DATA BEYOND BORDERS

OPTIMISING MOVEMENT AND PROTECTION MECHANISMS FOR CROSS-BORDER DATA FLOWS IN G20 ECONOMIES

CONTENTS

FOREWORD

Cross-border data flows are lifeblood for the global economy, and for GDP of national economies. When data flows, the economy grows.

There is strong evidence to support this. McKinsey estimates that global data flows account for 3 percent of global GDP output, the equivalent of US$2.3 trillion. The Brookings Institution estimates that unobstructed digital trade raises the GDP of the United States by 3.4 to 4.8 percent, contributing to the creation of 2.4 million new jobs.

Speaking at the 2019 World Economic Forum in Davos, Japan's Prime Minister Shinzo Abe recognized the importance of data as the powering resource for the fourth industrial revolution. Accordingly, he proposed the creation of the Data Free Flow with Trust (DFFT) framework for cross-border data sharing.

With Japan hosting the G20 in 2019, and consistent with Prime Minister Abe's vision for the DFFT, this report examines G20 economies' openness of cross-border data flows, as well as the extent to which the degree of openness affects economic competitiveness.

Commissioned by Salesforce and prepared by TRPC, this report also provides recommendations for G20 members to strengthen the mechanisms of cross-border data flows, making frameworks less restrictive while safeguarding national interests.

Based on findings in the report, the primary recommendations include:

- Committing to in-principle policies that enable cross-border data flows;
- Developing a risk-based data classification scheme;
- Promoting international interoperability between privacy regimes;
- Considering bilateral or multilateral agreements to bridge gaps between national privacy laws;
- Maintaining multilateral discussions on mechanisms to reduce cross-border data barriers.

Among these recommendations, one stands out as particularly actionable: developing a risk-based data classification scheme. Such a risk-based approach allows organizations in the public or private sector to focus their protection and security efforts appropriately, based on the risk/sensitivity of the specific data type. This approach focuses effort and resources on the most sensitive data, while enabling the free flow of less-sensitive information in order to maximize economic growth and innovation.

G20 economies have much to gain from exploring ambitious approaches to cross-border data flows, and much to lose if they use unnecessary market barriers or protectionist policies.

Eric Loeb
EVP, Global Government Affairs
Salesforce

EXECUTIVE SUMMARY

Globalisation and digitisation have led to greater connectivity, which in turn has rapidly increased the quantities of data being accessed, moved, and exchanged both within and between countries.

This is especially important for G20 economies, who have jointly agreed to foster dynamic digital societies and enable inclusive digital economies.[3] To fulfil their commitments, they must carefully assess the impact cross-border data flows have on innovation, investment, and efficient governance.

This means determining whether their regulatory frameworks restrict or enhance cross-border data flows, as well as evaluating the extent to which their approach allows them to seize economic opportunities ahead of others.

Commissioned by Salesforce and prepared by TRPC, this report examines and compares the openness of G20 economies in regard to the flow of data across borders.

The Cross-Border Data Flows Index (CBDFI) has been developed to provide a benchmark performance assessment of G20 economies' approach to cross-border data flows, as well as its impact on economic growth and opportunity.

The CBDFI sources publicly available indicators to quantify and evaluate eight key regulatory dimensions that impact the volume and the variety of data flowing across borders.

Overall, the CBDFI finds that:

1. Enabling cross-border data flows clearly contributes to the growth and dynamism of an economy. The more flows there are between economies, the greater the overall benefits. This speaks to the central role that groups such as the G20, OECD, and others can play in promoting enhanced cross-border data flows between members.
2. Barriers to data flows hinder businesses' and institutions' ability to benefit from global opportunities, not only through restrictions on access and participation, but by increasing compliance costs. Both of these issues disproportionately impact SMEs, which should therefore be a guiding condition in policy design.
3. Data classification frameworks, when applied consistently as part of balanced data governance strategies, appear to enhance economic opportunity, and enable a more nuanced approach to cross-border data flows. Specifically, such frameworks allow governments to make proportionate decisions about certain specific types of data which may require restrictions, but to do so without unduly impacting the movement of data across borders.

Cross-border data flows contribute to the growth and dynamism of economies

With a total CBDFI score of 38 out of a maximum of 48, Japan takes the top spot in the CBDFI rankings – showing that, among G20 economies it has the least restrictive and the most consistent approach to cross-border data flows.

It is closely followed by the United States (score of 35), the European Union, and the United Kingdom (both tied at 34) – three G20 members with relatively comprehensive data-sharing frameworks in place.

At the other end of the spectrum are economies with policies and regulations that significantly restrict the flow of data: China (score of 10), Indonesia (9), and Russia (4).

Correlations between CBDFI scores and key economic indicators clearly show the impact that cross-border data openness can have on economic growth (GDP per capita), dynamism (Ease of Doing Business Index), and competitiveness (Global Competitiveness Index).[4]

The correlation is strong enough to suggest that the more open an economy's approach to cross-border data flow, the more likely there are to be economic rewards. On a global scale, the International Trade Commission (ITC) has found that removing foreign digital trade barriers would increase real wages by 0.7 to 1.4 percent in digitally intensive sectors.[5]

Barriers to data flows hinder businesses' ability to benefit from global opportunities

Cross-border data flows are an enabling force for businesses around the world. From manufacturing and services to agriculture and retail, all sectors increasingly rely on data – and on its global flow – to plug into global value chains and contribute to the global economy.

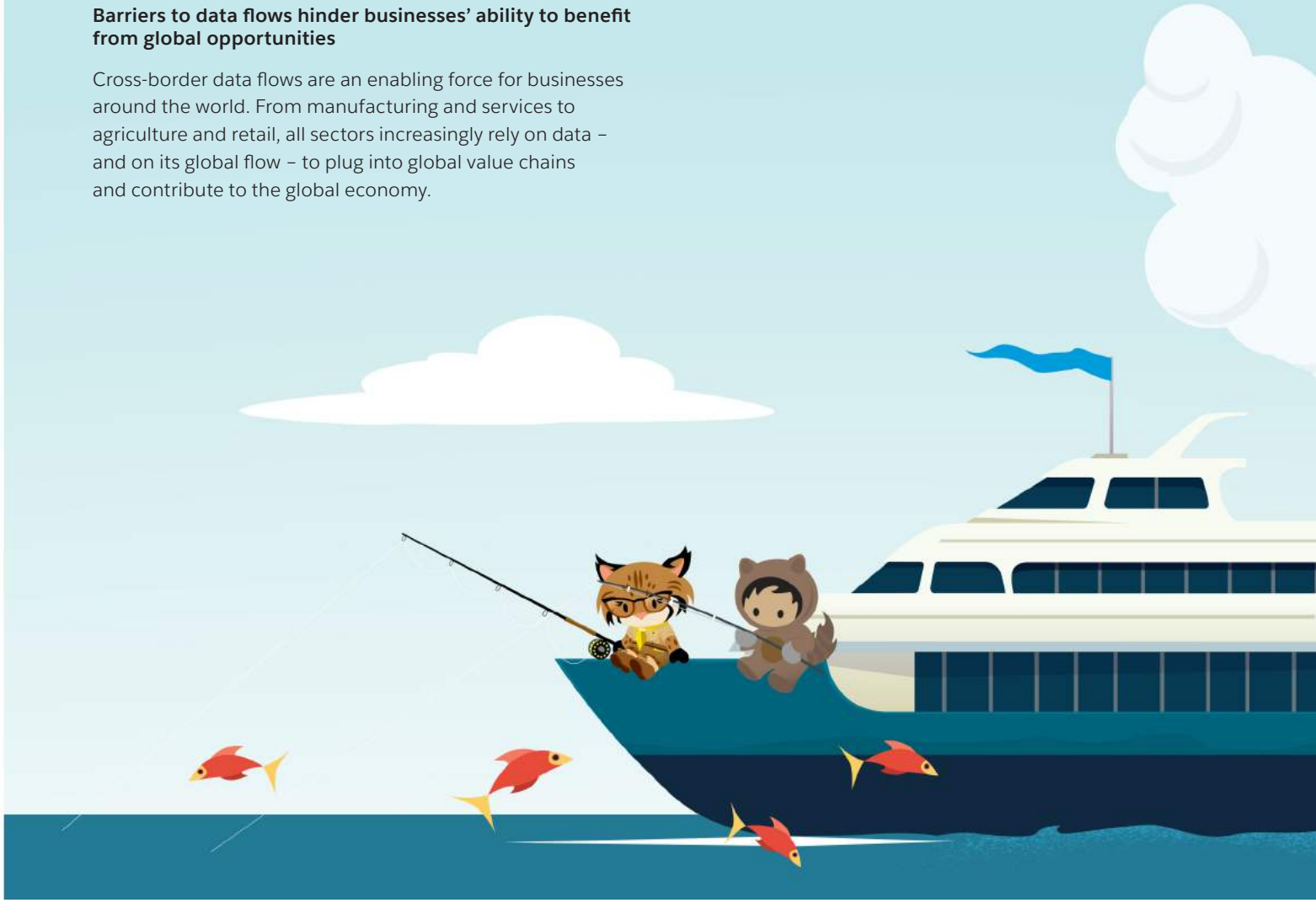
Across the board, the free flow of data accelerates the spread of ideas, research, and technologies, leading to the emergence of new, innovative business models that propel economies forward.

Small and medium enterprises (SMEs), especially, benefit from the flow of data across borders. They help reduce transaction costs and mitigate the constraints of geographic distance, increasing overall efficiencies as well as opportunities. This allows businesses of all sizes to reach global markets and leverage data-driven services to meet consumers' fast-evolving needs and expectations.

The public sector also benefits from cross-border data flows. Access to global digital resources can help governments take effective action in the face of complex challenges (natural catastrophes, crime, poverty, financial crises, etc.).[6]

Conversely, restrictions on cross-border data flows can hamper global opportunities, and even negate the benefits brought about by global connectivity.

According to the Information Technology & Innovation Foundation (ITIF), countries that enact barriers to data flows make it harder and more expensive for domestic companies to gain exposure and to benefit from the opportunities that accompany data flows.[7]



Barriers can also reduce confidence in a country's economic dynamism. A study by the European Centre for International Political Economy (ECIPE) finds that restrictions on cross-border flow of information can reduce domestic investments in Brazil, China, India, Indonesia, South Korea, and the European Union (EU) from 0.5 to 4.2 percent.[8]

Furthermore, data localisation requirements make it more difficult for local entities to access global services, such as cloud services provided by multinational companies.

Data classification frameworks enable a balanced approach to cross-border data flows

Despite the significant benefits of cross-border data flows, many G20 economies have measures in place that limit or restrain data movement across borders.

These barriers often take the shape of data-residency requirements that confine data within a country's borders. Such data localisation measures can be explicitly required by law or be the result of several restrictive policies that make it expensive, complicated, or unfeasible to transfer data transnationally.

G20 economies implement such measures for a number of reasons, but the most prominent one is the fact that the global exchange of data raises a number of privacy and security concerns.

Regarding privacy, governments want to ensure that personal data collected, accessed, transferred, used, and shared across organisations and jurisdictions is done in a transparent and responsible manner. In terms of security, the fast-evolving threat of transnational cyber-crime pushes governments to protect their strategic data from entities working against their national interests.[9]

Whichever the reason, broad restrictions on data flows have two fundamental flaws.

First, they are not targeted at a specific problem, which means they could leave issues unresolved, or even have unintended consequences.

Second, such measures inevitably work against the very economic interests they claim to safeguard. The ECIPE has shown that the presence of data localisation measures can lead to major GDP losses for G20 economies – from 0.7 to 1.1 percent in Brazil, India, Indonesia, South Korea, and the EU.[10]

This is largely due to the barriers that limit entrepreneurs' and SMEs' access to the global marketplace.

The CBDFI shows that governments do not need to choose between enabling the flow of data across borders and upholding privacy and security principles. Indeed, several of the highest-ranking economies have implemented – or are looking to implement – regulations that structure cross-border data flows in a more balanced, nuanced, and targeted manner.

Data classification frameworks allow governments to bring specific solutions to specific problems, without adding unnecessary risks, costs, or burdens.

Of foundational importance, organising data by specific criteria – level of sensitivity, degree of strategic value, or extent of exposure to threats – makes it possible to determine which data can flow without limit (business-enabling data, for example), and which – small – amount of data may be clearly identified as so vital or sensitive that it needs to be restricted in movement (data related to national security, for instance).

Data classification frameworks may not be easy to design and implement, but they do constitute a potential path forward.

METHODOLOGY

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's 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.[11]

Each of the G20 economies is scored on a scale from 0 to 6 for each of the above-mentioned indicators.[12] Table 1 provides details on the scoring mechanisms.[13]

Table 1: *Scoring mechanisms for regulations impacting data flows*

	Questions on regulations impacting data flows	Scoring mechanisms (0-6)
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** (not a favourable mechanism) > 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?	> No consent or notice requirements = **6** > No consent requirements but notice needs to be given to data subjects = **4** > Yes, express consent requirements (freely given, specific, informed, and unambiguous) = **2** > Written (or equivalent) consent is required = **0**
6	Is the country a participant of the EU's GDPR regime or meets GDPR adequacy requirements?	> Yes = **6** > Partial = **3** > No = **0**
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: TRPC Research

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

A lower score indicates restrictive regulations that promote data localisation and hinder cross-border data flows, while a higher score indicates a less restrictive approach to data residency and cross-border data flows.


#1 JAPAN
38 POINTS
#2 UNITED STATES
35 POINTS
#3 EUROPEAN UNION
UNITED KINGDOM
34 POINTS
#4 ITALY
32 POINTS
#5 CANADA
31 POINTS
#6 AUSTRALIA
FRANCE
GERMANY
30 POINTS
#7 SOUTH KOREA
24 POINTS
#8 BRAZIL
22 POINTS
#9 MEXICO
21 POINTS

KEY FINDINGS

The CBDFI measures G20 economies' openness to the cross-border flow of information through eight indicators related to data protection and data residency requirements.

The higher the score, the more the law and public policy environment of an economy enables the flow of data across borders and the fewer legal barriers to such flows – thereby opening opportunities for organisations to thrive where their activities rely on cross-border data flows.

A lower score indicates the existence of regulatory restrictions, including policies and compliance requirements, that place a heavy burden on businesses looking to leverage the flow of information across borders.

SCORES AND RANKINGS

The CBDFI scores below show that G20 economies respond differently to the challenge of cross-border data flows, leading to a variety of strategies to enable or curb the movement of data across borders.

This is because some see them as an opportunity for economic growth, while others see them more as a threat to their privacy and security principles. There is also the fact that not all G20 economies have the institutional capabilities to design and uphold sophisticated strategies in this area.

The G20 average score is 23.

Note: See the Methodology and the Statistical Annex for more details on the scoring mechanism.
Source: TRPC Research

HIGH SCORERS RECOGNISE THE IMPORTANCE OF ENABLING DATA FLOWS

With a score of 38, Japan scores highest among G20 economies, demonstrating that it has taken the most proactive approach to promoting cross-border data flows through a comprehensive and balanced approach to data protection.

Japan has enacted the Act on the Protection of Personal Information (APPI), which ensures its domestic regulations provide clarity to the business community with regard to cross-border data flows. This regulatory consistency has facilitated its participation in both the APEC's CBPR framework, as well as meeting the EU's GDPR Adequacy requirements for data transfers.

Together, these measures allow Japanese businesses to participate in the global digital economy as 'trusted data transaction partners', enabling companies to both leverage data to pursue trans-national opportunities and ensure the data they handle is effectively protected.

The United States follows closely behind with a score of 35.

The 1974 Privacy Act (the national law addressing data protection for information collected, controlled, or used by the federal government) does not establish a general prohibition with regard to the transfer of federal government data outside the United States. And generally speaking, consumer data is allowed to flow outside the United States.

But several federal and state industry-specific data laws and legal practices (such as federal 'national security letters') do restrict the transfer of certain data (such as personal health information, financial institutions' records, etc.) outside the United States. At the same time, certain agencies, such as the Internal Revenue Service (IRS) and the Department of Defence (DoD), have regulations that require their data to remain on American soil (including embassies and military installations).

These sector-specific requirements are not catch-all prohibitions, but more compliance measures that aim to foster a conducive, business-friendly environment in which data-driven business models can be developed and cross-border data exchanges can spur investment and innovation.

With CBDFI scores of 34, the European Union (EU) and the United Kingdom can be seen to be largely enablers of cross-border data flows.

For the EU, the establishment of the GDPR framework has demonstrated the importance of designing thorough and comprehensive measures to frame the conditions in which personal information moves across jurisdictions.

The United Kingdom, meanwhile, is one of a handful of countries to have developed and implemented a data classification framework for the public sector. This means the government has mechanisms in place to structure and segregate the data for which it is responsible, allowing it to define appropriate cross-border transfer conditions for each specific type of data.

This not only rationalises cross-border data flows, it also ensures the movements of non-critical data do not hinder or jeopardise the security of more sensitive data.

MODERATE SCORERS LIMIT THEIR OWN POTENTIAL

Italy (32), Canada (31), Australia, France, and Germany (all three tied at 30), are all in the middle of the pack and well above the G20 average of 23 – suggesting a relative openness to cross-border data flows, but limited by a number of restrictive measures.

Canada, for instance, allows consumer data to move to other jurisdictions as a general principle, but it has no comprehensive, nationwide framework that structures its approach to cross-border data flows. This leads to some provinces – such as British Columbia and Nova Scotia – having their own regulations, including data localisation requirements that restrict the movement of certain types of data.

In Australia, the Privacy Act sets out the minimum standards for dealing with personal information, including the conditions in which data can be transferred abroad. In addition, there are sector-specific legislations that regulate data protection in the health sector, telecommunications sector, and consumer credit reporting.

In France and Germany, the cloud souverain (sovereign cloud) and the Bundescloud (government cloud) are current proposals.

LOW SCORERS HAVE INHIBITIVE MECHANISMS IN PLACE

At the lower end of the spectrum are China (score of 10), Indonesia (9), and Russia (4) – who all have restrictive data transfer policies in place, such as strict data localisation requirements.

Their analysis identifies two unfavourable features:

- Laws restrict the flow of data for the purposes of meeting the needs of law enforcement agencies and to define and enforce domestic internet sovereignty.
- Data localisation is driven by broader "national security" or domestic industrial policies, and therefore are both very strict and broad in application – making them difficult to overturn.

China's policies include (but are not limited to): the Cybersecurity Law 2016, which states that personal information and important data must be stored locally;[14] various financial regulations around e-banking, credit reporting, insurance administration, and personal financial information, which all require data to be stored within China; and the Chinese Counter Terrorism Law, which requires all Internet service providers to locate their servers within China.[15]

Indonesia, meanwhile, has a number of broad, largely unfocused regulations that either severely restrict the movement of data across platforms and jurisdictions, or increase uncertainty by threatening existing openness. Its data localisation requirements, for instance, force providers of a public service to establish local data centres and disaster recovery centres in Indonesia.

Other regulations require local storage and processing of certain personal data and financial data. In addition, providers of "over the top" (OTT) services – the vague definition of "OTT services" essentially covers every service provided via the Internet – are required to register with the government, identify permanent local representatives, and open bank accounts in Indonesia.

In Russia, the 2015 amendments to the Personal Data Law 2006 require that certain data on Russian citizens collected electronically by companies be processed and stored in Russia.[16]

The statistical relationships are significant enough to suggest that greater cross-border data flow is strongly associated with economic growth, dynamism, and competitiveness. This means that the more open an economy's approach to cross-border data flow, the more likely there are to be economic rewards.

In short, there is compelling evidence that G20 economies have more to gain from enabling cross-border data flows than limiting them.

CORRELATIONS

To estimate the potential economic impact of cross-border data flows on G20 economies, TRPC calculated the correlation between total CBDFI scores and eight key economic indicators:

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; and
8. The World Economic Forum (WEF)'s Global Competitiveness Index (GCI) 4.0.

Table 2 shows that the CBDFI scores are strongly correlated with GDP per capita, with the Ease of Doing Business Index, as well as with the Global Competitiveness Index (GCI) 4.0 (all statistically significant at the 0.01 level).

***Table 2:** Correlation between countries' CBDFI scores and selected economic indicators*

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

Note: This table is based on Pearson Correlation values. See the Statistical Annex for more detailed results.
Source: TRPC Research

RECOMMENDATIONS

Enabling the cross-border flow of data positively affects economic growth, dynamism, and competitiveness. It is therefore urgent for G20 economies to lead by example and develop policies that enable information to move across physical and virtual boundaries.

Five main recommendations stand out:

COMMIT TO IN-PRINCIPLE POLICIES THAT ENABLE CROSS-BORDER DATA FLOWS

Cross-border data flows are, and will continue to grow more fundamental for advances in technological innovations such as cloud computing, artificial intelligence (AI), autonomous systems, the Internet of Things (IoT), 5G communications, and quantum computing. These technologies will drive advances in all sectors from agriculture to energy and smart cities. G20 governments must enable cross-border data flows by eliminating broad requirements that data be stored or processed locally. Such restrictions severely hinder businesses' ability to operate and evolve in a competitive world where growth and opportunity, driven by digital transformation, benefit the national economy.

DEVELOP A RISK-BASED DATA CLASSIFICATION SCHEME

G20 governments should consider adopting a consistent risk-based data classification framework as part of wider data protection laws. By classifying information based on risk, an organisation can focus its protection and security efforts appropriately, mobilising adequate resources to protect the information that it considers the most sensitive, while allowing flow of the large percentage of less sensitive information in order to promote economic growth and innovation. This leads to better security, exactly where the security is needed.

PROMOTE INTERNATIONAL INTEROPERABILITY BETWEEN PRIVACY REGIMES

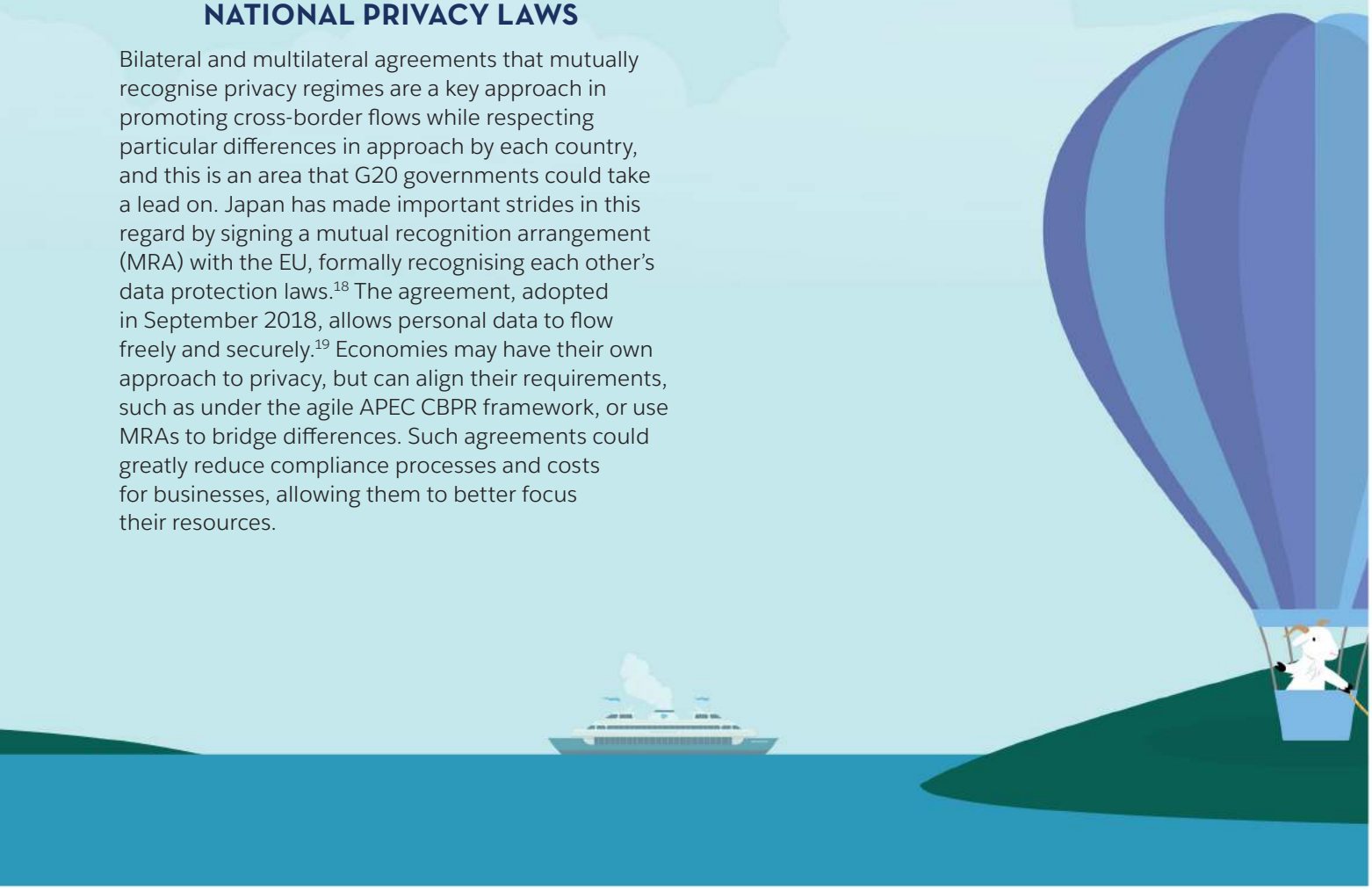
G20 governments must work together to support interoperability in data protection regimes to facilitate the secure transfer of information across borders. Most legal frameworks allow transfers to economies which provide similar protections to data. This compatibility is essential to cross-border data flows. More effective is participation in a regional data protection framework. APEC's CBPR facilitates the free flow of data across participating economies. The OECD's Guidelines on the Protection of Privacy and Transborder Flows of Personal Data recognise interoperability among privacy frameworks and increased cooperation between privacy authorities as key to enabling the cross-border flow of information.[17] G20 governments could use this experience to ensure both domestic and multinational businesses thrive within their markets.

CONSIDER BILATERAL OR MULTILATERAL AGREEMENTS TO BRIDGE GAPS BETWEEN NATIONAL PRIVACY LAWS

Bilateral and multilateral agreements that mutually recognise privacy regimes are a key approach in promoting cross-border flows while respecting particular differences in approach by each country, and this is an area that G20 governments could take a lead on. Japan has made important strides in this regard by signing a mutual recognition arrangement (MRA) with the EU, formally recognising each other's data protection laws.[18] The agreement, adopted in September 2018, allows personal data to flow freely and securely.[19] Economies may have their own approach to privacy, but can align their requirements, such as under the agile APEC CBPR framework, or use MRAs to bridge differences. Such agreements could greatly reduce compliance processes and costs for businesses, allowing them to better focus their resources.

MAINTAIN MULTILATERAL DISCUSSIONS ON MECHANISMS TO REDUCE CROSS-BORDER DATA BARRIERS

Governments should urge international organisations such as the World Trade Organisation (WTO) and the World Bank to establish or enhance mechanisms to continually monitor and report on economies that introduce data localisation that will negatively impact the cross-border flow of data.[20] This could be by elevating visibility of restrictions on the movement of data at the World Bank/WTO's Integrated Trade Intelligence Portal. Other international institutions such as the United Nations Conference on Trade and Development (UNCTAD), the International Monetary Fund (IMF), and the Inter-American Development Bank (IDB) could be encouraged to elevate advocacy for the free flow of data across borders and, where appropriate, oppose policies that require data localisation. Such efforts would help create an environment where businesses could develop optimal strategies when expanding internationally.



MARKET HIGHLIGHT: JAPAN

The CBDFI finds that Japan is the highest-scoring G20 economy.

The Japanese government has taken concrete steps to create a regulatory environment that both enables and protects the free flow of data across boundaries. This regulatory balance ensures that the data that moves internationally and across borders is strengthened – not hindered – by the regulatory safeguards designed to keep it safe.

This approach allows information to move faster and further than in economies with more restrictive regulations, helping Japanese businesses remain competitive on the global digital market.

This is a major factor behind Japan's rapidly growing digital trade and commerce sectors (both domestically and abroad).

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

CBDFI DIMENSION 1: Data localisation requirements

Japan's Act on the Protection of Personal Information (APPI),[21] amended in May 2017, sets out rules around the protection of personal data and transfer of information across borders. The APPI recognises the importance of cross-border flow of information, and as such does not impose data localisation requirements. Data residency requirements can limit data transfers, directly hampering the cross-border flow of information and indirectly impacting economic growth and competitiveness.

CBDFI DIMENSION 2: Explicit provisions on extraterritorial transfers

The APPI also includes explicit provisions for international and/or extraterritorial transfers of data. They are specified in Article 24, Restriction on Providing Personal Data to a Third Party in a Foreign Country.[22] This is one of the measures that has allowed Japan to become the first Asia-Pacific economy to enter a mutual adequacy arrangement with the EU, formally recognising each other's data protection laws and thereby allowing data to flow freely and safely between them.[23] This is a major advantage, as explicit provisions for data transfers across borders provide greater clarity to businesses and citizens alike, building confidence in the digital economy.

CBDFI DIMENSION 3: Mechanisms to transfer personal data across borders

A clear mechanism to facilitate the transfer of data across borders ensures businesses have clear rules when managing such transfers. In the case of Japan, Article 6 of the APPI states that the government must, considering the nature and utilisation method of personal information, take necessary legislative action to protect personal information and the rights and interests of individuals. It shall also take necessary action in collaboration with the governments of other countries to construct an internationally conformable system concerning personal information through fostering cooperation with an international organisation and other international frameworks. Thus, a clear mechanism is anticipated.

CBDFI DIMENSION 4: Data classification framework

There appear to be no data classification frameworks for the public sector, or generally applicable to the private sector related to facilitating cross-border data flows. To continue on its upward trajectory, Japan should consider further strengthening its APPI by introducing a data classification framework.

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

Consent requirements for the collection, storage, or dissemination of personal data extraterritorially are an important facet of cross-border data flows. Obtaining prior consent can slow down the flow of information and may increase the compliance burden on businesses. Japan's APPI has a number of sections that, taken together, constitute a set of consent requirements for international data transfers. Personal data can be transferred to a third party in another economy, if the foreign economy has adequate and equivalent data protection laws or standards to those in Japan, or if they have obtained prior consent from the individual whose data is being transferred ('principal'). Japan's APPI also imposes a purpose-limitation clause, wherein a business operator handling personal information must not use it without obtaining prior consent from the principal, nor for purposes other than previously scoped and agreed ones.[24] Given the adequacy requirement, whereby consent is not required, and no written consent is required, Japan is relatively favourable in this dimension.

CBDFI DIMENSION 6: Participation in the EU's GDPR regime

Interoperability between data protection regimes can help enable the secure flow of data across borders and Japan has made a number of strides in this regard. While it is not a member of the EU, and hence not an EU's GDPR party, it has been recognised by the EU as providing an adequate level of data protection,[25] which means that personal data can flow between the EU and Japan without the need for any additional safeguards.

CBDFI DIMENSION 7: Participation in the APEC's CBPR system

The APEC's CBPR is a non-binding, risk-based and accountability-based approach to data protection, focused on facilitating the free flow of data across geographies.[26] The CBPR framework holds organisations transferring personal data accountable – where they must take reasonable steps to ensure that the recipient will protect the information consistent with the APEC Privacy Principles – enabling data to flow in the absence of governments' having recognised each other's data protection laws as adequate/equivalent. Apart from Japan, five other economies are part of CBPR, namely Canada, Mexico, Singapore, South Korea, and the United States.[27] A work in progress, the framework aims to establish a harmonised and interoperable data protection regime across the APEC region.

CBDFI DIMENSION 8: Inclinations towards allowing cross-border data flows

Overall, Japan is a strong advocate for cross-border data flows. Its participation in APEC's CBPR and its agreement with the EU demonstrate a clear trajectory toward greater cross-border data flows. In addition, Prime Minister Shinzo Abe's recent declarations on the need to build a global data-sharing and data-governance framework (the Data Free Flow with Trust) show a strongly determined approach to enable cross-border data flows on a global scale.

Overall, Japan is a strong advocate of cross-border data flows. To continue on its upward trajectory, Japan should consider further strengthening its APPI by introducing a comprehensive data classification framework.

Restrictions on cross-border data transfers stem primarily from concerns around personal data security or of national security for highly sensitive government information, which is why a data classification system can enable the appropriate protection of different types of sensitive data based on its associated risk level.

One common approach is a three-tier classification system based on risks associated with harm to society or risk to the operation of the enterprise:

- Low – If the loss of confidentiality, integrity, or availability could be expected to have a limited adverse impact;
- Moderate – If the loss could be expected to have a serious adverse impact; and
- High – If such loss could be expected to have a severe or catastrophic adverse impact.

Distinguishing levels of data sensitivity makes it easier for data controllers (governments or businesses) to give each level an appropriate security control based on a specific risk assessment. High-risk data, such as state secrets, can be barred from ever moving anywhere outside of the government's control. Low-risk data, meanwhile, can be transferred internationally, without affecting the integrity of high-risk data. In many economies, data classification frameworks have resulted in governments classifying 90 percent or more of public-sector data as non-sensitive (low-risk).[28]

The United States and the United Kingdom have implemented cross-government data classification systems for all public-sector information.[29] Developing such a system for both the public and private sectors would enable securing sensitive data, while enabling the transfer of the majority of data across borders – improving benefits and opportunities for consumers, businesses, and the national economy.

STATISTICAL ANNEX

Table 3: *Detailed CBDFI scores according to the eight CBDFI dimensions relating to cross-border data flow requirements*

Data Regulations/Requirements	ARG	AUS	BRA	CAN	CHN	EU
1. Is there a data localisation requirement?	1	4	6	4	0	4
2. Are there explicit provisions allowing for international or extra-territorial transfers of personal data/ personally-identifiable data?	4	6	4	4	4	6
3. Does the data protection law include a specific mechanism to transfer personal data across borders subject to certain protections?	2	2	2	0	2	6
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	4	6	6	2	6
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
6. Is the country a participant of the EU's GDPR regime or meets GDPR adequacy requirements?	6	0	0	3	0	6
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
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)?	2	4	2	6	2	4
TOTAL score (/48)	**17**	**30**	**22**	**31**	**10**	**34**

Note: For each of the eight dimensions, scores range from 0 to 6. See the Methodology for more details on the scoring mechanism.
Source: TRPC Research

FRA	DEU	IDN	IND	ITA	JPN	MEX	RUS	SAU	ZAF	KOR	TUR	GBR	USA
2	2	0	0	4	6	4	0	2	2	2	2	2	4
6	6	4	2	6	6	2	2	4	6	4	4	6	4
6	6	6	3	6	6	0	0	0	2	4	6	6	2
4	4	0	0	4	0	2	0	0	2	2	2	6	6
2	2	2	0	2	2	2	0	4	4	2	2	2	4
6	6	0	0	6	6	3	0	0	0	0	0	6	3
0	0	2	2	0	6	6	0	2	0	6	0	0	6
4	4	3	2	4	6	2	2	2	2	4	2	6	6
30	**30**	**17**	**9**	**32**	**38**	**21**	**4**	**14**	**18**	**24**	**18**	**34**	**35**

Table 4: *Eight indicators of economic growth, dynamism, and confidence used to calculate the correlations*

	GDP per capita (current US$), 2017	GDP annual growth rate, 2017	Foreign direct investment, net inflows (% of GDP)	Ease of Doing Business Index (score)
Argentina	14,398	2.9	1.8	57.93
Australia	53,800	2	3.2	80.14
Brazil	9,821	1	3.4	57.05
Canada	45,032	3	1.7	78.88
China	8,827	6.9	1.4	65
European Union	33,723	2.4	3.5	78.33
France	38,477	1.8	1.8	76.3
Germany	44,470	2.2	2.1	78.9
India	1,942	6.7	1.5	60.6
Indonesia	3,847	5.1	2.1	66.54
Italy	31,953	1.5	0.5	72.71
Japan	38,428	1.7	0.4	75.6
Mexico	8,910	2	2.8	72.27
Russia	10,743	1.5	1.8	76.76
Saudi Arabia	20,849	-0.9	0.2	61.88
South Africa	6,151	1.3	0.4	64.66
South Korea	29,743	3.1	1.1	84.15
Turkey	10,546	7.4	1.3	69.99
United Kingdom	39,720	1.8	2.5	82.32
United States	59,532	2.3	1.8	82.76

Table 5: *Detailed breakdown of the calculations used to determine the impact of cross-border data flows on economic performance*

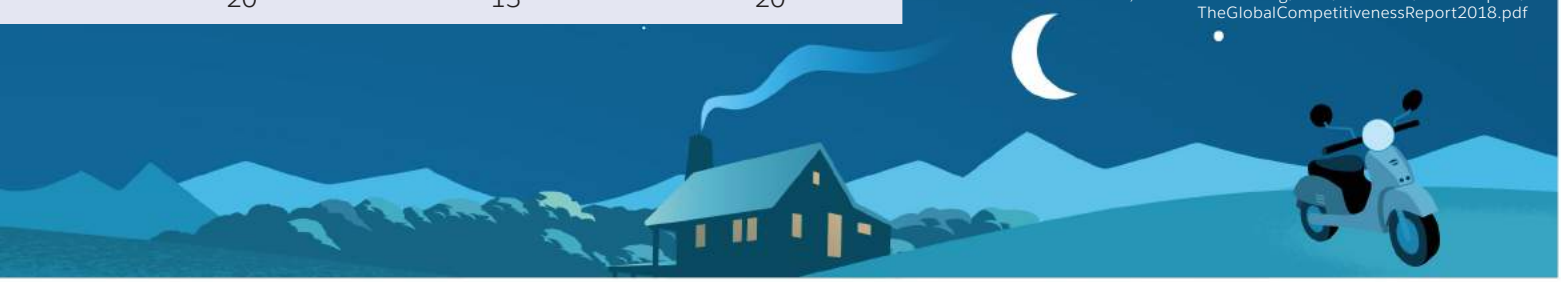
	GDP per capita	GDP growth	FDI, net inflows	Ease of Doing Business Index	Unemployment Rate
Pearson Correlation	.822**	-.321	.150	.593**	-.089
Sig. (2-tailed)	.000	.167	.527	.006	.710
N	20	20	20	20	20

** Correlation is significant at the 0.01 level (2-tailed)
* Correlation is significant at the 0.05 level (2-tailed)
Source: TRPC Research

Unemployment, total (% of total labour force)	Employment to population ratio	FDI Confidence Index	Global Competitiveness Index	CBDFI SCORE
8.3	42	..	57.5	**17**
5.6	61.5	1.66	78.9	**30**
12.3	54.6	1.37	59.5	**22**
5.8	61.6	1.82	79.9	**31**
3.9	67.9	1.76	72.6	**10**
7.6	53.7	..	69.65	**34**
10	50.5	1.7	78	**30**
3.7	58.9	1.81	82.8	**30**
2.7	50.2	1.56	62	**17**
4.2	64.2	..	64.9	**9**
11.2	44.2	1.57	70.8	**32**
2.4	60	1.72	82.5	**38**
3.3	57.6	1.47	64.6	**21**
5.2	59.5	..	65.6	**4**
5.9	51.7	..	67.5	**14**
26.9	40.3	..	60.8	**18**
3.7	60.7	1.46	78.8	**24**
10.8	47.1	..	61.6	**18**
4.3	60.2	1.77	82	**34**
3.9	60.4	2.09	85.6	**35**

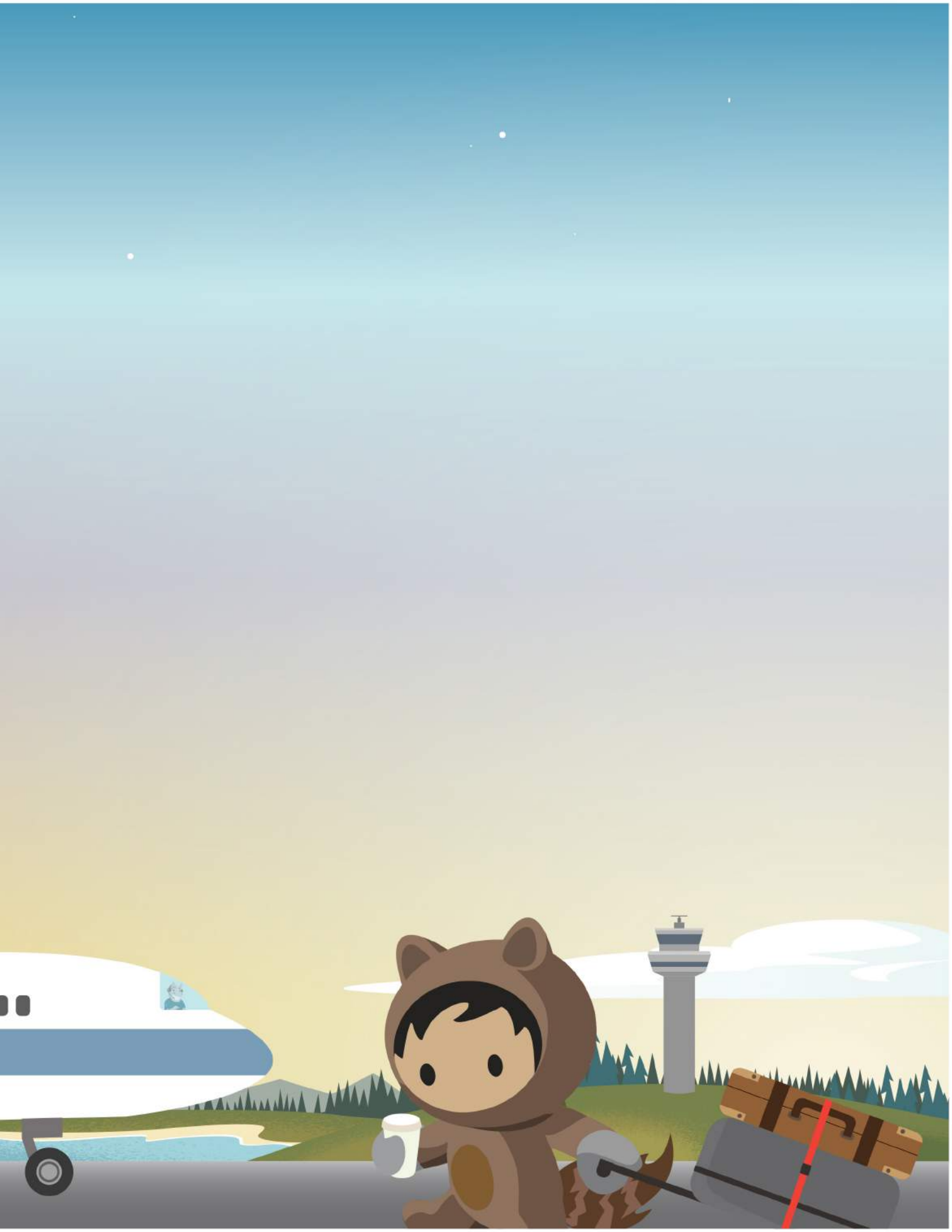
Employment Ratio	FDI Confidence Index	Global Competitiveness Index
.032	.444	.691**
.894	.129	.001
20	13	20

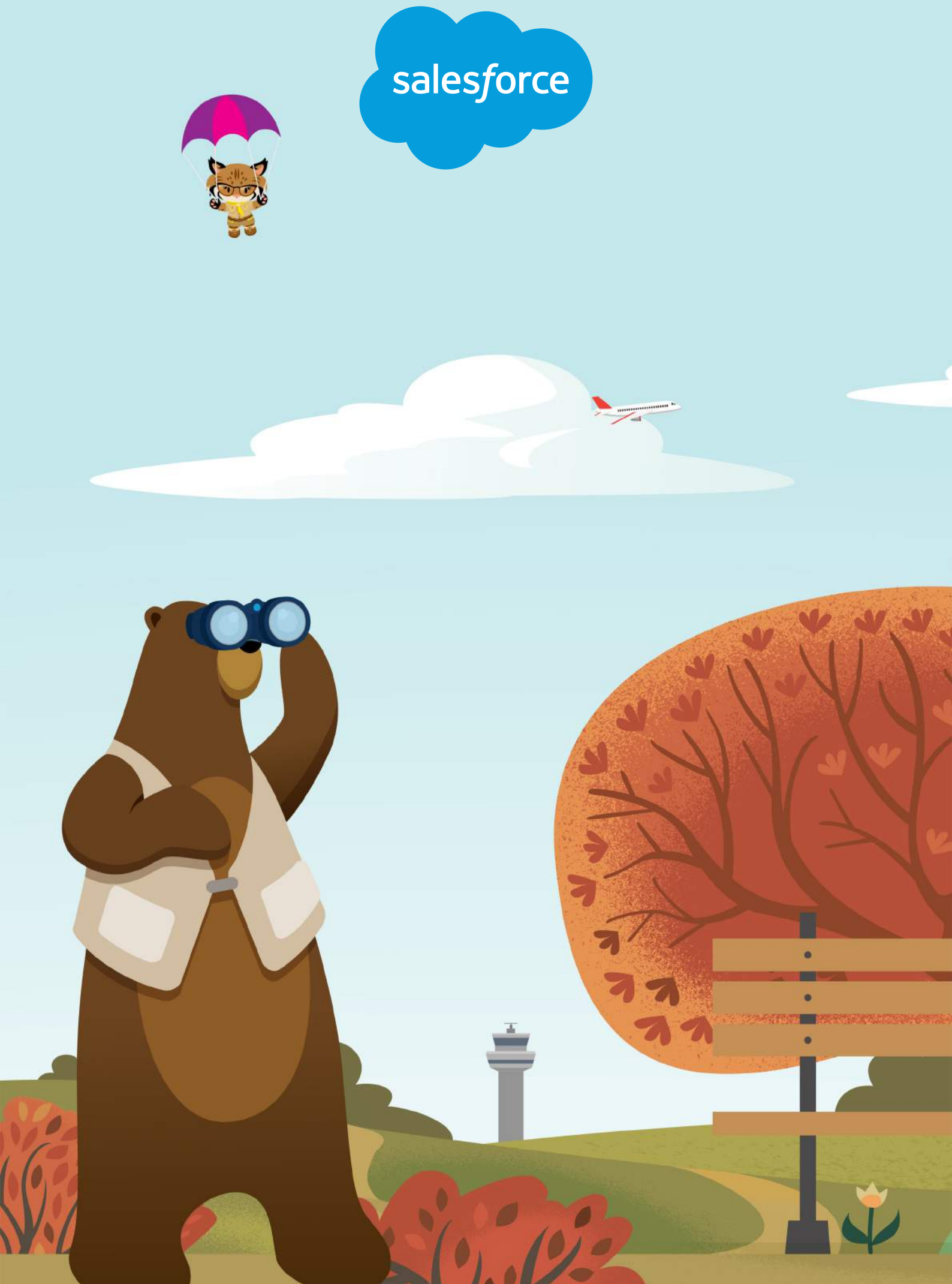
Table 4 Sources:
- GDP per capita (current US$), 2017, World Bank, https://data.worldbank.org/indicator/NY.GDP.PCAP.CD
- GDP annual growth rate, 2017, World Bank, https://data.worldbank.org/indicator/NY.GDP.MKTP.KD.ZG
- Foreign direct investment, net inflows (% of GDP), 2017, World Bank, https://data.worldbank.org/indicator/bx.klt.dinv.wd.gd.zs
- Ease of doing business score, 2018, World Bank, www.doingbusiness.org/en/data/doing-business-score
- Unemployment, total (% of total labour force), 2017, World Bank, https://data.worldbank.org/indicator/SL.UEM.TOTL.NE.ZS
- Employment to population ratio, 2017, World Bank, https://data.worldbank.org/indicator/SL.EMP.TOTL.SP.NE.ZS
- FDI Confidence Index 2018, AT Kearney, www.atkearney.com/foreign-direct-investment-confidence-index
- Global Competitiveness Report 2018, WEF, www3.weforum.org/docs/GCR2018/05FullReport/TheGlobalCompetitivenessReport2018.pdf



REFERENCES

1. McKinsey, www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalization-the-new-era-of-global-flows
2. Brookings Institution, www.brookings.edu/wp-content/uploads/2018/03/digital-economy_meltzer_lovelock_web.pdf
3. G20, www.g20.utoronto.ca/2017/170407-digitalization-annex1.html
4. For more details on correlations, see the Statistical Annex.
5. International Trade Commission (ITC), www.usitc.gov/publications/332/pub4485.pdf
6. Government Technology, www.govtech.com/em/disaster/Is-Data-Best-Preparation-Natural-Disasters.html
7. Information Technology & Innovation Foundation (ITIF), https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost
8. ECIPE, http://ecipe.org/publications/dataloc
9. OECD, www.oecd-ilibrary.org/trade/trade-and-cross-border-data-flows_b2023a47-en
10. ECIPE, http://ecipe.org/publications/dataloc
11. Includes the prospect for a more favourable environment, such as proactive use of mutual legal assistance treaties (MLATs), international data flow network-sharing participation, or clear and supportive policy statements from government leadership.
12. Note: This assessment is based on a thorough examination of national, regional, and international data protection policies and regulations. TRPC's findings provide an insightful snapshot of countries' openness to cross-border data flows, and aim to be as representative as possible. They are nevertheless based on both primary and secondary sources, which means the insights provided throughout this report are as accurate as the information they are based on, as much as they can be considered complete, up-to-date, and reliable.
13. For additional methodological information, please refer to the Statistical Annex.
14. Reed Smith, www.reedsmith.com/-/media/files/perspectives/2018/chinas-cybersecurity-law-002.pdf; and Mondaq, www.mondaq.com/china/x/668910/Data+Protection+Privacy/China+To+Implement+Widespread+Data+Localisation+For+Personal+Information+And+Important+Data
15. International Association of Privacy Professionals (IAPP), https://iapp.org/news/a/the-implications-of-chinas-draft-anti-terrorism-law-for-global-technology
16. The Kremlin, www.kremlin.ru/acts/bank/24154/page/1
17. *Ibid.*
18. European Commission, http://europa.eu/rapid/press-release_IP-18-4501_en.htm
19. The agreement became effective in January 2019. European Commission, http://europa.eu/rapid/press-release_IP-19-421_en.htm
20. Information Technology & Innovation Foundation (ITIF), www2.itif.org/2017-cross-border-data-flows.pdf
21. Personal Information Protection Commission, www.ppc.go.jp/files/pdf/Act_on_the_Protection_of_Personal_Information.pdf
22. *Ibid.*
23. European Commission, http://europa.eu/rapid/press-release_IP-18-4501_en.htm
24. ICLG, https://iclg.com/practice-areas/data-protection-laws-and-regulations/japan
25. European Commission, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en
26. The CPEA is a mutually reinforcing mechanism and a prerequisite to join CBPR.
27. Personal Data Protection Commission (PDPC), www.pdpc.gov.sg/pdpc/news/latest-updates/2018/03/singapore-joins-apec-cross-border-privacy-rules-and-privacy-recognition-for-processors-systems
28. Cabinet Office, www.gov.uk/government/uploads/system/uploads/attachment_data/file/251481/Government-Security-Classifications-Supplier-Briefing-Oct-2013.pdf
29. In the United States, the three levels are Confidential, Secret, and Top Secret (see AWS, https://d1.awsstatic.com/whitepapers/compliance/AWS_Data_Classification.pdf). In the United Kingdom, the three levels are Official, Secret, and Top Secret (see UK Government, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715778/May-2018_Government-Security-Classifications-2.pdf).




salesforce