of doing business score, 2020, World Bank, www.doingbusiness.org/en/data/doing-business-score
Unemployment, total (% of total labour force), 2019, World Bank, https://data.worldbank.org/indicator/SL.UEM.TOTL.NE.ZS
Employment to population ratio, 2019, World Bank, https://data.worldbank.org/indicator/SL.EMP.TOTL.SP.NE.ZS
FDI Confidence Index 2020, AT Kearney, www.atkearney.com/foreign-direct-investment-confidence-index
Global Competitiveness Report 2019, WEF, http://www3.weforum.org/docs/WEF_TheGlobalCompetitivenessReport2019.pdf
2020 Index of Economic Freedom, heritage.org, https://www.heritage.org/index/ranking?version=633

Appendix IV. Abbreviations

AI	Artificial Intelligence
APEC	Asia-Pacific Economic Cooperation
ASEAN	Association of South East Asian Nations
BI	Bank Indonesia
BSP	Central Bank of Philippines
CBDFI	Cross Border Data Flow Index
CBPR	Cross Border Privacy Rules (APEC)
CCPA	California Consumer Privacy Act
CCPS	Cybersecurity Classified Protection Scheme (China)
CEPA	Indonesia-Australia Comprehensive Economic Partnership Agreement
CPTPP	Comprehensive and Progressive Agreement for Trans-Pacific Partnership
CSPs	Cloud Service Providers
DEPA	Singapore-Chile-NZ Digital Economy Partnership Agreement
DMF	Data Management Framework
EC	European Commission
ECIPE	European Centre for International Political Economy
EU	European Union
FTAs	Free Trade Agreements
FDI	Foreign Direct Investment
G20	Group of Twenty
GDP	Gross Domestic Product
GDPR	General Data Protection Regulation
IoT	Internet of Things
ISO	International Organisation of Standardisation
MAS	Monetary Authority of Singapore
MCC	Model Contractual Clauses
MLATs	Mutual Legal Assistance Treaties
OECD	Organisation for Economic Cooperation and Development
OJK	Otoritas Jasa Keuangan
SADEA	Singapore-Australia Digital Economy Agreement
SKDPA	Singapore-Korea Digital Partnership Agreement
USMCA	United States-Mexico-Canada agreement
WEF	World Economic Forum
WTO	World Trade Organisation

Appendix V. References

1 Trade and Cross-Border Data Flows, OECD, 2019

2 FutureScape–Worldwide IT Industry 2019 Predictions, IDC, 2018

3 UN (2021) World Economic Situation Prospects, https://www.un.org/development/desa/dpad/wp-content/uploads/sites/45/WESP2021_FullReport.pdf

4 Joshua P. Meltzer (2020) How APEC can address restrictions on cross-border data flows, https://app.glueup.com/resources/protected/organization/895/event/29824/f4ede14f-b70e-45a4-84e4-098bc975a67b.pdf

5 Global Data Alliance (2020) Submission for National Trade Estimate on Foreign Trade Barriers, https://www.globaldataalliance.org/downloads/10292020GDA2020NTESubmission.pdf

6 MTI (2019) Australia, Japan and Singapore welcome WTO electronic commerce negotiations, https://www.mti.gov.sg/-/media/MTI/Newsroom/Press-Releases/2019/01/Australia-Japan-and-Singapore-welcome-WTO-electronic-commerce-negotiations.pdf

7 METI (2020) Joint Statement Initiative on E-commerce: Co-Conveners Update, https://www.meti.go.jp/press/2020/12/20201215001/20201215001-1.pdf

8 Council of the European Union, Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act), https://data.consilium.europa.eu/doc/document/ST-6297-2021-INIT/en/pdf

9 Global Data Alliance (2020) Submission for National Trade Estimate on Foreign Trade Barriers, https://www.globaldataalliance.org/downloads/10292020GDA2020NTESubmission.pdf

10 This replaced the highly contentious GR82.

11 Saudi Arabia does not have a specific national data protection regulation.

12 ABLI (2020) Comparative Review of Data Transfer Laws and Regulations in Asia, https://app.glueup.com/resources/protected/organization/895/event/29824/9209bc06-f8e0-4aff-bc53-1f4cc8912d0d.PDF

13 Microsoft (2019) Strengthening Privacy Regulatory Coherence In Asia, https://www.microsoft.com/cms/api/am/binary/RE4KiGz

14 ABLI (2020) Comparative Review of Data Transfer Laws and Regulations in Asia, https://app.glueup.com/resources/protected/organization/895/event/29824/9209bc06-f8e0-4aff-bc53-1f4cc8912d0d.PDF

15 G20 Digital Economy Ministers Meeting 2020, http://www.g20.utoronto.ca/2020/2020-g20-digital-0722.html#:~:text=Ministerial%20D-eclaration%3A%20G20%20Digital%20Economy%20Ministers%20Meeting%2C%20July%2022%2C%202020&text=Building%20on%20the%20achievements%20and,the%2021st%20century%20for%20all

16 European Commission (2021) The EU-UK Trade and Corporation Agreement, https://ec.europa.eu/info/relations-united-kingdom/eu-uk-trade-and-cooperation-agreement_en

17 European Commission (2021) Press Release - Data protection: Commission adopts adequacy decisions for the UK, https://ec.europa.eu/commission/presscorner/detail/en/ip_21_3183

18 European Commission, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018R1807

19 European Commission, https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy

20 TechEu (2020) Europe's pursuit of digital sovereignty could affect the future of the Internet, https://tech.eu/-features/32780/europe-digital-sovereignty/

21 Telecom Paper (2020) Germany, France sign common paper to support European cloud infrastructure Gaia-X, https://www.telecompaper.com/news/germany-france-sign-common-paper-to-support-european-cloud-infrastructure-gaia-x--1327334

22 Lexology (2020) French report proposes payments data localisation requirements, https://www.lexology.com/library-/detail.aspx?g=cdc2f545-70bb-4673-959d-c0be5f49c4ff

23 Telecommunications Legislation Amendment (International Production Orders) Bill 2020, https://www.aph.gov.au/Parliamentary_Business/Bills_LEGislation/Bills_Search_Results/Result?bId=r6511

24 ECIPE (2014), The Costs of Data Localisation: A Friendly Fire on Economic Recovery, http://ecipe.org/publications/dataloc

25 McKinsey Global Institute (2016), Digital globalization: The new era of global flows, www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalization-the-new-era-of-global-flows; GDP for France, Germany and Italy have been excluded in the calculation to avoid double counting under EU areas.

26 Joshua P. Meltzer (2020) How APEC can address restrictions on cross-border data flows, https://ab46bb92-a539-4d61-9a28-f77eb5f41c00.usrfiles.com/ugd/ab46bb_830a70b4f8dc4508a38d3e480ffa9cb2.pdf

27 Microsoft (2019) Strengthening Privacy Regulatory Coherence In Asia, https://www.microsoft.com/cms/api/am/binary/RE4KiGz

28 U.S. Department of the Treasury, United States – Singapore Joint Statement on Financial Services Data Connectivity, https://home.treasury.gov/news/press-releases/sm899

29 Monetary Authority of Singapore, Joint Statement of Intent on Data Connectivity between Bangko Sentral ng Pilipinas and The Monetary Authority of Singapore, https://www.mas.gov.sg/news/media-releases/2020/joint-statement-of-intent-on-data-connectivity-between-bsp-and-mas

30 WEF (2020) A Roadmap for Cross- Border Data Flows: Future-Proofing Readiness and Cooperation in the New Data Economy, https://www.weforum.org/whitepapers/a-roadmap-for-crossborder-data-flows-future-proofing-readiness-and-cooperation-in-the-new-data-economy

31 BCG & Salesforce (2020) The Trust Imperative, https://www.salesforce.com/au/form/conf/pov-report/?leadcreated=true&redirect=true&DriverCampaignId=7010M000001z0DpQAI&FormCampaignId=7010M000001z0DuQAI

32 WTO (2016) World Trade Report, https://www.wto.org/english/res_e/publications_e/wtr16_e.htm

33 PDPC (2017) Advisory Guidelines on Key Concepts in the PDPA, https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/the-transfer-limitation-obligation---ch-19-(270717).pdf

34 Microsoft (2019) Strengthening Privacy Regulatory Coherence In Asia, https://www.microsoft.com/cms/api/am/binary/RE4KiGz

35 Smart Nation Public Sector Data Security Review Committee Report, https://www.smartnation.gov.sg/docs/default-source/press-release-materials/annexes-to-the-psdsrc-final-report.pdf?sfvrsn=39ff3472_2

36 PDPC (2017) Advisory Guidelines on Key Concepts in the PDPA, https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/the-transfer-limitation-obligation---ch-19-(270717).pdf

37 ABLI (2020) Comparative Review of Data Transfer Laws and Regulations in Asia, https://app.glueup.com/resources/protected/organization/895/event/29824/9209bc06-f8e0-4aff-bc53-1f4cc8912d0d.PDF

38 Comparing privacy laws: GDPR v. Singapore's PDPA, https://www.dataguidance.com/sites/default/files/gdpr_v_singapore_final.pdf

39 Comparing privacy laws: GDPR v. Singapore's PDPA, https://www.dataguidance.com/sites/default/files/gdpr_v_singapore_final.pdf

40 In the GDPR, data controllers must notify supervisory authorities of data breaches. There is currently no mandatory obligation to notify PDPC and/or affected individuals of data breaches. PDPC's Guide to Managing Data Breaches 2.0, issued on 22 May 2019, provides guidelines as to when an organisation is required to notify the PDPC and/ or affected individuals about a data breach.

41 PDPC (2020) Singapore now recognises APEC CBPR and PRP Certifications Under PDPA, https://www.pdpc.gov.sg/news-and-events/announcements/2020/06/singapore-now-recognises-apec-cbpr-and-prp-certifications-under-pdpa

42 APEC (2019) What is the Cross-Border Privacy Rules System? https://www.apec.org/About-Us/About-APEC/Fact-Sheets/What-is-the-Cross-Border-Privacy-Rules-System

43 MTI Digital Economy Agreements, https://www.mti.gov.sg/Improving-Trade/Digital-Economy-Agreements

44 METI (2020) Joint Statement Initiative on E-commerce: Co-Conveners Update, https://www.meti.go.jp/press/2020/12/20201215001/20201215001-1.pdf

45 U.S. Department of the Treasury, United States – Singapore Joint Statement on Financial Services Data Connectivity, https://home.treasury.gov/news/press-releases/sm899

46 Monetary Authority of Singapore, Joint Statement of Intent on Data Connectivity between Bangko Sentral ng Pilipinas and The Monetary Authority of Singapore, https://www.mas.gov.sg/news/media-releases/2020/joint-statement-of-intent-on-data-connectivity-between-bsp-and-mas


salesforce