



# **Regional Privacy Frameworks and Cross-Border Data Flows**

How ASEAN and APEC can Protect  
Data and Drive Innovation

**September 2018**



---

The GSMA represents the interests of mobile operators worldwide, uniting more than 750 operators with over 350 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and internet companies, as well as organisations in adjacent industry sectors. The GSMA also produces industry-leading events such as Mobile World Congress, Mobile World Congress Shanghai, Mobile World Congress Americas and the Mobile 360 Series of conferences.

For more information, please visit the GSMA corporate website at [www.gsma.com](http://www.gsma.com)

For information on the GSMA's work in public policy / data privacy, visit [www.gsma.com/mobileprivacy](http://www.gsma.com/mobileprivacy)

Follow the GSMA on Twitter:  
[@GSMA](https://twitter.com/GSMA) and [@GSMAPolicy](https://twitter.com/GSMAPolicy)



---

The GSMA commissioned Access Partnership to conduct research and write this report. Access Partnership is a specialised public policy consultancy that provides market access for the tech sector. Access Partnership's team monitors and analyses global trends for the risks and opportunities they create for technology businesses and identifies strategies to mitigate those risks and optimise outcomes for companies operating at the intersection of technology, data and connectivity. For more information, visit [www.accesspartnership.com](http://www.accesspartnership.com)

# Contents

<b>Executive Summary</b>	<b>2</b>	<b>ANNEX A</b>	<b>58</b>
<b>Introduction</b>	<b>7</b>	A1 ASEAN Framework on Personal Data Protection (2016)	58
<b>SECTION 1</b>		A2 APEC Privacy Framework (2004, 2015)	60
<b>Introduction to international data privacy frameworks</b>	<b>12</b>	A3 OECD Privacy Framework (1980, 2013)	62
Privacy frameworks in Asia and across the world	13	A4 The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) (1981)	64
Commonalities, divergence and key issues	16	A5 Madrid Resolution (2009)	65
Reconciling frameworks	19	A6 General Data Protection Regulation (2016)	65
<b>SECTION 2</b>		A7 EU-US Privacy Shield (2016)	67
<b>Harmonising data privacy frameworks in Asia – bridging ASEAN and APEC</b>	<b>20</b>	<b>ANNEX B</b>	
Introduction	21	<b>Economic impact of cross-border data flows and data localisation in the Asia Pacific</b>	<b>68</b>
Challenges to harmonisation	22	Economic benefits of cross-border data flows	68
Harmonising mechanisms to bridge ASEAN and APEC	24	Barriers to cross-border data flows	72
Technical options	24		
Political options	26		
Cross-regional adequacy options	26		
The process to make harmonisation work for ASEAN and APEC	28		
<b>SECTION 3</b>			
<b>Privacy regime roadmap</b>	<b>30</b>		
Background	31		
Roadmap overview	32		
How to apply key principles at the nascent stage	35		
How to apply key principles at the progressing stage	36		
How to apply key principles at the advanced stage	41		
Case studies	43		
Timeline for countries at different stages	48		
<b>SECTION 4</b>			
<b>Regulator survey and roadmap solutions</b>	<b>50</b>		
<b>SECTION 5</b>			
<b>Next steps for data privacy and cross-border data flows in Asia</b>	<b>54</b>		





---

# Executive summary

---

## Context

Regulatory frameworks for data privacy are critical to facilitate cross-border data flows in Asia and around the world. Over the past decade, international data flows have increased global GDP by 10.1 per cent. Data flows accounted for US\$2.8 trillion of global GDP in 2014, a larger share than the global trade in goods.<sup>1</sup>

Governments in Asia have worked hard to develop and implement data privacy frameworks that can effectively protect the data of their citizens, while also allowing data to flow across borders in ways that support trade and innovation. These frameworks encourage convergence across the region, which enables data to flow while maintaining a similar level of protection. Yet gaps remain.

Now is an important time to accelerate progress so that the region can continue to expand in business and trade. This process may be hastened and made easier by improving linkages at the regional level between Asia's two main privacy frameworks: the ASEAN Framework on Personal Data Protection, and the APEC Privacy Framework and its accompanying systems.

The GSMA commissioned this report to consider these data privacy frameworks – at both the regional and national levels – with the objective to identify specific steps that can be taken to support the evolution and convergence of data privacy frameworks in Asia, and do so in ways that meet the growing challenges facing ASEAN and APEC regulators. The report builds on the GSMA's previous work with Asian governments, including a 2017 Data Privacy Survey of ASEAN, and additional GSMA reports on data privacy.

## Methodology and approach

The methodology taken included research on various regional data privacy frameworks and their key principles, as well as diving down into individual countries to identify the approaches they had taken to establish a national data privacy framework. In addition, direct interviews with regulators in several ASEAN

and APEC economies (Hong Kong, Japan, Malaysia, Philippines, Singapore, and Vietnam) were conducted to understand their own views about national and regional data privacy frameworks, the challenges faced when advancing their data privacy laws, and factors that helped propel the countries forward.

## Building bridges between ASEAN and APEC privacy frameworks

### Challenges to harmonisation

Asian governments surveyed for this report acknowledged that mechanisms like the APEC Cross-Border Privacy Rules (CBPR) system or something similar present a good model for ASEAN. Yet they also noted concerns regarding the feasibility of harmonisation given the different status of data privacy laws (or lack thereof) in some ASEAN countries.

Government stakeholders also suggested there is some concern about the cost of implementation as well as the skills and expertise required to manage the process.

Another major challenge noted by several governments with regard to the APEC CBPR is the

system's reliance on third-party Accountability Agents (AAs) that serve as the key certification bodies that underpin the system.

### Reconciling frameworks

The identified differences in approach and focus across different data privacy frameworks translate into different levels of regulatory stringency. This may create complications for entities handling data of citizens in diverse jurisdictions, which may be subject to one or more regimes.

<sup>1</sup> James Manyika, et al., "Digital Globalisation: The New Era of Global Flows," McKinsey Global Institute, (February 2016), <https://goo.gl/5jvm1a>, 10.






## Harmonising mechanisms to bridge ASEAN and APEC

While regional governments acknowledge challenges to greater harmonisation exist (such as the different

status of data privacy laws, cost and capacity issues, and certification problems), there are several interesting options to more formally integrate and harmonise ASEAN's Framework and the APEC privacy systems. These include technical, political, and cross-regional adequacy options.

### Bridging ASEAN and APEC privacy frameworks

<div style="background-color: #004a80; color: white; padding: 10px; display: flex; align-items: center;">  <div> <p><b>Technical options</b></p> </div> </div> <div style="background-color: #d9e1f2; padding: 10px; margin-top: 10px;"> <p>Introduce APEC CBPR implementation measures into ASEAN framework</p> <hr style="border: 0; border-top: 1px solid #ccc; margin: 10px 0;"/> <p>Develop formal equivalence mechanisms (MoU or MRA)</p> </div>	<div style="background-color: #004a80; color: white; padding: 10px; display: flex; align-items: center;">  <div> <p><b>Political options</b></p> </div> </div> <div style="background-color: #d9e1f2; padding: 10px; margin-top: 10px;"> <p>Get remaining ASEAN states in APEC to join CBPR</p> <hr style="border: 0; border-top: 1px solid #ccc; margin: 10px 0;"/> <p>Extend APEC mechanisms to non-member countries</p> </div>	<div style="background-color: #004a80; color: white; padding: 10px; display: flex; align-items: center;">  <div> <p><b>Cross-regional adequacy options</b></p> </div> </div> <div style="background-color: #d9e1f2; padding: 10px; margin-top: 10px;"> <p>Rely on data protection authorities to broker MoUs</p> <hr style="border: 0; border-top: 1px solid #ccc; margin: 10px 0;"/> <p>Introduce Binding Corporate Rules</p> </div>
---	--	--

## Data privacy regime roadmap

Data privacy discussions are gaining traction not only at the regional level, but in individual ASEAN and APEC countries. The benefit of evolving a country's approach to data privacy is that it will help to reduce barriers to investment that restrictive data flow regulations may cause; it should also create a clearer compliance environment for businesses that wish to operate in that country.

On the other hand, data localisation – requiring that certain types of data remain in country, or be stored on local servers – and other barriers to cross-border data flows are likely to have a negative economic impact.

Regional data privacy frameworks can help guide national-level regulation which, once enacted, can in turn help prepare countries to better integrate with their regional neighbours, to the economic benefit of all. Establishing a mature data privacy framework at the national level can help a country prepare to join either the APEC CBPR system, an evolved ASEAN equivalent or other data privacy equivalence systems.

### Roadmap overview

Any country seeking to advance towards a mature national-level data privacy regime will need to engage in three distinct processes that often overlap, and could be revisited in light of technological change and evolving best practices.

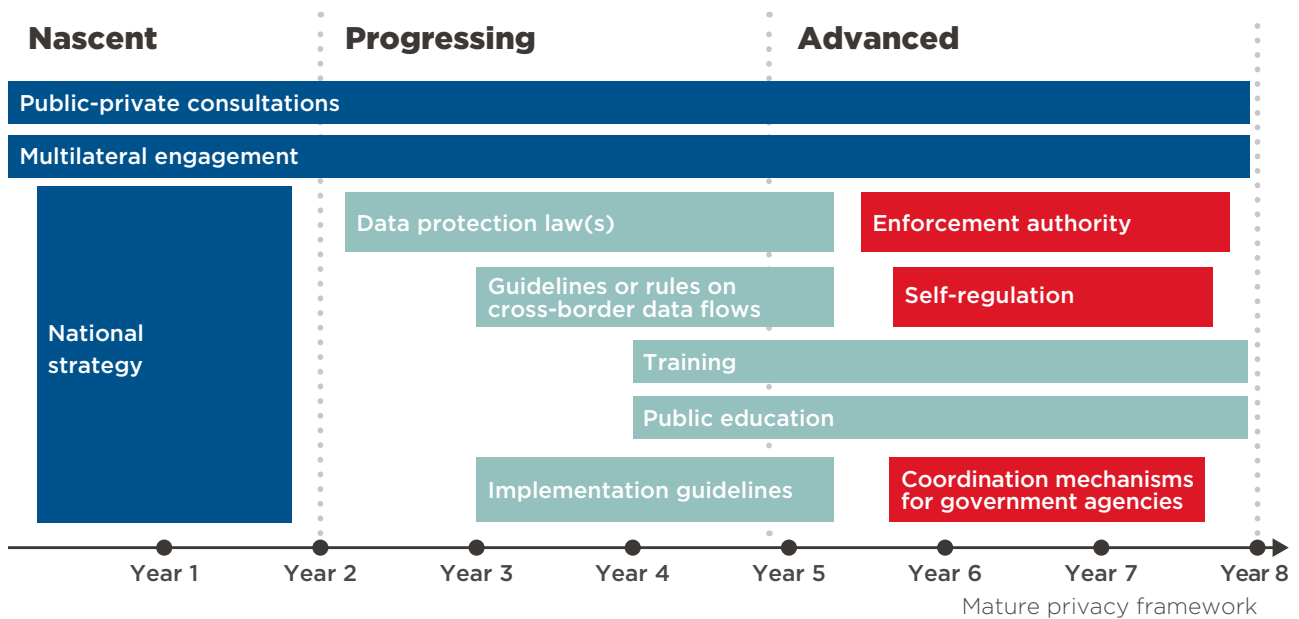
The first process is to understand where a country currently stands in terms of data privacy. This can be done by considering the various elements of a mature data privacy framework, and then checking to see which elements a country may already have in place and which ones it may still need.

The second process focuses on where a country wants to go. Like the landscaping process, this will be somewhat different for each country. Yet the progression of steps from a nascent to mature data privacy regime often follows a path that can be understood based on priority-setting, regulatory norms, and common sense.

The third and final process for a country to advance its data privacy regime at the national level is to execute across one or more elements of a data privacy regime, appropriate to where it stands on the roadmap. While there is no single path, key principles

– drawn from global and multilateral regional data privacy frameworks – can be extremely helpful for governments to consider when determining which elements to address and how best to address them.

## Roadmap of privacy elements – possible stages and timeframes



## Next steps for data privacy and cross-border data flows in Asia

Governments and societies face significant challenges when determining the best approach to data governance. The immense economic opportunities arising from the digital economy and data flows are indisputable, as are the potential perils of ignoring data privacy concerns.

At the regional level, this report describes a range of options for ASEAN and APEC governments to consider implementing towards a pan-Asian approach to data privacy. These include everything from joint ASEAN-APEC members taking up joint requirements to formal equivalence mechanisms like MoUs and MRAs between ASEAN and APEC. The region may also draw on some of the cross-regional adequacy models that have been agreed elsewhere, and adapt them to an Asian context. Whichever approach is adopted, ASEAN and APEC governments should

put in place actionable steps and a timeframe to ensure participation across all countries, including less-developed states. Harmonisation should also be sensitive to the status of various data privacy regimes, as well as the cultural and socio-political nuances across the different jurisdictions.

ASEAN and APEC governments and enforcement authorities should at a minimum bolster their interaction with one another in ways that can spur deeper collaboration and cross-learning. These engagements – either through their respective organisations or bilaterally – serve as platforms for sharing problems and discussing innovative regulatory solutions to address them. Governments should also draw on non-government data privacy experts in the private sector, civil society, and academia to inform their approaches.



# Call to action

1

ASEAN and APEC governments should attempt to bridge the differences between their respective privacy frameworks by considering technical, political and cross-regional adequacy options.

2

ASEAN and APEC governments should advance harmonisation of national-level privacy regimes. To do so, they can:

- Conduct a landscape analysis to see where they stand in terms of privacy;
- Set goals and objectives for where they want to go based on the elements of a privacy roadmap;
- Execute a plan to evolve privacy elements based on where they stand on the privacy roadmap; and
- Review the experience and case studies of other regional governments to understand common challenges and potential paths forward.

3

ASEAN and APEC governments and privacy enforcement authorities should bolster their interaction with one another to spur deeper collaboration and cross-learning, as well as to build trust and confidence.

4

ASEAN and APEC governments should also draw on non-government privacy experts in the private sector, civil society, and academia to inform their approaches.



---

# Introduction

---

Over the past decade, international data flows have increased global GDP by 10.1 per cent.<sup>2</sup> Data flows accounted for US\$2.8 trillion of global GDP in 2014, a larger share than the global trade in goods.<sup>3</sup> This matters from an economic standpoint across ASEAN and APEC given Asia's size and the growth in data flows that are expected to increase at a rate of 26 per cent CAGR through 2021.<sup>4</sup>

---

<sup>2</sup> James Manyika, et al., "Digital Globalisation: The New Era of Global Flows," McKinsey Global Institute, (February 2016), <https://goo.gl/5jvm1a>, 10.

<sup>3</sup> Ibid, 10.

<sup>4</sup> Cisco, "The Zettabyte Era: Trends and Analysis" (June 2017), <https://goo.gl/KKnyeh>, Executive Summary.

## Worldwide cross-border data flows

Desk research of reports from international organisations, such as the World Economic Forum, trade associations and research think tanks including the European Centre for International Political Economy and the Asia-Pacific MSME Trade Coalition, provides some insights on the economic benefits of cross-border data flows. It also highlights the impact of barriers such as data localisation – requiring that certain types of data remain in country, or be stored on local servers – on the economy (see Annex B for full references):

- Over the past decade, international data flows have increased global GDP by 10.1 per cent, and data flows now account for US\$2.8 trillion of global GDP (2014), a larger share than global trade in goods.
- Between 2005 and 2015, global flows of data grew 45 times, while by the end of 2016, the raw volume of global data flows reached 400 terabits per second. Projections suggest that cross-border data flows will increase another nine-fold by 2020. This growth in data flows contrasts the growth of traditional value flows of physical goods and services, which have barely managed to grow at the pace of worldwide nominal GDP.
- Current trade statistics significantly underestimate the magnitude and growth of cross-border data flows, and as a result, the contributions of cross-border data flows to global growth and to small businesses are significantly underestimated.
- According to UNCTAD, world trade in IT and ICT-enabled services amounted to approximately US\$1.6 trillion or 48 per cent of all traded services in 2007.
- Worldwide, the shift to cloud computing could create nearly 14 million new jobs by 2015, with a majority of these new jobs potentially being in large emerging economies.
- Estimates show that removing foreign digital trade barriers would increase U.S. GDP by US\$16.7 to US\$41.4 billion (0.1 to 0.3 per cent) and wages by 0.7 to 1.4 per cent in the seven digitally intensive sectors.
- The elimination of current data localisation measures in the EU can generate GDP gains of up to 1.1 per cent.
- More than US\$339 billion can be saved by export-focused micro, small and medium enterprises (MSMEs) through the utilisation of digital tools.
- Each one per cent increase in usage of electronic payments produces, on average, an annual increase of -US\$104 in the consumption of goods and services, a 0.04 per cent increase in GDP.
- The shift from cash to digital payments could increase GDP across developing economies by six per cent before 2025, adding US\$3.7 trillion and around 95 million jobs.

## Asia Pacific

- Economies stand to reap multiple benefits if they take action on creating an open, competitive marketplace for cross-border ICT services by removing a number of barriers. By doing so, Asian countries can save up to US\$17.84 billion in Japan, US\$7.42 billion in South Korea, US\$3.04 billion in Indonesia and US\$0.22 billion in Vietnam.
- Global liberalisation of cross-border data flows creates new demand for ICT services, which in turn generates new businesses and creates new jobs. In the long-run it is estimated that global liberalisation will lead to the creation of 2.89 million companies and 23 million new jobs, with over 361,000 new businesses and 2.8 million jobs being created in Japan, South Korea, Indonesia and Vietnam.
- Global liberalisation of cross-border data flows can potentially increase global GDP by US\$1.72 trillion. In Japan, South Korea, Indonesia and Vietnam, GDP is estimated to increase by US\$83.64 billion, US\$33.01 billion, US\$29.38 billion and US\$3.46 billion respectively.
- More than US\$339 billion can be saved by export-focused MSMEs through the utilisation of digital tools.

## India

- 10% increase in total internet traffic and mobile internet traffic increases India's GDP by 3.3% and 1.3% respectively.
- If in the last decade, India had accelerated its participation in all types of global data flows to match leading countries, its GDP is estimated to have been US\$1.2 trillion higher.
- E-commerce is expected to add up to 20 million jobs by 2020. While adjusting for the replacement of offline jobs, it is still expected that e-commerce will create a net addition of 10 million new jobs in India by 2020.

## Philippines

- In the Philippines, six of the top ten fastest growing fintech companies were involved in the payments space. This highlights the importance of digital payments in, to and from the Philippines, and the growing potential of mobile e-commerce.

## Indonesia

- Productivity improvements from digitalising processes and using cross-border data flows including in manufacturing and retail, are estimated to have a US\$34.4 billion and US\$24.5 billion contribution to GDP respectively.
- Digitalisation has boosted overall revenues for micro, small and medium enterprises by up to 80%.
- Cross-border data flows and cloud computing have allowed local firms like Go-Jek to springboard from a small operation in 2014 to a "unicorn" company in just a few short years, raising over billions in investment.
- Data localisation and other barriers to data flows will impose a cost of US\$0.5 billion.

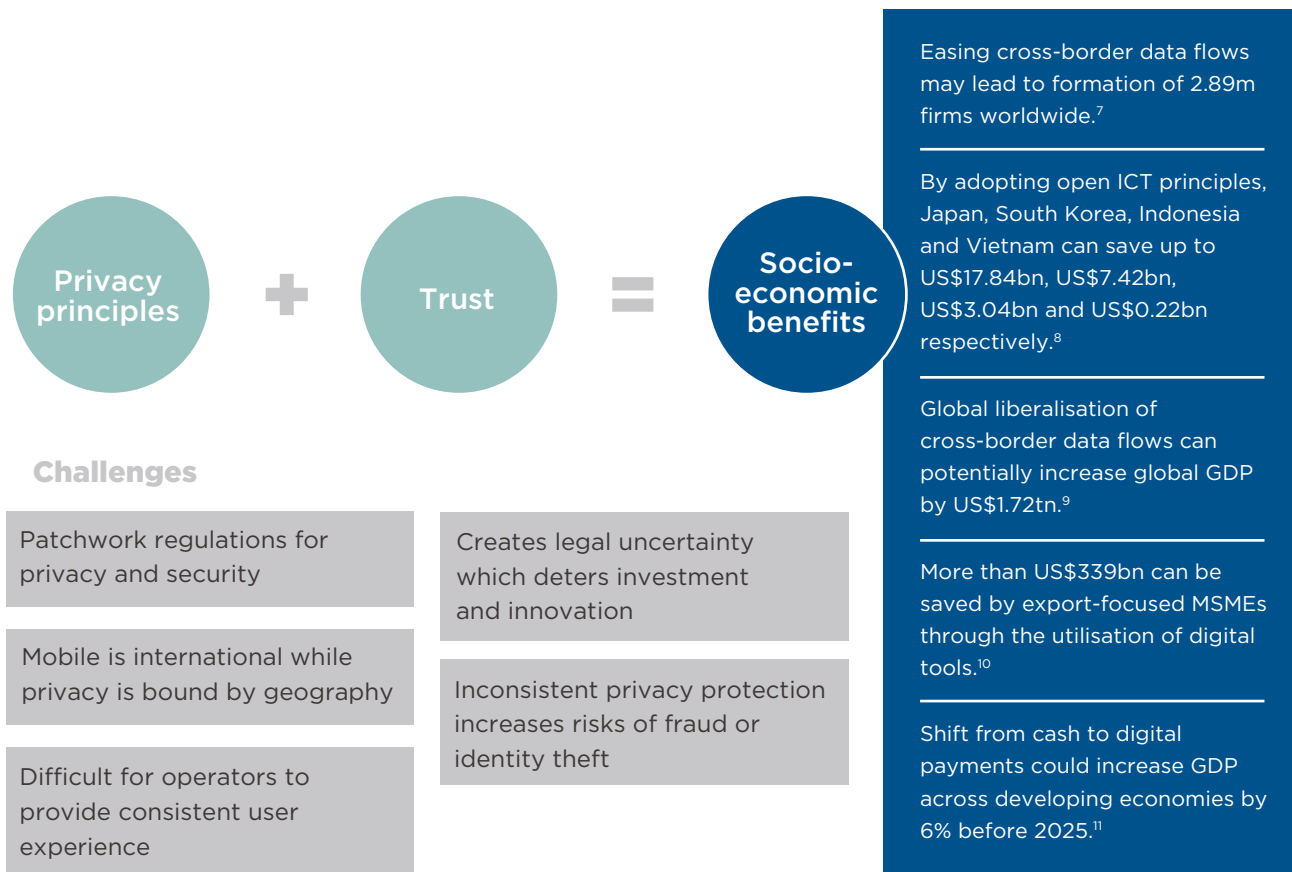
Both ASEAN and APEC have officially recognised in each of their privacy frameworks the vital contribution to trade and economic growth provided by the movement of data between their member economies.<sup>5</sup> Despite this, there are varying applications of national privacy laws in ASEAN and APEC member countries, and no real regional standards for data sharing that are in use. Overarching privacy regulatory frameworks, in particular, will be critical to facilitate cross-border data flows across Asia and around the world, and to improve on the socio-economic outcomes detailed below.

The positions of ASEAN and APEC on data flows track to indicators that clearly show that cross-border data flows enable rapid economic growth across Asia. For

example, the productivity improvements expected from digitising processes and using cross-border data flows in Indonesia's manufacturing and retail sectors are estimated to lead to an additional US\$34.4 billion and US\$24.5 billion contribution to GDP respectively by 2025.<sup>6</sup> Or take the Philippines where, as one of the world's top business process outsourcing locations, the sector generates close to US\$25.5 billion annually, employs 1.4 million people, and is built on low-cost and efficient cross-border data flows across all vertical sectors. Furthermore, the Asia Pacific surpassed North America in 2014 as the world's largest e-commerce market, with US\$525.2 billion in business-to-consumer e-commerce sales.

Figure 1

## Socio-economic benefits of cross-border data flows



5 ASEAN Members include 10 countries in Southeast Asia, and APEC Members include 21 countries spanning across Asia and the Americas. The following countries are members of both groups: Brunei Darussalam, Indonesia, Malaysia, Philippines, Singapore, Thailand and Vietnam. ASEAN-only members include: Cambodia, Laos, and Myanmar. APEC-only members include Australia, Canada, Chile, China, South Korea, Japan, Hong Kong, Mexico, New Zealand, Papua New Guinea, Peru, Russia, Taipei, and the United States. With regards to regional trade and trade agreements specifically, Article 14.8 of the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (incorporating text from the unsigned Trans-Pacific Partnership (TPP-11)) accommodates the APEC Cross-Border Privacy Rules system at a high-level, by requiring each Party to adopt or maintain a legal framework that provides for the enforceable protection of users' personal information, and by encouraging the development of mechanisms to promote compatibility between legal frameworks. In addition, Article 14.11 focuses on enhancing cross-border data transfers.

6 Kaushik Das, Michael Gryseels, Priyanka Sudhir, Khoon Tee Tan. "Unlocking Indonesia's Digital Opportunity," McKinsey & Company (2016) [https://www.mckinsey.com/-/media/McKinsey/Locations/Asia/Indonesia/Our%20Insights/Unlocking%20Indonesias%20digital%20opportunity/Unlocking\\_Indonesias\\_digital\\_opportunity.ashx](https://www.mckinsey.com/-/media/McKinsey/Locations/Asia/Indonesia/Our%20Insights/Unlocking%20Indonesias%20digital%20opportunity/Unlocking_Indonesias_digital_opportunity.ashx), 16.

7 U.S. Chamber of Commerce, "The Economic Impact of Cross-Border ICT Services" (2016), [https://www.uschamber.com/sites/default/files/executive\\_summary.pdf](https://www.uschamber.com/sites/default/files/executive_summary.pdf), 14.

8 Ibid, 13.

9 Ibid, 16.

10 Asia-Pacific MSME Trade Coalition, "SMEs: The New Stakeholders of International Trade" (December 2017), <http://tradecoalition.org/resource/smes-the-new-stakeholders-of-international-trade/>

11 James Manyika, et al., "Digital Finance for All: Powering Inclusive Growth in Emerging Economies," McKinsey & Company (2016), <https://www.mckinsey.com/featured-insights/employment-and-growth/how-digital-finance-could-boost-growth-in-emerging-economies>.



The mobile industry recognises the socio-economic benefits that cross-border data flows help facilitate in a way that respects well-established privacy principles and fosters an environment of trust. One of the major challenges faced by the growth of the mobile internet is that the security and privacy of people's personal information is regulated by a patchwork of geographically-bound privacy regulations, while the mobile internet service is, by definition, international. This misalignment between national privacy laws and global standard practices that have developed within the internet ecosystem makes it difficult for operators to provide customers with a consistent user experience. Equally, the misalignment may cause legal uncertainty for operators, which can deter investment and innovation. The inconsistent levels of protection also create risks that consumers might unwittingly provide easy access to their personal data, leaving them exposed to unwanted or undesirable outcomes such as identity theft and fraud.<sup>12</sup>

Governments in Asia have worked hard to develop and implement privacy frameworks that can effectively protect the data of their citizens, while also allowing data to flow across borders in ways that support trade and innovation. These frameworks encourage convergence across the region, which enables data to flow while maintaining a similar level of protection. Yet gaps remain.

The GSMA commissioned this report to consider these privacy frameworks – at both the regional and national levels – with the objective to identify specific steps that can be taken to support the evolution and convergence of privacy frameworks in Asia, and do so in ways that meet the growing challenges facing ASEAN and APEC regulators. The report builds on the GSMA's previous work with Asian governments, including a 2017 Data Privacy Survey of ASEAN, and additional GSMA reports on privacy.<sup>13</sup>

The methodology taken included research on various regional frameworks and their key principles, as well as diving down into individual countries to identify the approaches they had taken to establish a national privacy framework. In addition, direct interviews with regulators in several ASEAN and APEC economies (Hong Kong, Japan, Malaysia, Philippines, Singapore, and Vietnam) were conducted to understand their own views about national and regional privacy frameworks, the challenges faced when advancing their privacy laws, and factors that helped propel the countries forward. Key challenges cited include:

- How to effectively balance between privacy protections and ICT adoption that drives innovation;
- Costs, skills and time needed to advance privacy frameworks;
- Need to access information;
- Enforcement issues;
- How to implement accountability mechanisms; and
- Lack of understanding and awareness around privacy.

In an effort to develop a resource that may be useful to government stakeholders in Asia, this report first introduces the concept of privacy frameworks and considers and compares examples from around the world in Section 1. In Section 2, it describes the linkages and benefits of harmonisation between ASEAN and APEC frameworks and the options available to further harmonise frameworks at the regional level. Section 3 considers how privacy frameworks evolve at the national level, outlines key elements, and provides a roadmap for Asian privacy regulators to advance their national-level regimes to meet today's challenges and better participate in regional frameworks.

12 For more information and background, see the GSMA's Mobile Policy Handbook sections on "Privacy" and "Privacy and Big Data," [https://www.gsma.com/publicpolicy/handbook/search-results?search\\_keyword=privacy#2](https://www.gsma.com/publicpolicy/handbook/search-results?search_keyword=privacy#2).

13 The GSMA, "The GSMA Data Privacy Survey" (August 2017), Key Findings from the Survey of ASEAN Member States, <https://www.gsma.com/publicpolicy/gsma-data-privacy-survey>; The GSMA Mobile Policy Handbook, sections on, "Privacy", "Privacy and Data Protection for IoT", "Privacy and Big Data", "Cross-Border Data Flows," [https://www.gsma.com/publicpolicy/handbook/search-results?search\\_keyword=privacy#2](https://www.gsma.com/publicpolicy/handbook/search-results?search_keyword=privacy#2), accessed on 28 May 2018; The GSMA, "Mobile Privacy Principles" (5 February 2016), <https://www.gsma.com/publicpolicy/mobile-privacy-principles>; The GSMA, "Cross-Border Data Flows Enable the Digital Economy" (25 September 2017), <https://www.gsma.com/publicpolicy/cross-border-data-flows-enable-digital-economy>; The GSMA, "Safety, Privacy and Security across the Mobile Ecosystem" (24 February 2017), <https://www.gsma.com/publicpolicy/safety-privacy-security-across-mobile-ecosystem>.

---

# Introduction to international data privacy frameworks

---

This section reviews a selection of regional and international data privacy frameworks that were chosen to highlight variations across geography and focus areas, and indicates why they are relevant for Asia. The similarities and differences are subsequently explored in further detail.

---



**“The digital economy, powered by frontier technologies such as the Internet of Things and Artificial Intelligence, has led to a shift in the data landscape where personal data of individuals is increasingly used to gain new business and behavioural insights for provision of better products and services to customers. As organisations harness the value of data, it is crucial that they understand the importance of using personal data responsibly and putting in place adequate safeguards to prevent abuse or unauthorised disclosure or access to the information.”**

Anonymous quote from the GSMA's survey of regulators across APEC and ASEAN that was conducted to inform this report.

## Privacy frameworks in Asia and across the world

### ASEAN Framework on Personal Data Protection (2016)

As a diverse region with different levels of development, ASEAN reached a milestone when it adopted a regional declaration with provisions concerning data privacy in 2012.<sup>14</sup> Four years later, ASEAN Ministers adopted the ASEAN Framework on Personal Data Protection that indicates a set of principles to guide the implementation of data protection measures at both national and regional levels.<sup>15</sup>

The ASEAN Framework on Personal Data Protection seeks to foster regional integration and cooperation and to propel ASEAN towards a secure, sustainable and transformative digitally-enabled economy. It recognises that to achieve this goal, it is essential to strengthen personal data protection which will

contribute to the promotion and growth of trade and flow of information within and among ASEAN member states in the digital economy.

The ASEAN Framework is important for Asian governments since it represents one of the two multilateral data protection and privacy frameworks in the region and was developed to flexibly accommodate varying levels of maturity around data protection and privacy regulation. Economies implementing the ASEAN Framework at a domestic level may adopt exceptions that suit their particular domestic circumstances, and the framework does not create legally binding domestic or international obligations of any type.

*See Annex A1 for more information and a table with the ASEAN Framework on Personal Data Protection Principles*



**“The ASEAN Framework on Personal Data Protection is commendable. It is similar to the Data Protection Principles in Hong Kong’s Personal Data Privacy Ordinance. The accountability principle (which is not stipulated in the PDPO) under the ASEAN Framework is particularly important in the digital age.”**

Anonymous quote from the GSMA’s survey of regulators across APEC and ASEAN that was conducted to inform this report.

### APEC Privacy Framework (2004, 2015)

In November 2004, Ministers for the 21 APEC member economies endorsed the APEC Privacy Framework. The Framework comprises nine guiding principles to help APEC member economies develop a consistent domestic approach to protection of personal information (see table in Annex A2). The second iteration of the Framework was published in 2015. The Framework forms the basis for a regional system called the APEC Cross-Border Privacy Rules (CBPR) that seeks to ensure the continued free flow of personal information across borders, while establishing a voluntary accountability mechanism for meaningful protection for the privacy and security of personal information. Six countries currently participate in CBPR: Canada, Japan, Korea, Mexico, Singapore and the U.S.

Additional implementing measures include the Privacy

Recognition for Processors System (PRP) which employs a similar accountability system to CBPR, with the focus on data processors instead of data controllers, as well as a multilateral mechanism to encourage coordination among data privacy authorities through the Cross-Border Privacy Enforcement Arrangement (CPEA).<sup>16</sup> These are mutually reinforcing measures. For example, a country must first agree to participate in CPEA before it can join the CBPR. The U.S. and Singapore are participants in the APEC PRP System.

The APEC Privacy Framework is important in Asia because it was the first framework developed specifically by and for Asian countries and their counterparts in the Americas, and it incorporates a set of implementing measures to operationalise and enhance accountability.

*See Annex A2 for more information and a table of APEC Information Privacy Principles.*

<sup>14</sup> ASEAN, “ASEAN Human Rights Declaration” (November 2012), <http://asean.org/asean-human-rights-declaration/>, Article 21: Every person has the right to be free from arbitrary interference with his or her privacy, family, home or correspondence including personal data, or to attacks upon that person’s honour and reputation.

<sup>15</sup> ASEAN, “Framework on Personal Data Protection” (16 November 2016), <http://asean.org/storage/2012/05/10-ASEAN-Framework-on-PDP.pdf>.

<sup>16</sup> Cross-Border Privacy Rules System, “Glossary for the APEC CBPR system,” <http://www.cbprs.org/GeneralPages/Glossary.aspx>, accessed on 28 May 2018; data controller refers to organisations that determine the purpose of data collection and how personal data will be processed, while a data processor simply processes the data on behalf of controllers; some regulators only impose obligations on data controllers while others may impose obligations on both.



## OECD Privacy Framework (1980, 2013)

The OECD privacy framework was developed in 1980 and was updated in 2013 to modernise its approach.<sup>17</sup> The original framework represents the first international consensus on how best to balance effective privacy protection with the free flow of personal data. Crafted towards a technology-neutral and flexible set of official guidelines that allow for various means of compliance, the framework has served as a key reference for a large number of national regulatory and self-regulatory instruments, including both the ASEAN and APEC frameworks, as well as many national regimes. As such, the OECD framework is a critical component for Asia and includes guidance on both the necessary elements of a privacy regime, as well as implementing measures.

*See Annex A3 for additional background and a table of OECD principles; see Section 3 for national-level guidance that incorporates OECD recommendations.*

## The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) (1981)

Building on the OECD's work, Convention 108 was signed in 1981 by Member States of the Council of Europe seeking to reconcile the fundamental values of the respect for privacy and the free flow of information between countries. The Convention serves as the first example of a regional agreement to seek to establish minimum standards (such as committing to take necessary measures in their domestic law, and not to prohibit transborder flows of personal data). It has also recently been adopted by several countries outside of Europe: Uruguay in 2013, Mauritius and Senegal in 2016, and Tunisia in 2017. This is a model that Asia could refer to when developing its own regional data flow agreement.

*See Annex A4 for more information and a table of Convention 108 Principles.*

## Madrid Resolution (2009)

In 2009, data protection authorities from over 50 countries approved the "Madrid Resolution" on international privacy standards. This resolution brought together multiple approaches to the protection of the right to privacy, integrating legislation from five continents. It was intended to constitute the foundation for the development of an internationally binding tool that would contribute to a greater protection of individuals' rights and freedoms at a global level.<sup>18</sup> Similar to Convention 108's regional approach, it offers a set of standards that represent international minimums.

The Madrid Resolution is important for Asia because it includes a set of principles and rights to allow for the achievement of a greater degree of international consensus that would serve as reference for those countries that do not have a legal and institutional structure for data protection, along with tools to encourage and aid countries with compliance.

*See Annex A5 for more information.*

## General Data Protection Regulation (2016)

The European Union finalised its General Data Protection Regulation (GDPR) in 2016 and it was put into effect from 25 May 2018.<sup>19</sup> The GDPR has several key elements that have changed the global regulatory landscape in terms of data privacy, control, processing and cross-border data flows. The single most important innovation of the GDPR is the operationalisation of accountability requirements that make organisations liable not just to comply with the law but to be able to demonstrate how they comply. This shifts the burden on to organisations to step up and take responsibility.<sup>20</sup> In return organisations are allowed a certain degree of flexibility and the regulatory approach shifts from ex ante to ex post. It also further adapts the EU's longstanding rights-based approach to privacy.

*See Annex A6 for a table of GDPR Data Subject Rights.*

17 OECD, "The OECD Privacy Framework" (2013), <http://www.oecd.org/sti/ieconomy/privacy-guidelines.htm>; the updated framework focused on the practical implementation of privacy protection due to the incredible volume of personal data being collected, used and stored, the range of analytics leveraging data, the value of data, the evolving threats to privacy, and the global availability of data, while also addressing the global dimension of privacy through improved interoperability.

18 The intention was for the Madrid Resolution to become a "soft law" tool, widely demanded by international companies, in order to respect the minimum privacy needs of citizens worldwide.

19 European Data Protection Supervisor, "The History of the General Data Protection Regulation," <https://goo.gl/4e8UTN>, Accessed on 28 May 2018; the GDPR updated the EU's previous Data Protection Directive of 1995.

20 Some countries apply additional privacy rules for telco/mobile operators.





**In a February 2018 address to the Asia Business Law Institute, Singapore’s Honourable Chief Justice Sundaresh Menon highlighted how the GDPR will have “far-reaching extra-territorial effects” and bring increased “pressure” for companies to adhere to the requirements imposed under the regulation.**

Of additional importance for Asian privacy regulators is that the GDPR extends the jurisdiction of its regulatory landscape of data privacy, as it applies to companies processing the personal data of individuals residing in the EU, regardless of the location of an organisation that is handling the data. It also extends the scope to include conditions on both the entity that determines how and why personal data is collected and processed (“controllers” for its purposes) and the one that processes the data on behalf of the controller (“processors”).<sup>21</sup> And unlike under other regimes, under the GDPR, processors will have significantly more obligations – and liability in the event of a breach.<sup>22</sup>

*Further obligations and additional information can be found in Annex A6.*

## **EU-U.S. Privacy Shield (2016)**

In February 2016, the European Commission and the U.S. Department of Commerce adopted the EU-U.S. Privacy Shield to facilitate transatlantic exchanges of personal data for commercial purposes. It was formally adopted on 12 July 2016, after a predecessor agreement, the U.S.-EU Safe Harbor Framework,<sup>23</sup> was struck down at the Court of Justice of the European Union (CJEU) in 2015. It is important to Asia because the agreement represents an important and working model of a cross-regional approach to privacy.

The EU-U.S. Privacy Shield aims to protect the fundamental rights of EU individuals where their data is transferred to the U.S. and ensure legal certainty for businesses. It builds on the previous U.S.-EU Safe Harbor Framework and imposes stronger obligations on companies in the U.S. to protect the personal data of individuals and stronger monitoring and enforcement by the U.S. Department of Commerce and Federal Trade Commission, including an increased cooperation with the European data protection authorities.<sup>24</sup>

*See Annex A7 for more information.*

21 Where the activities relate to: offering goods or services to EU citizens (irrespective of whether payment is required) and the monitoring of behavior that takes place within the EU. Non-EU businesses processing the data of EU citizens will also have to appoint a representative in the EU.

22 The GDPR also places further obligations on controllers to ensure their contracts with processors comply with the GDPR. Organisations in breach of the GDPR can be fined up to 4 per cent of annual global turnover or €20 million (whichever is greater). This is the maximum fine that can be imposed for the most serious infringements. There is a tiered approach to fines. It is important to note that these rules apply to both controllers and processors.

23 <https://www.ftc.gov/tips-advice/business-center/privacy-and-security/u.s.-eu-safe-harbor-framework>

24 For example, the U.S. Department of Transportation may also be called upon in the context of air traveler information, such as passenger logs.

## Commonalities, divergence and key issues

The analysis below compares the primary frameworks described on the preceding pages. The objective is to identify similarities and points of divergence, as well as the key issues these bring about and what they mean for global cross-border data flows. The comparison intentionally leaves out the EU-U.S. Privacy Shield, which while important as a global example of a cross-regional agreement, is more relevant as an implementing mechanism, as opposed to a normative regulatory framework.

### Common ancestry

The OECD Guidelines represent a common starting point for all the frameworks discussed in this section. The OECD Guidelines include eight principles, which have been incorporated into each of these regimes to some extent or another.

Table 1

### Comparison of data privacy frameworks

	OECD Privacy Framework	Convention 108	Madrid Resolution	APEC Privacy Framework	ASEAN Framework on Personal Data Protection	EU GDPR
<b>Objective</b>	Economic	Fundamental rights	Fundamental rights	Economic	Economic	Fundamental rights
<b>Application scope by jurisdiction</b>	Territorial – subject to national law	Territorial – subject to national law	Territorial – subject to national law	Territorial – subject to national law	Territorial – subject to national law	Extra-territorial – not subject to national law
<b>Application scope by entity – data controllers vs processors</b>	Data controllers	Data controllers	Data controllers	Data controllers + processors (voluntary)	Data controllers	Data controllers + processors (mandatory)
<b>Accountability provisions<sup>25</sup></b>	Principle	None (in original agreement)	Principle + voluntary mechanism	Principle + voluntary mechanism	Principle	Principle + voluntary mechanisms + legal requirements
<b>Consent requirements</b>	Consent, where applicable	N/A	Consent (free, unambiguous and informed)	Consent, where applicable	Consent, where applicable	Consent (freely given, specific, informed and unambiguous, and in some cases, explicit consent)
<b>Default position on data flow – serves to promote vs restrict</b>	Promotes data flow	Restrictive (outside the group); promotes data flow (within the group)	N/A	Promotes data flow	Promotes data flow	Restrictive (outside the group); promotes data flow (within the group)

<sup>25</sup> Accountability provisions here refers to the inclusion or absence within each framework of an accountability principle, as well as implementable mechanisms to drive accountability that can be either voluntary or legal requirements.



## Economic goals vs fundamental rights

The foundational objectives of the OECD, ASEAN, and APEC frameworks all seek to avoid unnecessary barriers to information flows and to ensure continued trade and economic growth in their respective regions. This foundational goal differs from that in Convention 108, the Madrid Resolution, and the GDPR which emphasise fundamental rights to data privacy. For example, the GDPR seeks to enable “free movement of personal data within the EU while protecting fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.” In sum, while the former group emphasises continued trade and economic growth, the latter focuses on fundamental rights, with the impact on the economy or trade emphasised less.

## Application scope by jurisdiction

Perhaps the most critical variation concerns the jurisdictional scope of the agreements. The OECD, ASEAN and APEC frameworks do not seek to replace domestic rules but call on member states to voluntarily implement their provisions. The OECD Guidelines consist of recommendations for member states around the protection of privacy and the cross-border flow of personal data. Participants in the ASEAN Framework endeavor to cooperate, promote and implement the Principles of Personal Data Protection in their domestic laws and regulations, and facilitate the free flow of information among participating economies. However, there is tolerance for those that are not yet in a position to adopt such commitments. APEC is intended to provide a minimum level of protection where there are no applicable domestic privacy protection requirements in a country but does not displace or change a country’s domestic laws and regulations. Convention 108 is more forceful – stating that each signatory “shall take the necessary measures in its domestic law” – but does not explicitly supersede national rules. Alternatively, the GDPR is directly applicable on legislation in the 28 EU Member States.<sup>26</sup> It applies to all organisations that target or monitor

the personal data of data subjects located in the EU, regardless of the company’s location or where the data is processed. So, while almost all the other frameworks seek to guide national legislation voluntarily, the GDPR more explicitly blurs national borders and jurisdictions by focusing on the protection of EU data subjects’ rights, regardless of geography – including protection of EU subjects’ rights outside of the EU.

## Application scope by entity – data controllers vs processors<sup>27</sup>

Before the GDPR, data privacy requirements typically only applied to data controllers. The GDPR represents an important change in the privacy sphere as it applies to both controllers and processors. Unlike under other regimes (except for Convention 108 which does not address this issue), the GDPR imposes significant obligations and potential liabilities on processors. This, however, in no way relieves controllers of their obligations. On the contrary, the GDPR places further obligations on controllers to ensure their contracts with processors comply with the GDPR. The GDPR also provides for competent supervisory authorities to approve Binding Corporate Rules (BCRs) for data processors.<sup>28</sup> Meanwhile, APEC has a separate but voluntary compliance track for processors through its Privacy Recognition for Processors (PRP) system.

## Accountability provisions

Except for Convention 108, all privacy regimes have the common principle of accountability but the compliance requirements and execution differ.<sup>29</sup> For APEC and its CBPR and PRP systems, compliance assessments are done by the Accountability Agent of each member economy. Under the GDPR, controllers and processors are expected to put into place comprehensive but proportionate governance measures to this end. For example, certain organisations (such as public authorities, or whose processing activities are at a large scale or deal with sensitive information) are

<sup>26</sup> Though it does require some legislation for member states to derogate from some of its provisions (e.g. age at which a child can consent under the GDPR). Further, the United Kingdom voted to leave the European Union on 23 June 2016 but, at time of writing, is committed to passing enabling legislation for the GDPR to take effect, and to maintain it indefinitely.

<sup>27</sup> Data controller refers to organisations that determine the purpose of data collection and how personal data will be processed, while a data processor simply processes the data on behalf of controllers. Some regulators only impose obligations on data controllers while others may impose obligations on both.

<sup>28</sup> General Data Protection Regulation, <https://gdpr-info.eu/>, Accessed on 28 May 2018, Article 47 on BCRs; BCRs govern transfers of personal data by a corporate group or a group of enterprises engaged in a joint economic activity for international transfers from organisations established in the EU to organisations within the same group established outside the EU; Data Protection Working Party, “Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules” (29 November 2017), [https://ec.europa.eu/newsroom/just/document.cfm?doc\\_id=48798](https://ec.europa.eu/newsroom/just/document.cfm?doc_id=48798) (this document was released to facilitate the use of BCRs for processors).

<sup>29</sup> Convention 108 does not address accountability in the original agreement, but a separate protocol on supervisory authorities and transborder data flows signed in 2001 calls on signatories to establish independent supervisory authorities. See Council of Europe, “Convention 108 and Protocol,” <https://www.coe.int/en/web/data-protection/convention108-and-protocol>, accessed on 28 May 2018.



required to appoint Data Protection Officers within their organisation, and their ability to demonstrate compliance will have an important impact on authorities' determination of liability and corresponding penalties. Meanwhile, ASEAN maintains accountability as a principle, but has yet to develop an implementation process around accountability.

---

## Consent requirements

Again, except for Convention 108, all regimes have a common principle of consent. However, the OECD, APEC, ASEAN, and Madrid frameworks have a broader interpretation of consent compared to the GDPR. The former three frameworks require that, where appropriate, individuals should be provided with clear, prominent, easily understandable, accessible and affordable mechanisms to exercise choice in relation to the collection, use and disclosure of their personal information. The Madrid Resolution is a little firmer, calling for “free, unambiguous and informed” consent, while the GDPR’s is more stringent through its interpretation of consent as “freely given, specific, informed and unambiguous” and in some cases “explicit consent.”

## Default position on data flows – serves to promote vs restrict

Frameworks differ in their default approach to data transfers across borders. The OECD encourages countries to restrain from restricting data flows where there are sufficient safeguards and if the other country also observes similar guidelines. Likewise, under the APEC system, governments should ensure that there are no unreasonable impediments to cross-border data transfers while protecting the privacy and security of personal information. The ASEAN Framework’s objective is to “strengthen the protection of personal data in ASEAN and to facilitate cooperation among the Participants, with a view to contribute to the promotion and growth of regional and global trade and the flow of information” though it does not explicitly address restrictions on data flow.

The GDPR, and to a lesser extent Convention 108, is more restrictive in the transfer of personal data of EU citizens to third countries or international organisations unless they meet a set of conditions, in order to ensure that the level of protection of individuals afforded by the GDPR is not undermined. The conditions – which are legally enforceable – include the designation by the European Commission that a country meets an “adequate” level of personal data protection, or where standard contractual clauses or Binding Corporate Rules (BCRs) exist. It should be recognised, however, that the EU approach also prohibits restrictions on data flows between Member States/Parties.

---

## Reconciling frameworks

The identified differences in approach and focus across different data privacy frameworks translate into different levels of regulatory stringency. This may create complications for entities handling data of citizens in diverse jurisdictions, which may be subject to one or more regimes. Furthermore, regimes may collide as different economies and jurisdictions seek to obtain different objectives. While the EU seems keen to adopt increasingly strict regulation, even at the risk of hampering data flows with countries outside the EU, other countries may emphasise data flows to foster trade and economic growth. Both objectives –

protecting privacy and promoting economic growth – are being promoted through the recent EU-Japan mutual adequacy agreement, the ongoing EU-Korea discussions, as well as the longstanding dialogue between the EU and APEC.

Across Asia, the divergence between various frameworks may create tensions between countries and regions. Data privacy regulators and stakeholders are today grappling with these tensions, and data privacy frameworks are continually evolving in various attempts to address these challenges.

# Harmonising data privacy frameworks in Asia – bridging ASEAN and APEC



**“Participating in a regional privacy scheme like APEC CBPR or ASEAN Framework on Personal Data Protection brings the benefit of gaining trust among countries, and therefore improving the ASEAN/APEC cross-border transactions among citizens, companies, organisations and governments.”**

Anonymous quote from the GSMA's survey of regulators across APEC and ASEAN that was conducted to inform this report.

## Introduction

ASEAN countries have realised steady progress towards regulatory frameworks for data protection and privacy. Now is an important time to accelerate progress so that the region can continue to expand in business and trade. This process may be hastened and made easier by improving linkages at the regional level between Asia's two main data privacy frameworks – the ASEAN Framework on Personal Data Protection, and the APEC Privacy Framework and its accompanying systems.

While these two frameworks already share many of the same principles, further formal integration and harmonisation of their respective approaches may help countries, especially those in ASEAN, more fully and broadly bridge data protection gaps and reduce inconsistencies across data privacy regimes. Such harmonisation may support the dual objectives of increased economic growth and improved data protection and privacy.

Table 2

### Common data privacy principles between ASEAN and APEC

ASEAN Framework on Personal Data Protection	APEC Privacy Framework
	Preventing harm
Consent, notification and purpose	Notice
	Choice
	Collection limitations
Accuracy of personal data	Integrity of personal information
Security safeguards	Security safeguards
Access and correction	Access and correction
Transfer to another country or territory	Uses of personal information
Retention	
Accountability	Accountability

Given the strong overlap in general principles, the most substantive differences between ASEAN and APEC are the:

- Addition of formal mechanisms within APEC to encourage cooperation between data privacy enforcement authorities in the Cross-Border Privacy Enforcement Arrangement (CPEA); and
- Existence in APEC of functional self-assessment and accountability mechanisms in both the Cross-Border Privacy Rules (CBPR) and Privacy Recognition for Processors System (PRP).

There are several options to more formally integrate and harmonise the ASEAN and APEC frameworks. This section will consider and analyse these available options, after first considering some of the challenges that harmonisation poses.

## Challenges to harmonisation

### Different status of data privacy laws

Asian governments surveyed for this report acknowledged that mechanisms like APEC CBPR or something similar present a good model for ASEAN.<sup>30</sup> Yet they also noted concerns regarding the feasibility of harmonisation given the different status of data privacy laws (or lack thereof) in some ASEAN countries. Some countries are simply much further along in the development of data protection and privacy regulation and administrative capacity. One government representative interviewed for this report stated that it is more important for each ASEAN country to develop and implement their own personal data protection/privacy laws before moving towards the harmonisation of regional frameworks, while others acknowledged these processes can work in parallel and that the harmonisation of frameworks will be made easier as more countries develop their data protection and privacy regulations at the national level. Section 3 of the report presents a roadmap covering the key elements of a national-level approach to data privacy.

### Cost and lack of capacity

Government stakeholders also suggested there is some concern about the cost of implementation and the skills/expertise required to manage the process. For example, a number of countries in the region have not yet established independent data privacy enforcement authorities. And some countries have specifically noted their interest in further training and assistance to better understand regional data privacy frameworks like APEC.

Various efforts are underway to tackle this challenge. ASEAN's Framework on Personal Data Protection suggests implementation to include capacity building efforts like workshops or seminars to impart ASEAN member states with the knowledge and skills necessary to develop personal data protection policies, and there

are additional upcoming initiatives like the ASEAN Framework on Digital Data Governance to support governments and businesses further.<sup>31</sup> Organisations like the Asia Business Law Institute (ABLI) have gathered governments and non-government stakeholders together to conduct in-depth research and produce knowledge products around the regulation of international data transfers, privacy, and data protection across Asia.<sup>32</sup> Additionally, ASEAN and APEC governments are conducting more and more consultations with stakeholders that serve as critical mechanisms to share information.<sup>33</sup> Undoubtedly, as data privacy continues to become an ever more important realm of policy, it will be accorded additional priority and resources across all stakeholder groups.

### Certification problems

Another major challenge noted by several governments with regard to the APEC CBPR is the system's reliance on third-party Accountability Agents (AAs) that serve as the certification bodies that underpin the system. Currently only two AAs are accredited within CBPR: TrustArc in the U.S. and JIPDEC in Japan.<sup>34</sup> Some uncertainty exists about whether countries will be able to identify and appoint accredited organisations to serve as agents throughout Asia.<sup>35</sup>

However, governments that are already participating in CBPR and those with more developed data privacy regimes see this as less of a major obstacle, citing the existence of capable certification bodies within their respective geographies. One ASEAN government (who is not yet participating in CBPR) suggested that identifying an Accountability Agent should be built around information sharing among different sectors within a country, cooperation and discussions between the countries in the region, and internal capacity building. Another APEC member economy (also not yet participating in CBPR) provided the following quote:

30 The GSMA surveyed six governments across ASEAN and APEC (Hong Kong, Japan, Malaysia, Philippines, Singapore, Vietnam) that were selected to represent a diversity of development levels, political and social cultures, and maturity in data protection regimes.

31 ASEAN, 17th ASEAN Telecommunications and Information Technology Ministers Meeting and Related Meetings Joint Media Statement (1 December 2017), [http://asean.org/storage/2017/12/14-TELMIN-17-JMS\\_adopted.pdf](http://asean.org/storage/2017/12/14-TELMIN-17-JMS_adopted.pdf); in the Joint Media Statement, ASEAN announced a Work Plan for the development of the Framework on Digital Data Governance to strengthen digital data collection and management capabilities of businesses across the region, engender trust in businesses' data collection and management practices, and foster an environment that encourages digital adoption, data flows and data innovation for the benefit of ASEAN citizens.

32 ABLI held a meeting in February 2018 entitled "Towards A Shared Legal Ecosystem for International Data Flows in Asia." The forum information and program are available at <http://abli.asia/NEWS-EVENTS/Whats-New/ID/52>.

33 ASEAN regularly holds stakeholder consultations along the sidelines of meetings like the Telecommunications and Information Technology Senior Officials Meeting (TELSOM); APEC convenes stakeholders through various mechanisms like the APEC Business Advisory Council.

34 Information on TrustArc and JIPDEC available at <http://www.cbprs.org/Agents/AgentDetails.aspx>.

35 While countries can signal their intent to use existing AAs, there exists interest to deepen the bench of AAs in the region.





**“Accountability Agents are crucial to the success of the APEC CBPR because they are the primary gatekeepers to make sure that all participating organisations live up to the high data protection standard. A good Accountability Agent should have good track record in auditing or certification; be proficient in data protection regulations; and have high credibility. The Accountability Agent should also have a strong financial position to ensure the continuity of its operation, as well as the operation of the CBPR system.”**

Anonymous quote from the GSMA’s survey of regulators across APEC and ASEAN that was conducted to inform this report.

Additionally, governments relayed concerns that the certification cost is high, which may be too burdensome to small and medium-size enterprises (SMEs). While SME participation is an issue, one government suggested that their interactions with industry indicated that APEC CBPR certification for companies in general “is one way of differentiating themselves from competitors as it demonstrates that the organisation’s data protection policies and practices meet international standards.” Another suggested that “with APEC CBPR certification, business operators can appeal both domestically and

overseas to improve their brand power as trusted business partners.”<sup>36</sup> These may be strong incentives for both large and small businesses to participate in various schemes as data protection and data privacy becomes a more pressing issue. Furthermore, governments indicated their support to raise awareness about the benefits of systems like APEC CBPR.

All of the above suggest there is a need for these issues to be reviewed when considering implementation of the existing ASEAN and APEC regimes and possible methods to harmonise them further.



**“Frameworks are a reflection of the culture, custom, and history of countries or regions. When considering the system of countries or regions and the harmonisation with enforcement activities, it is essential to look at the system and understand the culture or soft law as well. Even though it might take a lot of time, there is a possibility to develop those mechanisms in the future.”**

Anonymous quote from the GSMA’s survey of regulators across APEC and ASEAN that was conducted to inform this report.

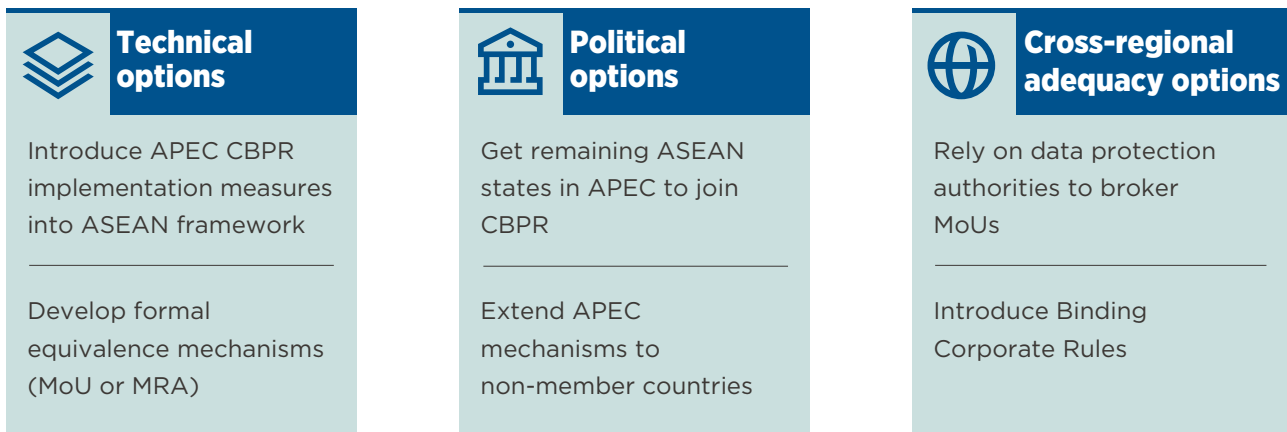
36 Anonymous quote from the GSMA’s survey of regulators across APEC and ASEAN that was conducted to inform this report.

## Harmonising mechanisms to bridge ASEAN and APEC

While regional governments acknowledge challenges to greater harmonisation exist (such as different status of data privacy laws, cost and capacity issues, and certification problems), several interesting options exist to more formally integrate and harmonise ASEAN's Framework and the APEC privacy system. These include technical, political, and cross-regional adequacy options.

Figure 2

### Bridging ASEAN and APEC privacy frameworks



## Technical options

### Introduce CBPR implementation measure into ASEAN framework

The APEC Privacy Framework and its accompanying implementing measures contain important provisions that ASEAN could incorporate to accelerate progress on its own personal data and privacy framework. Section 3 of this report outlines many of these elements in greater depth from the perspective of a national regulator moving towards a more mature personal protection and privacy regime, but it is worth ASEAN leadership considering how to better match and deploy more functional accountability mechanisms, be these through:

- The appointment of data protection authorities (DPAs) across ASEAN member states who do not yet have them, and a system for DPAs to effectively cooperate across borders, akin to APEC's CPEA<sup>37</sup>; and

- The development of voluntary certification schemes that allow private firms and organisations to implement data protection and privacy rules for cross-border transfer of personal data that meet ASEAN Framework on Personal Data Protection and APEC privacy guidelines, such as the APEC CBPR and PRP.

Any such effort to bridge the ASEAN and APEC frameworks around these components will require ASEAN leaders to determine whether to mirror APEC's system as a whole or devise their own that is tailored for the region. Given the unique and diverse nature of ASEAN – as well as the fact that data protection and privacy norms are constantly evolving to match technological, legal and societal changes – it is more likely ASEAN will consider the merits of the APEC System but is likely to formulate its own system that will incorporate certain aspects of APEC, in addition to bringing in additional elements unique to ASEAN.

37 For example, Hong Kong, Japan, Korea, Macau, the Philippines and Singapore data privacy authorities belong to the Asia Pacific Privacy Authorities (APPA) meeting that convenes twice a year.



**“The general principles for data protection are similar across different countries and regions. Under the strong tide of globalisation, there is a genuine need to facilitate cross-border data transfers by mutual recognition of different privacy rules systems.”**

Anonymous quote from the GSMA’s survey of regulators across APEC and ASEAN that was conducted to inform this report.

## Developing formal equivalence mechanisms

Equivalence mechanisms present several interesting opportunities to deepen harmonisation between ASEAN and APEC. According to consultations with ASEAN and APEC governments conducted for this report, any solution should be based on common principles allowing data to be transferred between the member states of each group based on a form of “equivalence” test.<sup>38</sup> Some of these principles can be realised between the ASEAN bloc and APEC, others are better suited to individual ASEAN member economies and APEC, and some pertain to ways in which ASEAN-based organisations and companies may leverage APEC systems.

### 1 Memorandum of Understanding

To develop formal equivalence mechanisms between the ASEAN bloc and the APEC economies, it may be useful to engage in a Memorandum of Understanding (MoU). An MoU is a nonbinding agreement between two or more parties outlining the terms and details of an understanding, including each party’s requirements and responsibilities. There is a precedent for this in ASEAN: the group has signed multiple MoUs, including with the Government of China (on Cooperation in Information and Communications Technology).<sup>39</sup> These usually detail objectives, areas for cooperation, and implementation.

ASEAN as a bloc could engage in an MoU with APEC relating to data protection and privacy, such as an extension of APEC CBPR to ASEAN member states who meet CBPR requirements. The MoU could evolve into a more formal contract and afford ASEAN member

countries the same trusted mechanisms for cross-border flows of personal information recognised by APEC. Individual ASEAN countries could also consider MoUs.

Negotiating an MoU as a bloc would take more time but broaden the application, while individual MoUs could be advanced more quickly at the expense of a more patchwork set of commitments.

### 2 Mutual Recognition Agreements

Another means to implement a formal equivalence mechanism could include something similar to Mutual Recognition Agreements (MRAs).<sup>40</sup> ASEAN has traditionally used MRAs to establish frameworks that encourage member economies to recognise qualifications of professionals who are certified in other economies, especially in the services sector. For example, previous MRAs have provided a means to recognise another country’s conformity assessment in telecom equipment.<sup>41</sup>

This type of bilateral agreement could be executed by the ASEAN bloc to recognise privacy certifications for cross-border data protection set forth by the APEC CBPRs. Also, as the readiness level of ASEAN countries varies, individual member states could choose to execute an MRA at a level of data protection set forth by the APEC CBPRs.

The pros and cons of a bloc approach versus an individual country approach are similar to the cost and benefit analysis of MoUs briefly described above, although because MRAs deal with specific professional accreditations, they are typically longer, more complicated and less readily adapted to multiple iterations.

38 The concept of an “equivalence test” comes from the EU, where it relates to a finding by courts that the laws and practices of the third country is “essentially equivalent” to that guaranteed within the EU. Note that the EU’s adequacy test has been interpreted by the European Court of Justice in the Maximilian Schrems v Data Protection Commissioner case as an “essentially equivalent”; Maximilian Schrems v Data Protection Commissioner (Case C-362/14), (Court of Justice of the European Unions, 2014), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CJ0362>. The notion of equivalence in Asia may be different and more flexible than that in the EU.

39 ASEAN, Memorandum of Understanding between ASEAN and the People’s Republic of China on Cooperation in Information and Communications Technology (8 October 2003), <https://goo.gl/C2za98>.

40 MRAs are non-binding agreements.

41 ASEAN, ASEAN Sectoral Mutual Recognition Arrangement for Electrical and Electronic Equipment (5 April 2002), <https://goo.gl/FvB4tS>.

## Political options

### ASEAN members in APEC

One option to align ASEAN further with APEC is for countries that are member states in both groups to begin participating formally in APEC mechanisms like CBPR, PRP, and CPEA. Seven of ASEAN's ten

members are also APEC members.<sup>42</sup> Singapore has joined all three APEC mechanisms, and the Philippines recently indicated it will join CPEA, which often serves as a precursor to joining CBPR. However, other ASEAN members have been less active and vocal about potentially joining APEC CBPR.



**“Equivalence mechanisms between different privacy rules system will be valuable, particularly if the mechanisms will not pose a heavy compliance burden to companies.”**

Anonymous quote from the GSMA's survey of regulators across APEC and ASEAN that was conducted to inform this report.

The benefit of an organic and gradual merging of ASEAN and APEC through its joint member states is that it requires little additional coordination (and thus cost) through ASEAN or APEC. However, this approach would, without further adjustment to either system, leave 3 ASEAN members (Cambodia, Laos and Myanmar) without means to participate in APEC and its data protection regime.

### Extending APEC mechanisms to non-member countries

Another option to further align ASEAN with APEC is for APEC to begin allowing non-APEC members states to participate in APEC accredited systems like CBPR. A number of countries outside of APEC are rumoured to have expressed an interest in APEC CBPR in the context of bilateral trade discussions. Several consultation responses by governments for

this report indicate their interest in and support for having non-members participate in the APEC Privacy Framework and its implementing measures, as long as such a mechanism is contingent on a country's ability to meet the APEC data protection standard.

Discussions on this option are ongoing within APEC. One benefit of this approach is that it removes the need for action within the ASEAN political framework. However, discussions have been slow. Unless there are intense efforts by governments and industry to build momentum, this concept is unlikely to come to fruition in the immediate future. One government surveyed suggested the current focus is, and should be, on how to get existing members of APEC into the APEC CBPR system first.

It should be noted that this option and the option above concerning the integration of ASEAN-APEC countries are not mutually exclusive and could be explored in parallel. Indeed, they could be mutually reinforcing.

## Cross-regional adequacy options

Given the extra-territorial aspects and aspirations of the European Union's (EU) data protection law, the EU has developed models for fostering harmonisation between it and other countries. ASEAN and APEC could draw on and adapt these models when considering the above mechanisms.

**Rely on DPAs to negotiate.** The work of ASEAN towards an MoU with APEC could be realised in the same way the EU has been brokering a potential agreement with APEC on privacy protections. In 2012, the EU sent DPA representatives to the APEC meeting to review the APEC CBPR system and compare it with

<sup>42</sup> Joint members of both ASEAN and APEC include: Brunei Darussalam, Indonesia, Malaysia, Philippines, Singapore, Thailand and Vietnam. ASEAN-only members include: Cambodia, Laos, and Myanmar.



the framework in place in the EU. This interest grew and led to a formal joint review between European DPAs and the APEC Data Privacy Subgroup. The purpose was to determine where the systems share similarities, where there are potential gaps, and how the two systems could harmonise.<sup>43</sup>

An overlapping, but more granular and detailed, example to draw on is the EU's adequacy approach, where it negotiates directly with countries or economic blocs to ensure that other countries provide an "adequate" level of protection for personal data from the EU. One model outcome is the EU-U.S. Privacy Shield (discussed in Section 1) and there are other discussions in progress, including the EU-Japan reciprocal adequacy arrangement,<sup>44</sup> EU-Korea adequacy talks, as well as EU-APEC interoperability talks. The time needed for such negotiations varies. The EU-U.S. Privacy Shield took only one year of negotiations before it was adopted, because it was intended to address gaps in the 2000 U.S.-EU Safe Harbor Agreement. For EU-Japan, it took slightly over a year since the EU announced its prioritization of EU-Japan adequacy talks before both sides issued a joint statement in May 2018, stating that progress has been made to bridge the differences between the two economies.<sup>45</sup> Prior to that, Japan's Personal Information Protection Commission (PPC) opened consultations for its draft guidelines relating to adequacy findings for international personal data transfers from Europe to Japan. The draft guidelines required some supplementary measures for sensitive data, record keeping, data transfer and anonymised data.<sup>46</sup> This signifies significant progress in enabling data flows between the EU and Japan, while the EU-Korea discussions are ongoing.

**Binding Corporate Rules.** Another similar approach, but one that focuses on organisations as opposed to countries, is the use of Binding Corporate Rules (BCRs). BCRs were originally developed by the EU to allow multinational companies and organisations to

make transfers of personal data internationally within the same corporate group to countries that did not provide what the EU deemed an adequate level of protection. In Asia, the CBPR system currently applies to transfers between organisations operating within the geography of participating APEC economies. However, ASEAN governments could, on behalf of firms and organisations based in their jurisdiction, petition APEC to extend a BCR-type model to allow the CBPR system to operate outside of APEC within a company-level structure. EU and APEC experts have already developed an informal BCR-CBPR "referential" to serve as useful checklist for organisations applying for authorisation of BCR and/or certification of CBPR.<sup>47</sup>

This would alleviate the need to formally extend APEC to non-member economies and instead widen the scope of CBPR at the organisational-level. However, this would require significant changes to the current CBPR system. It is worth noting again that ASEAN-based organisations may also face difficulties identifying effective means to certify their adherence to the system, such as through an accredited AA (as discussed above). The BCR system in the EU has also been very expensive for companies, further underscoring the cost concern of some Asian governments.

Lastly, the EU GDPR came into effect on 25 May 2018. If ASEAN and APEC economies do not establish some ground and integrate further, the GDPR will continue to shape privacy regimes organically, as governments shift their privacy rules to meet the challenge of integrating with the EU. While some aspects of this are inevitable given the need for Asian entities to conduct digital trade with their European counterparts, ASEAN and APEC privacy laws may be impacted to an even greater extent. They may ultimately be driven by Europe and European culture and standards if the region does not develop a deeper set of privacy norms. ASEAN and APEC governments should engage more closely if they want to ensure their particular domestic imprimatur is applied in the region.

43 John Kropf and Malcolm Crompton, "The EU and APEC: A Roadmap for Global Interoperability?" International Association of Privacy Professionals (26 November 2013), <https://iapp.org/news/a/the-eu-and-apec-a-roadmap-for-global-interoperability/>.

44 European Commission, "The European Union and Japan agreed to create the world's largest area of safe data flows", (17 July 2018), [http://europa.eu/rapid/press-release\\_IP-18-4501\\_en.htm](http://europa.eu/rapid/press-release_IP-18-4501_en.htm)

45 European Commission, "Joint statement by Commissioner Věra Jourová and Haruhi Kumazawa, Commissioner of the Personal Information Protection on the state of play of the dialogue on data protection" (31 May 2018), [http://europa.eu/rapid/press-release\\_STATEMENT-18-4021\\_en.htm](http://europa.eu/rapid/press-release_STATEMENT-18-4021_en.htm).

46 Daisuke Tatsuno and Kensaku Takase, "Data Protection - Significant Developments on Adequacy Findings between Japan and Europe" (2 May 2018), <http://www.bakerinform.com/home/2018/5/2/data-protection-significant-developments-on-adequacy-findings-between-japan-and-europe>.

47 APEC, "Joint work between experts from the Article 29 Working Party and from APEC Economies, on a referential for requirements for Binding Corporate Rules submitted to national Data Protection Authorities in the EU and Cross-Border Privacy Rules submitted to APEC CBPR Accountability Agents" (2014), [https://www.apec.org/-/media/Files/Groups/ECSG/20140307\\_Referential-BCR-CBPR-regs.pdf](https://www.apec.org/-/media/Files/Groups/ECSG/20140307_Referential-BCR-CBPR-regs.pdf).

## The process to make harmonisation work for ASEAN and APEC

International harmonisation across privacy regimes is not an easy task. It is made even less so in Asia given several of the factors raised above, such as the size of the continent and its diverse array of countries, levels of economic development, legal systems, and social and cultural proclivities. These factors

can slow agreements through key institutions like APEC and ASEAN. This is not to belittle the effort, but to recognise it will take work and perseverance to promote greater harmonisation through these multilateral bodies. The end goal will be to reap the benefit of greater economic growth and development.



**“To seize common opportunities and responding to common challenges in the Asia-Pacific region and beyond, both ASEAN and APEC will benefit from shared learning of best practices and experiences. Moving forward, ASEAN and APEC can achieve more by working closer together.”**

Anonymous quote from the GSMA's survey of regulators across APEC and ASEAN that was conducted to inform this report.

ASEAN could adopt elements of APEC, especially CBPR, by taking concrete implementation measures. But any future ASEAN data protection and privacy framework should be an inclusive instrument that ensures the participation and economic acceleration of less-developed member countries. As harmonisation proceeds, ASEAN and APEC should include actionable steps and a timeframe to ensure participation across all countries.

As such, greater integration and harmonisation between Asia's privacy frameworks must recognise the level of maturity and readiness of a country to adopt

new features. Both ASEAN and APEC governments have expressed support for a pan-Asian approach to privacy and data protection, but “one that is responsive to the differences in the ASEAN region, and one that considers level of maturity of laws, cultural, and socio-political nuances across the different jurisdictions.”<sup>48</sup> A joint regional approach should be an evolving instrument that is updated and reviewed as specific countries adapt to regional changes and enact data protection regulation. The following section of this report addresses these issues and offers a roadmap for Asian privacy regulators.

<sup>48</sup> Anonymous quote from the GSMA's survey of regulators across APEC and ASEAN that was conducted to inform this report.





---

# Privacy regime roadmap

---



**“The establishment of rules considering the balance between utilisation and protection of personal information is one of organisational philosophy.”**

Anonymous quote from the GSMA's survey of regulators across APEC and ASEAN that was conducted to inform this report.



## Background

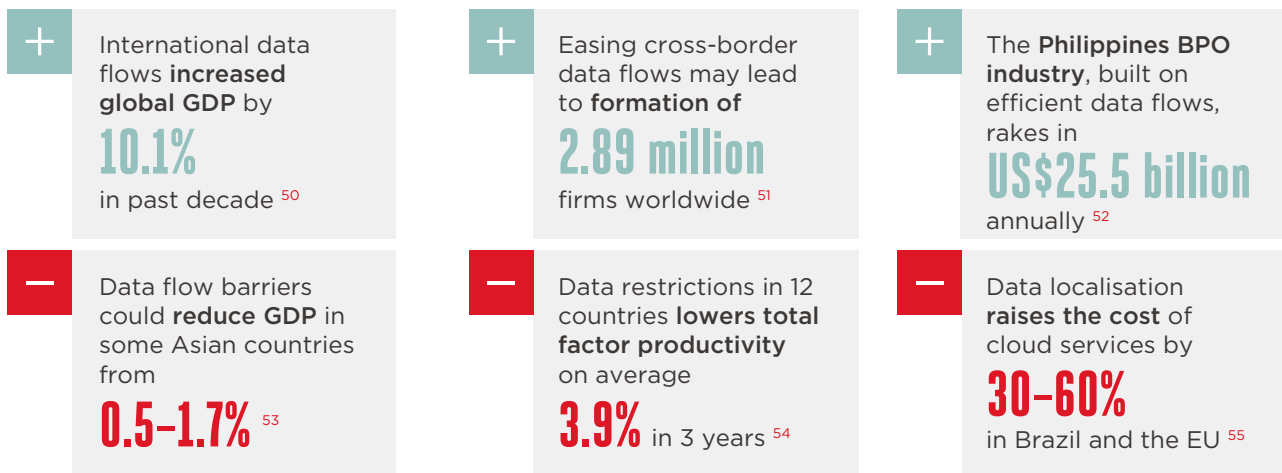
Privacy discussions are gaining traction not only at the regional level, but in individual ASEAN and APEC countries. The benefit of evolving a country's approach to privacy is that it will help to reduce barriers to investment that restrictive data flow regulations may cause; it should also create a clearer compliance environment for businesses that wish to operate in that country. This will lower costs and risks, making a country a more attractive investment and business destination – see the figure below that highlights some

of the economic benefits around cross-border data flows in Asia (and further information in Appendix B).

On the other hand, data localisation and other barriers to cross-border data flows are likely to have a negative economic impact. For example, a 2018 Asia Cloud Computing Association report found that barriers to cross-border data flows are estimated to reduce Indonesia's GDP by 0.5 per cent and Vietnam's GDP by 1.7 per cent.<sup>49</sup> Therefore, getting data protection right is critical for policymakers and regulators.

Figure 3

### Impacts of data flows



Regional privacy frameworks can help guide national-level regulation which, once enacted, can in turn help prepare countries to better integrate with their regional neighbours, to the economic benefit of all. Establishing a mature privacy framework at the national level can help a country prepare to join either the APEC CBPR system, an evolved ASEAN equivalent or other data privacy equivalence systems. So, whereas the previous section dealt with how those frameworks can better harmonise at the regional level, this section will focus on how countries can better harmonise at the national level. It should be recognised that these parallel harmonisation processes feed into one another and are mutually reinforcing. Countries

may adopt different approaches when it comes to privacy and are at different levels of progress, but they are all aiming for the same outcome – to achieve a mature privacy framework that can accord a good level of protection for individuals while ensuring businesses remain competitive

This section will identify the milestones in a country's journey towards developing a mature privacy framework that can aid policymakers' understanding of where their country stands, where they want to go, and key next steps for how to get there. Case studies of different countries will highlight some common challenges faced by countries and how they can be overcome.

49 Asia Cloud Computing Association, 28 and 57.

50 James Manyika, et al., "Digital Globalisation: The New Era of Global Flows," McKinsey Global Institute, (February 2016), <https://goo.gl/5jvm1a>, 10.

51 U.S. Chamber of Commerce, "The Economic Impact of Cross-Border ICT Services" (2016), [https://www.uschamber.com/sites/default/files/executive\\_summary.pdf](https://www.uschamber.com/sites/default/files/executive_summary.pdf), 13.

52 IDC, "Cloud Computing's Role in Job Creation" (March 2012), [https://news.microsoft.com/download/features/2012/IDC\\_Cloud\\_jobs\\_White\\_Paper.pdf](https://news.microsoft.com/download/features/2012/IDC_Cloud_jobs_White_Paper.pdf).

53 Asia Cloud Computing Association, "Cross-Border Data Flows: A Review of the Regulatory Enablers, Blockers, and Key Sectoral Opportunities in Five Asian Economies: India, Indonesia, Japan, the Philippines, and Vietnam" (2018), [http://www.asiacloudcomputing.org/images/acca2018\\_cddf\\_casestudies%201.pdf](http://www.asiacloudcomputing.org/images/acca2018_cddf_casestudies%201.pdf), 28 and 57.

54 Center for International Governance Innovation, "Tracing the Economic Impact of Regulations on the Free Flow of Data and Data Localisation" (2016), cited in Access Partnership, "Delivering the Fourth Industrial Revolution: The Role of Impact" (July 11, 2017), [https://www.accesspartnership.com/cms/access-content/uploads/2017/07/FINAL\\_Cloud4IR1.pdf](https://www.accesspartnership.com/cms/access-content/uploads/2017/07/FINAL_Cloud4IR1.pdf), 9.

55 Leviathan Security Group, "Quantifying the Cost of Forced Localisation" (2015), <https://static1.squarespace.com/static/556340e4b0869396f21099/t/559dad76e4b0899d97726a8b/1436396918881/Quantifying+the+Cost+of+Forced+Localization.pdf>, 3.

## Roadmap overview

Any country seeking to advance towards a mature national-level data protection and privacy regime will need to engage in three distinct processes that often overlap, and could be revisited in light of technological change and evolving best practices. These processes feed into determining where a country stands on a generic privacy roadmap, and will inform which next steps may be most appropriate.

### 1 Landscape analysis

The first step is to understand *where a country currently stands* in terms of data protection and privacy. This can be done by considering the various elements of a mature data protection and privacy framework, and then checking to see which elements a country may already have in place and which ones they still may need. The checklist below can be used to review these key elements and determine which approximate stage a country is at: nascent, progressing, or advanced.

The checklist is drawn from common principles and best practices in both Asian and global privacy frameworks. Checklist questions for government policymakers to consider are the following:

- ✓ Has the government developed a national privacy or data protection strategy?
- ✓ Has the government consulted with public and private stakeholders at the national level through discussions or workshop?
- ✓ Has the government engaged with other privacy policymakers in other countries through bilateral or multilateral channels?
- ✓ Has the government developed laws on privacy or data protection?
- ✓ What is the dynamic between any relevant sector specific laws and data privacy laws?
- ✓ Has the government enabled a self-regulation mechanism?
- ✓ Has the government developed mechanisms for cross-border data flow?
- ✓ Has the government introduced any implementation guidelines?
- ✓ Has an independent enforcement authority been appointed?
- ✓ Is there a coordination strategy between government agencies?
- ✓ Are government staff being trained on privacy principles?
- ✓ Is there a public education and awareness campaign?

Based on the answers to these questions, a country can see which elements already exist in its data protection and privacy framework, and which are yet to be tackled. Based on the experiences of countries in Asia (see the case studies later in this section as examples), certain elements are usually associated with various stages of progress towards a mature data protection and privacy regime (see Table 3).

Table 3

## Elements of a data protection and privacy regime

	Nascent	Progressing	Advanced
<b>National strategy</b> Goal setting and a coordinated approach across government agencies, initiatives, and compatibility with related policies.	✓	✓	✓
<b>Public-private consultation</b> Formal and informal dialogues among stakeholders in and outside of government, including private sector and civil society.	✓	✓	✓
<b>Multilateral and bilateral engagement</b> Formal and informal dialogues and coordination with other governments.	✓	✓	✓
<b>Data protection law(s)</b> Development and application of legislation, regulation, and jurisprudence.	—	✓	✓
<b>Self-regulation</b> Voluntary rules, guidelines, and compliance measures.	—	—	✓
<b>Guidelines or rules on cross-border data flows</b> Voluntary and mandatory rules governing the transfer of data across national borders.	—	✓	✓
<b>Implementation guidelines</b> Official guidance for how privacy laws will take effect (such as timelines, clarifications on definitions, and regulatory interpretations).	—	✓	✓
<b>Enforcement authority</b> An independent and neutral government agent tasked with ensuring adherence of the law.	—	—	✓
<b>Coordination mechanisms for government agencies</b> Establishment of processes or new lines of communication among government agencies and staff.	—	—	✓
<b>Training</b> Building administrative capacity and technical knowledge within government.	—	✓	✓
<b>Public education</b> Campaigns to inform the public about privacy risks, rules, and compliance.	—	✓	✓

## 2 Planning and goal setting

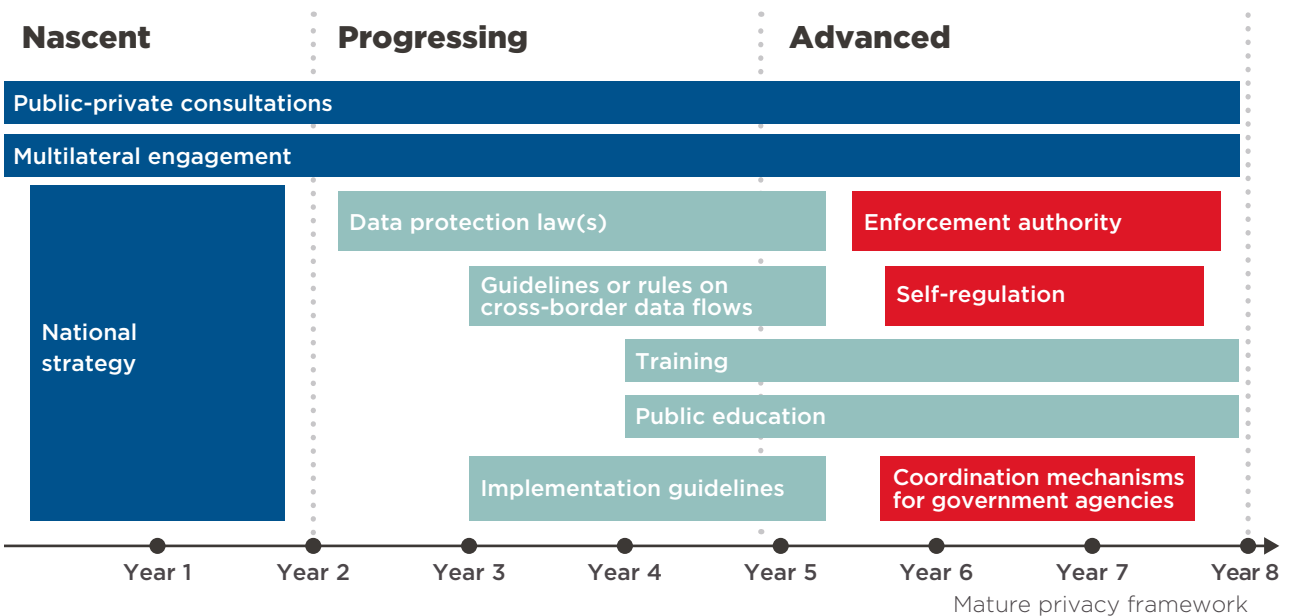
The second process focuses on *where a country wants to go*. Like the landscaping process, this will be somewhat different for each country. Yet the progression of steps from a nascent to mature privacy regime often follows a path that can be understood based on priority-setting, regulatory norms, and common sense.

Some elements are usually tackled first, while others come later, and still others (such as consultations)

usually remain ongoing. For example, it would be difficult for a country to develop a privacy training program for government employees without first enacting its laws on data protection. Similarly, the legal establishment of an enforcement authority is usually embedded in a country's privacy law, so countries generally enact their privacy law before an enforcement authority is created. A general timeline to implement elements of a privacy regime can be considered as follows in Figure 4.<sup>56</sup>

Figure 4

### Roadmap of privacy elements – possible stages and timeframes



## 3 Execution

The third and final process for a country to advance its privacy regime at the national level is to *execute across one or more elements of a privacy regime*, appropriate to where they stand on the roadmap. While there is no single path, key principles – drawn from global

and multilateral regional privacy frameworks – can be extremely helpful for governments to consider when determining which elements to address and how best to address them. The following sub-section will explore these principles and their application in further depth.

<sup>56</sup> The 8-year timeline is based off a review of past experiences of some countries who have developed mature privacy regimes in Asia. Actual timeframe may vary significantly between countries.



## How to apply key principles at the nascent stage

Several privacy frameworks indicate the importance of developing strategy, conducting consultations and holding multilateral cooperative arrangements.

### National strategy

Developing a national strategy to implement a data privacy framework is vital to ensure a coordinated approach and obtain high-level political buy-in to improve data protection. The OECD Guidelines indicated that a national strategy should include guidance on how different government agencies in the country will coordinate for effective implementation of any data protection and privacy framework.

### Public-private consultation

The APEC Privacy Framework recommends that member economies conduct consultation with public and private sectors, as well as civil society. Such consultations can help in developing support networks to ensure data protection and privacy compliance and enable sharing of information that might contribute to the development of a data protection and privacy framework.

### Multilateral and bilateral engagement

Multilateral and bilateral engagement is key for Asian data protection and privacy authorities to share knowledge, perspective, best practices, and for authorities to consider how to improve and harmonise data protection and privacy frameworks in the region.

Both the APEC and ASEAN privacy frameworks encourage countries to develop cooperative arrangements, whether bilateral or multilateral, to facilitate cross-border data flows and enforcement of privacy laws, and support consultation with other countries as a way to resolve any potential disputes. Early engagement with counterparts from other countries can therefore help build trust and confidence in one another's privacy frameworks. This includes both formal and informal consultations.

Some examples include:

- International Conference of Data Protection and Privacy Commissioners (ICDPPC) that connects 119 authorities from around the world for regulator-to-regulator discussion and cooperation around privacy;<sup>57</sup>
- Asian Business Law Institute that launched a multi-stakeholder Data Privacy Project in 2017 that focuses on creating a convergence in regulations that cover cross-border data flows;<sup>58</sup>
- Global Privacy Enforcement Network where privacy authorities can exchange experiences and discuss the practical aspects of enforcement cooperation;<sup>59</sup>
- Asia Pacific Privacy Authorities forum that also allows privacy authorities to form partnerships, share best practices and discuss new technology and changes to privacy regulation;<sup>60</sup>
- APEC Data Privacy Subgroup under the Electronic Commerce Steering Group, which is responsible for APEC's data privacy activities; and
- Cooperation between CPEAs under the APEC Privacy Framework.

57 International Conference of Data Protection and Privacy Commissioners, <https://icdppc.org/>, accessed on 28 May 2018.

58 Asian Business Law Institute, "Data Privacy Project," <http://abli.asia/PROJECTS/Data-Privacy-Project>, accessed on 28 May 2018.

59 Global Privacy Enforcement Network, <https://privacyenforcement.net/>, accessed on 28 May 2018.

60 Asia Pacific Privacy Authorities Forum, <http://www.appaforum.org/>, accessed on 28 May 2018.

## How to apply key principles at the progressing stage

As countries move into the progressing and advanced stages, key principles become even more important as they determine how rules and regulations will be drafted and influence how the data protection law will be operationalised. Below are some of the key issues governments should consider when operationalising privacy principles into regulatory requirements and implementation, as these are critical steps towards effectively leveraging regional privacy frameworks to a country’s advantage.

Several of these principles comport with the principles highlighted in the GSMA’s report entitled “Safety, privacy and security across the mobile ecosystem.” In particular, governments should ensure legislation

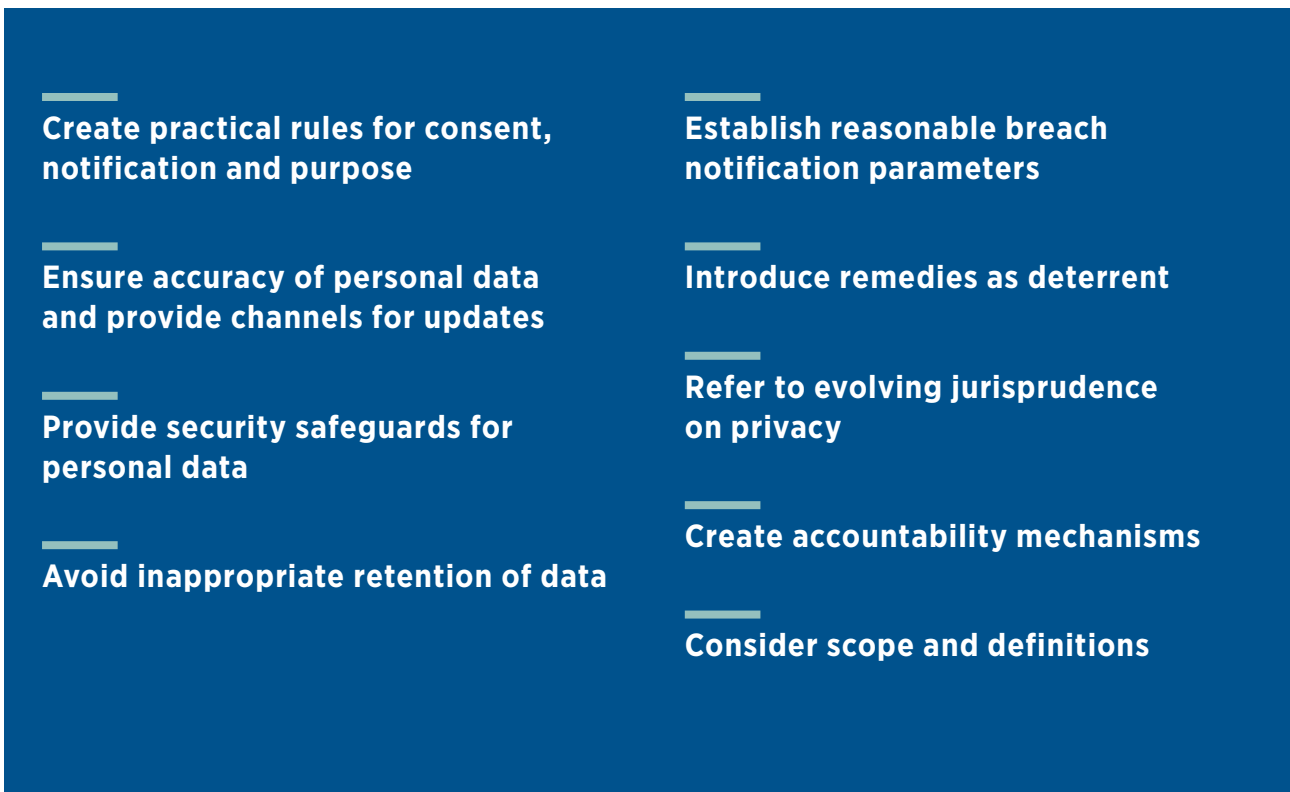
is service and technology-neutral, so that rules are applied consistently to all entities that collect, process and store personal data, and that legislation should focus on the overall risk to an individual’s privacy, rather than attempting to legislate for specific types of data.<sup>61</sup>

### Data protection laws

Various principles must be applied towards crafting practical and effective data protection laws. A non-exhaustive list of examples of how such principles can be operationalised is described in Figure 5.

Figure 5

## Examples of how data privacy principles can be operationalised



61 GSMA “Safety, privacy and security across the mobile ecosystem” [https://www.gsma.com/publicpolicy/wp-content/uploads/2017/02/GSMA\\_Safety-privacy-and-security-across-the-mobile-ecosystem.pdf](https://www.gsma.com/publicpolicy/wp-content/uploads/2017/02/GSMA_Safety-privacy-and-security-across-the-mobile-ecosystem.pdf).

**i Create practical rules for consent, notification and purpose**

The provisions for consent, notification and purpose are critical to all data protection and privacy law and can be implemented in various ways. Regulators should consider the pros and cons of each approach. Some of the questions to consider are laid out in Figure 6.

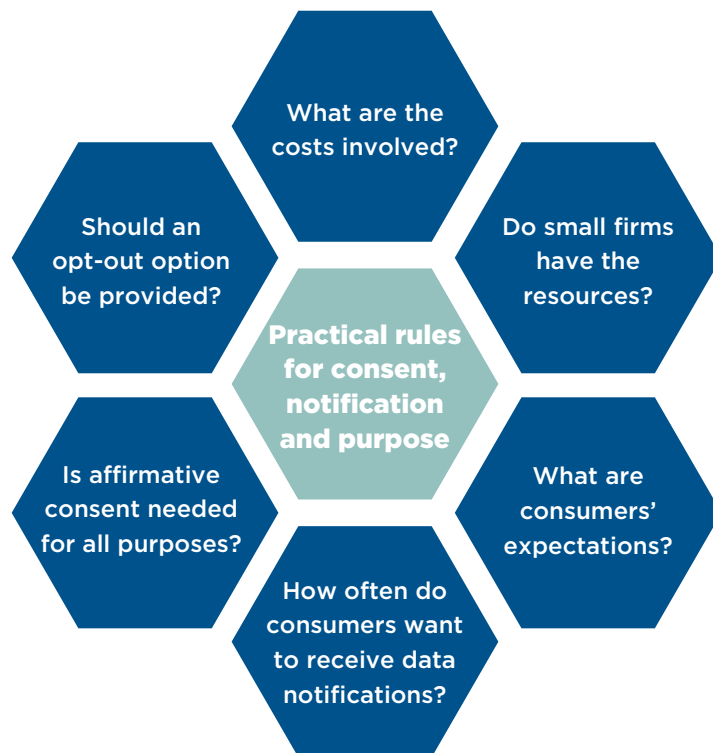
As a first step, regulators should determine which instances require consent and determine the best approach for organisations to obtain consent.<sup>62</sup> One option entails requiring organisations to display terms and conditions when the data subject signs up for their products or services, but this method raises the question of whether it is reasonable to expect consumers to read through the terms and conditions fully. Another option is to explicitly obtain consent for each purpose of data collection; the downside of this approach is potential notification fatigue and seeking

consent for each use may stifle innovation. Other approaches might be to allow passive consent for personal data that is required for contract performance or to fulfil legal requirements while requiring notification and explicit consent for sensitive data, such as ethnicity, political opinions, religious beliefs, trade union activities, or medical information. There is also debate about whether exemptions should be provided for companies below a certain size due to their lack of resources and the potentially lower impact of a breach.

These are all questions that regulators will have to discuss with companies, civil society, and individual members of the public to find an approach that works best for the country. Once these parameters are established within the law, regulators may consider implementation guidelines that provide examples of how consent can be obtained to provide a smoother compliance process for businesses.

**Figure 6**

Questions to consider in creating practical rules for consent, notification and purpose



62 Consent is not necessary in all cases, and other grounds for processing are available. Typical grounds include concepts such as legitimate interests.

## ii Ensure accuracy of personal data and provide channels for update

Maintaining accurate data is important, especially in situations where the information is used for a purpose that requires it to be updated. This includes payroll records, addresses to ensure the right delivery, and records of events, such as opening or closing of accounts, that would be important in dispute settlement. Authorities could provide guidelines on how organisations can take reasonable steps to ensure the accuracy of personal data, such as by sending requests for data subjects to update records or ensure that the source of any personal data is clear. Channels should also be created for data subjects to request access to their data and to update the information when needed.

## iii Provide security safeguards for personal data

Personal data should be accorded with the necessary protection against loss, destruction or damage. Data should be used only for its original purpose and security measures such as pseudonymisation<sup>63</sup> and encryption should be implemented. Regulators could consider setting a baseline of standards, such as design of security systems, clear designation of roles of people in charge of information security, policies that will need to be in place, as well as a response plan for any breach. Several other considerations include whether authorities will impose the same requirements for all companies or whether more stringent requirements will be imposed on only critical information infrastructure.



**“The two most pressing privacy concerns are access to information for investigations and the illegal use of personal information.”**

Anonymous quote from the GSMA's survey of regulators across APEC and ASEAN that was conducted to inform this report.

Security safeguards that protect user information also overlap and sometimes conflict with law enforcement requirements regarding data access for investigations.<sup>64</sup> Governments can determine various levels of legal due process so as to balance the security of personal data and the need to access it under particular circumstances.

Safeguards around personal data can be informed by consultation with stakeholders. For example, Vietnam's Ministry of Information and Communications has held consultations with ICT companies to understand their experiences in managing privacy requirements, including issues such as an encryption, data access control (based on type of data), and the terms and conditions around personal information used in digital transactions.

## iv Avoid inappropriate retention of data

With privacy in mind (rather than law enforcement), documents containing personal data should not be retained by organisations, or organisations should remove the ability to link personal data with particular individuals, as soon as it is no longer necessary for legal or commercial purposes. Authorities may want to consider best practices in terms of the length of

time to retain the personal data, setting guidelines for secure deletion or anonymisation of data that is no longer needed or to update the information when it is outdated. It will be important to reconcile these standardisations with law enforcement requirements for access to records and data. The two should not conflict.

Scenarios that may require further deliberation are whether some sectoral laws or industry practices require certain data to be retained (e.g. financial records may be required for legal reasons), and whether the data will be used in the near future or in the long term (e.g. CCTV data and resumes can likely be deleted sooner than later). Authorities may also consider setting rules that distinguish between permanent deletion and archiving of data. While offline archival may reduce the risk of misuse or mistake, organisations must have the capability to provide data subjects access to the data and maintain it in a way that complies with data protection rules.

## v Establish reasonable breach notification parameters

Breaches may happen quite frequently, but the degree of the breach may vary. Regulators will have to consider if all breaches should be reported to

<sup>63</sup> Pseudonymisation is a procedure for replacing personally identifiable information with one or more artificial identifiers or pseudonyms.

<sup>64</sup> GSMA's report on "Safety, privacy and security across the mobile ecosystem" acknowledges industry's legal and moral obligation to support public safety and to respect the legitimate mandates of governments following due process, as well as its legal and moral obligation to respect human rights. This is a complex area with differences between national jurisdictions, hence, the GSMA focuses on establishing common principles and educating all parties on best practices.



both authorities and consumers, or if only breaches that reach a certain level of threshold or involve a certain type of data will need to be notified. Notifying consumers for all breach occurrences will not only take a toll on the company's resources, it may also trigger unnecessary panic among consumers. If the data that is breached is encrypted and anonymised, it is unlikely that it will be able to be traced to an individual. But if the data involved are confidential information such as identifying numbers or bank account numbers, then that will have a greater significance to both data subjects and the authorities.

In the EU, under Art. 33 GDPR, the notice to the regulator is required "unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons." Breaches must be notified to individuals under Art.34 GDPR if the breach is "likely to result in a high risk to the rights and freedoms of natural persons." Determination of harm or potential harm should be a consideration during and after any privacy incident, and mitigating these harms should be paramount, and may require notification of consumers or authorities. Incidents where no risk or harm to individuals have occurred may not warrant notification. Conducting a "triage" of the incident can help companies determine which breaches pose risks to individuals.

In Singapore's recent consultation on mandatory breach notification, the Singapore Personal Data Protection Commission (PDPC) response note to the public consultation clarified that the criterion for breach notification to affected individuals and PDPC is based on an assessment of the breach that is "likely to result in significant harm or impact to the individuals whom the information relates."

#### **vi Introduce remedies as deterrent**

There is a wide range of remedies that can be introduced into data protection and privacy laws, but countries will have to consider remedies that are proportionate to the breach. Remedies will have to be stringent enough to motivate compliance, but they should also not be so difficult that companies avoid doing business in that country, to the detriment of the country's economy. Remedies can be monetary, restitution, rescission, or a specific performance. For example, Section 1 of this report outlined that the EU's GDPR sets criteria to determine the monetary fine of up to €20 million, or 4 per cent of the worldwide annual revenue of the prior financial year, whichever is higher. Meanwhile, beyond the option of imposing

a monetary fine not exceeding S\$1 million, PDPC may issue a direction for the deletion of data collected in contravention of the PDPA in a case that it investigates.

#### **vii Refer to evolving jurisprudence on privacy**

Data protection and privacy laws will evolve as jurisprudence responds to changes in technology and applications. Courts will make determinations that either support or undermine aspects of data protection and privacy law, or simply provide deeper direction and interpretation. Jurisprudence on certain issues will also differ across jurisdictions. For example, various jurisdictions maintain differing perspectives as to whether IP addresses constitute personal data. In Hong Kong, the privacy commissioner responded to a complaint on IP addresses by stating that "an IP address per se does not meet the definition of 'personal data'" as it is linked to a computer, not an individual.<sup>65</sup> In the EU, the GDPR's definition of personal data includes "online identifiers," which, according to Recital 30, includes IP addresses.<sup>66</sup> Even past opinions in the EU that dynamic IP addresses can constitute personal data, such as the October 2016 ruling by the Court of Justice of the European Union, support the treatment of IP addresses as personal data.

#### **viii Create accountability mechanisms**

Being accountable means organisations should comply with the data protection and privacy rules and laws in each market, and be able to demonstrate to internal and external stakeholders how to effectively manage the data, including how the data flows to vendors or service providers. As touched on in previous sections, there are several accountability mechanisms that are adopted by countries. Some countries, such as Malaysia, the Philippines and Singapore, appoint a data protection authority to regulate companies and impose penalties for any non-compliance or withholding of information. For Japan, in addition to having a data protection authority, the government appointed a third-party Accountability Agent under the APEC CBPR system. Under CBPR, companies and organisations are not mandated by law to participate, but they may voluntarily choose to certify their companies to facilitate the privacy compliance process.

Both approaches have their own merits. Appointing a government agency to conduct enforcement may reduce any risk of bias, but it requires dedicated resources on the part of the government. Outsourcing an accountability mechanism to a third-party organisation may reduce the burden on government

65 Out-law, "Hong Kong clears Yahoo! of privacy breach over jailed journalist," <https://www.out-law.com/page-7880>, accessed on 28 May 2018.

66 Privazy Plan, "Recital 30 EU GDPR," <http://www.privacy-regulation.eu/en/recital-30-GDPR.htm>, accessed on 28 May 2018.

resources, but it will still require some supervision to ensure high standards are maintained and to prevent anti-competitive measures.

## ix Consider scope and definitions

Besides the principles of the data protection and privacy framework, regulators will also need to consider definitions that will determine the extent to which the principles are applied. Different national and regional frameworks may apply differently based on the definitions used. A non-exhaustive list of examples of such differences include the following:<sup>67</sup>

- **Definition of personal data.** The definition of personal data refers to information that is personally identifying, such as name and identity number. As mentioned in earlier parts of the report, there are debates among regulators if data such as IP addresses or cookies should also be considered as personal data. Additionally, some privacy frameworks classify data into different categories, such as sensitive data.
- **Enforcement powers of data protection authorities.** Some data protection authorities have the authority to impose fines and other penalties, while others may not.
- **Data controller vs processor.** Data controller refers to organisations that determine the purpose of data collection and how personal data will be processed, while a data processor simply processes the data on behalf of controllers. Some regulators only impose obligations on data controllers while others may impose obligations on both.

## Guidelines or rules on cross-border data flows

Cross-border data flows are vital, and one of the most important examples revolves around the transfer of personal data. In today's digital economy where the supply chain is global, the transfer of personal data between organisations or within the same organisation across countries is inevitable. Some scenarios may include a company headquarters that requires access to the personal information of its staff in other countries or a company that has procured services from a vendor and needs to transfer the personal data for work to be conducted. Recognising that privacy can be protected

across borders through accountability and other mechanisms can prevent countries from attempting to use data protection and privacy as an excuse to introduce protectionist data localisation measures.

There are different approaches to cross-border data transfers between countries and regions that have been extensively detailed in sections 1 and 2 through various cross-border data protection and privacy frameworks, such as those in ASEAN and APEC. Additionally, ASEAN and APEC governments continue to work to ensure their laws are comprehensive and consistent with international standards on cross-border data transfers, including Asian frameworks and the EU's GDPR. The GSMA's "Safety, Privacy and Security Across the Mobile Ecosystem" report identified the need for cross-border data transfer rules to be risk-based and support measures to ensure adequate data protection while helping realise potential social and economic benefits.<sup>68</sup>

## Implementation guidelines

How governments implement data protection laws and cross-border data transfer rules are an important element of any data protection and privacy regime. Implementation guidelines can address various aspects, including timeframes for particular provisions to take effect, clarifications on definitions, and published case studies to highlight regulatory interpretations of the law. These can be very helpful in providing further context and clarifications of the legal framework and reduce uncertainty for entities, such as businesses, that may be subject to the law.

## Training

As noted previously, one of the biggest challenges faced by some countries in Asia is the lack of administrative capacity. This includes lack of resources, technical privacy knowledge, and coordination among government agencies. This can be addressed by establishing a clear definition of the roles of different government agencies and by according power to agencies to enforce those roles. Trainings and manuals can be provided to staff to equip them with sufficient knowledge and know-how on the privacy framework so they can follow-up when faced with a problem.

<sup>67</sup> Along with the example provided, there are additional principles and definitions to consider, such as those laid out in the EU GDPR. This report does not outline the GDPR in detail, as the framework's rights-based and supranational approach may not apply well across the Southeast Asian region with its diverse culture, political systems and maturity level of privacy discussions.

<sup>68</sup> GSMA "Safety, privacy and security across the mobile ecosystem" [https://www.gsma.com/publicpolicy/wp-content/uploads/2017/02/GSMA\\_Safety-privacy-and-security-across-the-mobile-ecosystem.pdf](https://www.gsma.com/publicpolicy/wp-content/uploads/2017/02/GSMA_Safety-privacy-and-security-across-the-mobile-ecosystem.pdf).

## Public education

As mentioned in the earlier portion of this report, engaging with both consumers and the private sector is important to understand what is practical and what can be implemented, as well as to learn about their concerns and expectations. Moreover, when stakeholders are aware of their rights and the law, it creates a collaborative enforcement mechanism that improves the effectiveness of the law. Regulators can also engage civil society to educate both the public and private sectors to enhance compliance.

Several privacy regulators in Asia have said the lack of awareness of the use of personal data among individuals is pronounced, especially individuals' lack of understanding and control over how their data is collected and used and the corresponding risks. Governments also describe gaps between awareness and implementation of rules (see Singapore case study box). Some ASEAN governments, like the Philippines, Vietnam, and Singapore, have advanced campaigns to increase awareness and improve the enforcement environment, as do APEC governments like Hong Kong and Japan.

## Singapore case study on data protection awareness

While awareness of the data protection obligations of the Personal Data Protection Act (PDPA) is high, the appointment of data protection officers (DPOs) by organisations, which is mandatory under the law, remains modest. The findings of PDPC's 2017 annual industry survey, conducted among some 1,500 organisations of various industry sectors and sizes, showed that the awareness had gone up from 77.9 per cent in 2016 to 92 per cent in 2017, but only about half had appointed a DPO. As a champion of personal data protection within an organisation, the DPO plays an important role in taking the lead on putting in place internal policies, designing processes and instilling the right data protection culture. The PDPC will continue to emphasise the importance of

implementing the legal requirement to appoint a DPO, as well as developing programmes and schemes to support and elevate the DPO in his or her role. A common misconception among businesses is that the PDPA is an obstacle to the use and sharing of personal data. However, the PDPA is not intended to prohibit or impede the pace of emerging trends and technologies, but to promote responsible use and sharing of data, so that data innovation can thrive. Consumers want to know that their personal data is in the good hands of organisations, and only with that trust and assurance will consumers share their data knowingly and willingly. The ultimate goal of PDPC's initiatives and enhancements is to establish a high level of consumer trust as the bedrock for Singapore's digital economy.

## How to apply key principles at the advanced stage

### Establish an enforcement authority

Appointing an independent and neutral enforcement agent is key to ensuring compliance. Within the enforcement agency or agencies there must first be internal buy-in, then officers must be trained in the subject of data protection and privacy, and eventually some resources will have to be solely dedicated to overseeing the local privacy rules. Although some countries appoint a single entity as an enforcement authority, the enforcement burden can be split among several entities. For instance, Japan used to suffer from multiple agencies with overlapping remits enforcing the

data protection and privacy law – which complicated supervision and regulatory action – before establishing a single authority. They slowly revised the Personal Information Protection Act to accord the new Personal Information Protection Commission (PPC) with greater authority, including audit and inspection powers, and the power to request that companies submit compliance reports. This could be an approach that countries take to enable agency staff to gain expertise.



## Encourage industry self-regulation

Self-regulation in certain areas may be a good approach to ensuring data protection due to several reasons:

- It brings in the expertise of the private sector;
- Private sector players are motivated to find a framework that works to prevent heavy handed laws;
- It reduces strain on government resources; and
- It is easier to change self-regulatory codes than national laws.

One example is Australia’s blend of laws and codes of conduct. While the Australian Information Commissioner implements a broad Privacy Act, there are complementary self-regulatory codes managed by the private sector. For instance, the Australian Association of National Advertisers (AANA) established a self-regulation mechanism in 1998 after consultations with industry, consumer and government representatives. Among its recent codes

includes a “Marketing in Digital Space” code that covers guidelines on data protection and privacy. The code touches on data collection, the use of location-based services for marketing and principles to give consumers transparency, choice and control over their online advertising preference.

## Coordination mechanism for government authorities

Given the complexity of privacy issues and regimes, governments require mechanisms that designate and assign responsibilities among agencies for certain aspects of implementation, monitoring, and enforcement of privacy rules and guidelines. These are often linked to a country’s national strategy, and usually require changes in government processes or the establishment of new lines of communication. Such coordinative mechanisms are especially important in fulfilling the aforementioned implementation guidelines.





## Case studies

Some case study examples of countries at various stages of the process can help inform Asian governments of what these various stages look like and may assist countries in understanding how to consider their own status and possible paths forward. The following cases include Japan (advanced), the Philippines (progressing), and Papua New Guinea (nascent).

### Case study Japan

 **ADVANCED**

- ✓ Extensive consultation with private sector before implementation
- ✓ Participates in bilateral and multilateral privacy arrangements
- ✓ Strategy laid out before drafting changes in privacy act
- ✓ Privacy rules have adapted to evolving technologies
- ✓ Clear rules on cross-border data flows
- ✓ Ample time given before change in law comes into effect
- ✓ Multiple privacy authorities streamlined into single Personal Information Protection Commission
- ✓ Public education and legislative changes were conducted in parallel

Japan represents one of Asia's most mature economies when it comes to its privacy framework. Japan's privacy journey presents a useful example for how to change laws and guidelines in ways that evolve with new technologies and provide the private sector ample time to adapt before more stringent measures are implemented.

The Act of the Protection of Personal Information (APPI)<sup>69</sup> was first passed in 2003 and came into effect in 2005.<sup>70</sup> The APPI was initially managed by various ministries that oversee specific sectors. Over the next 10 years, with the drastic changes in technology and the digital environment, the authorities decided that it was due for amendment. New challenges included the use of data for analytics, cloud and cross-border services. The multiple authority approach was also cumbersome and needed to be addressed.

Before amending the APPI, the government published the Policy Outline of the Institutional Revision for Use of Personal Data in 2014<sup>71</sup> to show the government's direction on which measures are to be taken to amend

the APPI and other personal information protection-related laws. In the same period, Japan also joined the APEC CBPR system<sup>72</sup> to enhance the ability of Japanese companies to adhere to privacy regimes among APEC member economies through a self-regulatory trust mark system.

The act was eventually amended in 2016.<sup>73</sup> One of the key changes was the differentiation between "sensitive data" and "anonymised data." The latter category enabled data to be used to support innovation in new industries such as big data, analytics and machine learning as long as it cannot be used to identify a specific person. Another change was the inclusion of an "opt-out" option for data subjects who do not want their personal data to be transferred to a third party. While Japan's Personal Information Protection Commission does not prescribe the opt-out method, it requires companies to notify data subjects before any joint use of the information with third-parties and to disclose to data subjects how they can submit an opt-out request to the company.

69 Personal Information Protection Commission, "Law on protection of personal information, Law No. 57 of May 30" (2003), [https://www.ppc.go.jp/files/pdf/290530\\_personal\\_law.pdf](https://www.ppc.go.jp/files/pdf/290530_personal_law.pdf).

70 Personal Information Protection Commission, "Outline of the amended Personal Information Protection Act" (February 2016), [https://www.ppc.go.jp/files/pdf/280222\\_outline\\_v2.pdf](https://www.ppc.go.jp/files/pdf/280222_outline_v2.pdf).

71 Personal Information Protection Commission, "Policy Outline of the Institutional Revision for Utilisation of Personal Data" (24 June 2014), [https://japan.kantei.go.jp/policy/it/20140715\\_2.pdf](https://japan.kantei.go.jp/policy/it/20140715_2.pdf).

72 APEC, "APEC expands data privacy system to protect consumers" (1 May 2014), [https://www.apec.org/Press/News-Releases/2014/0501\\_CBPR.aspx](https://www.apec.org/Press/News-Releases/2014/0501_CBPR.aspx).

73 Personal Information Protection Commission, "Amended Act on the Protection of Personal Information" (December 2016), [https://www.ppc.go.jp/files/pdf/Act\\_on\\_the\\_Protection\\_of\\_Personal\\_Information.pdf](https://www.ppc.go.jp/files/pdf/Act_on_the_Protection_of_Personal_Information.pdf); law took effect on 30 May 2017.

As the digital economy became more globalised, the act was also amended to introduce rules on the transfer of personal data across borders. To facilitate the use of overseas services, the government requires organisations to obtain affirmative consent before providing personal data to a third party located overseas. The law also provided a channel for the Japanese authority to provide information to an equivalent privacy authority in certain foreign jurisdictions to allow it to enforce this mandate.

With the revised Act, a single data protection authority was also appointed. This was a significant change as the past arrangement resulted in overlapping and conflicting rules that arose as a result of privacy protection guidelines that were developed in silos. The Personal Information Protection Commission (PPC), established in 2016, became the central enforcement agency across all sectors, except the financial sector. The PPC is given the powers

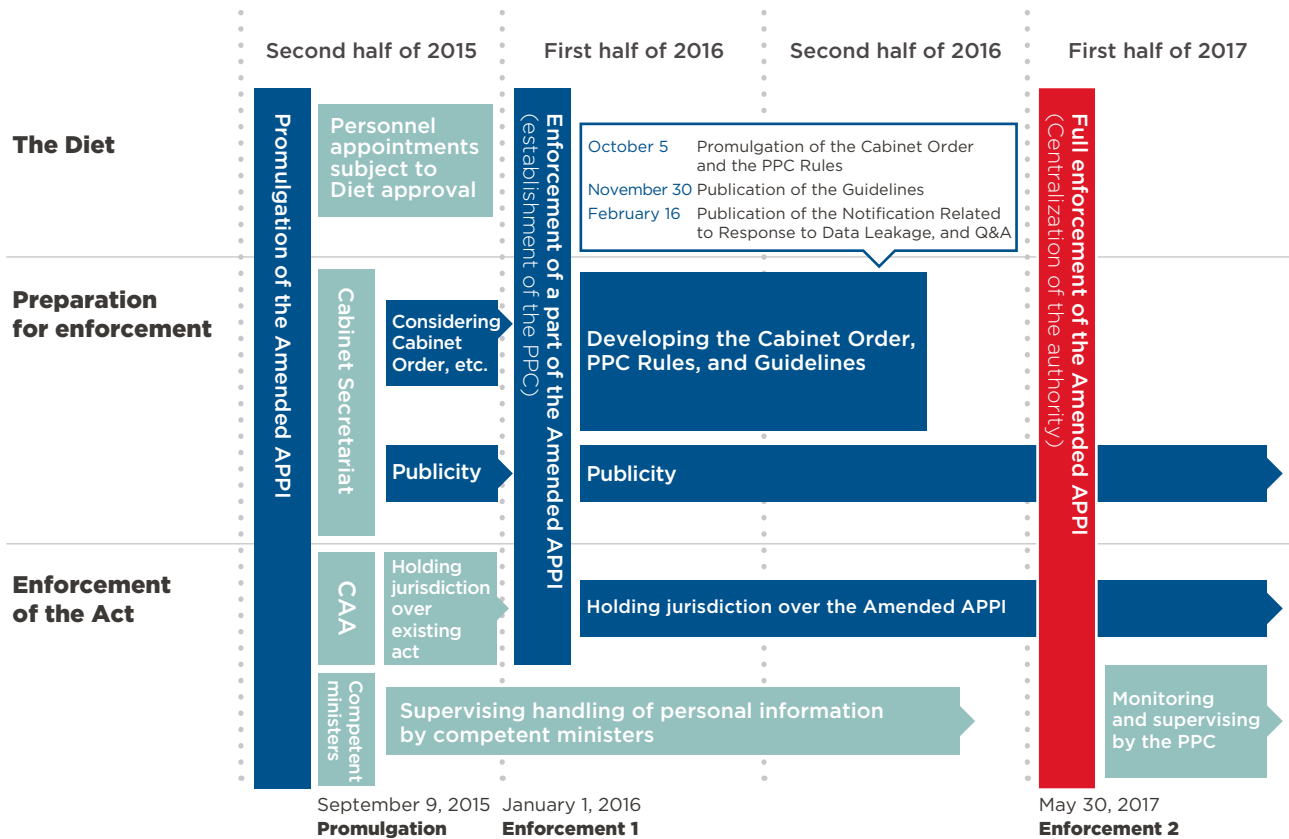
to enforce APPI and streamline existing privacy guidelines. In 2016, Japan also appointed JIPDEC as the first certification body under the APEC CBPR system for Japan. Besides providing a trust mark system, JIPDEC is also required to handle complaints and share information with the PPC.

With emerging trends and technologies, the Japanese government also made sure that they allocated sufficient budget for human resources. The PPC has 130 staff dedicated to enforcing the APPI, which includes lawyers, accountants, and IT experts.<sup>74</sup>

After the act was amended in 2015, the PPC held 16 public consultations on the order of enforcement of the act and nearly 3,000 comments were received.<sup>75</sup> The consultation process provided an avenue for organisations to clarify the requirements of the APPI before the act came into effect in 2017.

Figure 7

### Japanese authorities' timeline that reflects legal changes and publicity being conducted in parallel



Source: Presentation by Kuniko Ogawa, Counselor, Personal Information Protection Commission<sup>76</sup>

74 The GSMA's Interview with the Japan Personal Information Protection Commission.

75 Information Policy Centre, "The Amended Act on the Protection of Personal Information (APPI)" (11 May 2017), <https://goo.gl/CMY5bd>. 7.

76 Ibid, 17.



The PPC is also active in engaging with governments through bilateral (with the US, Singapore, European countries, etc.) and multilateral channels (Global Privacy Enforcement Network and Asia Pacific Privacy Authorities Forum) to learn the best practices and continue dialogues on privacy.<sup>77</sup>

## Case study Philippines

### ● PROGRESSING

- ✓ Data Privacy Act introduced in 2012 and covers cross-border data flow rules
- ✓ Actively engages with civil society, private and public sectors on privacy issues
- ✓ Interacts with other data protection authorities
- ✗ National privacy strategy is not yet developed
- ✗ Not yet introduced a self-regulation mechanism, although it has expressed interest to join the APEC CBPR
- ✓ Enforcement of Data Privacy Act is managed by National Privacy Commission
- ✓ Organises awareness drives and national campaigns on privacy issues for stakeholders, as well as capacity building trainings

Several ASEAN member states, including the Philippines, have ramped up data protection efforts over the past few years. The Philippines is one of the countries that fall under the “progressing” stage as it has fulfilled most requirements towards achieving a mature privacy framework.

While the country has not developed a national privacy strategy, the Philippines introduced in 2012 its Data Privacy Act, and its enforcement authority, the National Privacy Commission, was established four years later. The Philippine’s Data Privacy Act is a comprehensive law, consistent with international frameworks discussed in Section 1. The Data Privacy Act itself does not prohibit data transfer; data controllers can use contractual or other reasonable means to provide a comparable level of protection while the information is being processed by a third party overseas.

As Business Process Outsourcing (BPO) is a major industry for the Philippines, enabling cross-border data flows is key. Supporting the BPO and other data-heavy industries like healthcare may be one of the motivating factors for the government to have expressed interest in participating in the APEC CBPR system. With a self-regulatory mechanism like the CBPR, local businesses can become certified to show compliance with not just the Philippines Data Protection Law, but also other CBPR countries’ law – creating a channel for data to be transferred to support the BPO industry.<sup>78</sup> In December 2017, the Philippines joined APEC’s Cross-Border Privacy Enforcement Arrangement (CPEA), which is a necessary precursor to participation in CBPR.

The Philippines’ National Privacy Commission is active in engaging the public and private sector, as well as other government agencies. During the development of the implementation rule in 2016, the government opened the draft for consultation<sup>79</sup> and collaborated with a civil society organisation to hold public events to

engage the public.<sup>80</sup> Other efforts to raise awareness among stakeholders include a drive<sup>81</sup> organised for local governments in 2017 and a national awareness campaign in 2018.<sup>82</sup>

At the international level, the commission interacts and exchanges views with other privacy regulators through several channels. The Philippines was approved as a full member of the International Conference of Data Protection and Privacy Commissioners (ICDPPC) in 2016,<sup>83</sup> and also engages in bilateral collaborations. In 2017, the commission organised an APEC-CBPR Manila workshop with the U.S. Department of Commerce.<sup>84</sup>

The Philippines authorities have made good progress in enhancing its privacy framework and improving awareness among stakeholders. But there is still room to conduct more capacity building for enforcement officers to improve enforcement – an issue that has been identified as a challenge by the regulator – and to encourage industries to create self-regulatory codes of conduct for privacy. One example of a country that is in a similar stage as the Philippines and have done well in creating a co-regulatory model is Malaysia where the commission have approved codes of practice for the utilities,<sup>85</sup> insurance<sup>86</sup> and financial<sup>87</sup> sectors. While the Malaysian PDPA was formed in 2010, the codes of practices were only developed six to seven years after industries have a more mature understanding of data protection. The Philippines have taken similar steps with the Health Privacy Code but it may take several years for other industries to catch up.<sup>88</sup>

Lastly, the lack of private sector candidates that can help the authority with an accountability mechanism (e.g. trust mark certification) presents another challenge for the country. It will take time to cultivate a local privacy industry that can help the authority with compliance.

78 National Privacy Commission, “Data privacy compliance a competitive edge for PH companies” (31 July 2017), <https://privacy.gov.ph/data-privacy-compliance-competitive-edge-ph-companies/>; the authority and the Contact Center Association of the Philippines discussed how data privacy can help local companies be more competitive.

79 National Privacy Commission, “Invitation to Comment: Proposed Implementing Rules and Regulations of The Data Privacy Act” (19 July 2016), <https://privacy.gov.ph/invitation-to-comment/>.

80 National Privacy Commission, “Privacy Act IRR released – NPC to educate public about privacy” (30 August 2016), <https://privacy.gov.ph/privacy-act-irr-released-npc-to-educate-public-about-privacy/>.

81 National Privacy Commission, “NPC launches PH-wide data protection drive for LGUs in Region 11” (10 May 2018), <https://privacy.gov.ph/npc-launches-ph-wide-data-protection-drive-lgus-region-11/>.

82 National Privacy Commission, “Celebrate Filipino Data Privacy Rights on Privacy Awareness Week 2018 – NPC” (10 May 2018), <https://privacy.gov.ph/celebrate-filipino-data-privacy-rights-on-privacy-awareness-week-2018-npc/>.

83 National Privacy Commission, “PH Privacy Commission gets international accreditation” (21 October 2016), <https://privacy.gov.ph/ph-privacy-commission-gets-international-accreditation/>.

84 Cross-Border Privacy Rules System, “Report from Manila, Philippines APEC CBPR Workshop” (5 – 6 December 2018), [https://cbprs.blob.core.windows.net/files/SME%20Access%20Report\\_FINAL%20April%202018.pdf](https://cbprs.blob.core.windows.net/files/SME%20Access%20Report_FINAL%20April%202018.pdf).

85 Personal Data Protection Office, “The Personal Data Protection Code of Practice for the Utilities Sector (Electricity)” (September 2015), <https://goo.gl/4ZiGri>.

86 Malaysian Takaful, “Code of Practice on Personal Data Protection for the Insurance and Takaful Industry in Malaysia” (December 2016), <https://goo.gl/Yj3jaN>.

87 Personal Data Protection Office, “Personal Data Protection Code of Practice for the Banking and Financial Sector” (January 2017), <https://goo.gl/beFGiY>.

88 Department of Health, “Health Privacy Code Implementing the Joint Administrative Order No. 2016-0002, Privacy Guidelines for the Implementation of the Philippine Health Information Exchange” (20 January 2016), <http://ehealth.doh.gov.ph/images/HealthPrivacyCode.pdf>.



## Case study Papua New Guinea

### ○ NASCENT

- ✗ Not yet engaged in significant public-private consultation on privacy issues
- ✗ Does not yet participate actively in privacy-related discussions with international organisations
- ✗ Not yet developed a privacy strategy for the country
- ✗ No specific bill on privacy or data protection, although some frameworks offer limited protection
- ✗ Self-regulation mechanism for privacy is not yet introduced
- ✗ No rules on cross-border data transfer of personal data
- ✗ No data protection authority
- ✗ There is opportunity for public education campaign on data protection and capacity building



The Constitution of the Independent State of Papua New Guinea outrightly expresses the right to privacy for its people.<sup>89</sup> Although Papua New Guinea does not have a dedicated privacy law, several other laws provide some limited data protection provisions such as its recent Cybercrime Code Act 2016<sup>90</sup> and the National Information and Communication Technology Act 2009.<sup>91</sup> Together, these Acts criminalise the unlawful disclosure of private, confidential and sensitive personal data, and prohibits any actions that intercepts, modifies or records any communications.

Like other countries in this stage, Papua New Guinea may start engaging the public and private sector first to get a sense of their understanding of data protection and develop practical ideas on enhancing data protection for its citizens. With the laws mentioned above providing baselines for privacy protection, the local authority could start deliberating further privacy principles it may want to introduce for its country. As a country with close ties with others in the region like Australia, it could start discussions with the Australian Information Commissioner on potential capacity building workshops or knowledge-sharing.

## Timeline for countries at different stages

The presented case studies provide an indication of a timeline for countries in different stages of the roadmap. Even for a country like Japan, the maturity of the privacy framework developed over a 10 year period. But it took about two years from when Japan indicated an intent to adjust its privacy framework and join the APEC CBPR system to create a data protection authority and enforcement mechanisms, and to appoint an Accountability Agent. A clear strategy at the onset made it easier for Japan to navigate the bureaucratic system.

For the Philippines, it has a relatively well-established data protection act that was implemented in 2012, but enforcement remains a key challenge as well as a lack of industry maturity in their understanding of privacy that makes it tougher to develop self-regulatory mechanisms or appoint an Accountability Agent to help with compliance. It may take the Philippines some time to nurture the local industry before it is mature

enough to develop codes of practice, but the country is moving quickly to up-level its capacity and prepare to join regional frameworks like CBPR.

Lastly, Papua New Guinea is an example of a country that is still new to privacy issues. There is opportunity to engage both local and international stakeholders to understand where the country stands in terms of privacy issues compared to international standards. At this stage, it would be useful to carve out a strategy that would help chart the milestones that it hopes to achieve in the long term.

Ultimately, there is no right or wrong way to develop a mature privacy framework. Each economy will have to decide on its own journey. The processes outlined in this report can support countries, especially those at the nascent stage, to consider their position, options, and path forward.

89 World Intellectual Property Organisation, "Constitution of the Independent State of Papua New Guinea," [http://www.wipo.int/wipolex/en/text.jsp?file\\_id=199188](http://www.wipo.int/wipolex/en/text.jsp?file_id=199188), accessed on 28 May 2018.

90 Papua New Guinea Parliament, "Cybercrime Code Act 2016" (13 December 2016), [http://www.parliament.gov.pg/uploads/acts/16A\\_35.pdf](http://www.parliament.gov.pg/uploads/acts/16A_35.pdf).

91 Pacific Islands Legal Information Institute, "National Information and Communications Technology Act 2009," [http://www.paclii.org/pg/legis/num\\_act/niacta2009489.rtf](http://www.paclii.org/pg/legis/num_act/niacta2009489.rtf), accessed on 28 May 2018.





---

# Regulator survey and roadmap solutions

---

No one is better placed to understand the challenges and opportunities in crafting better data governance regimes than regulators themselves. As indicated earlier, this report includes views based on a set of interviews with regulators in Hong Kong, Japan, Malaysia, the Philippines, Singapore and Vietnam that span varying levels of privacy maturity. This report has touched on some of the challenges they describe when advancing data privacy laws, and factors that helped propel countries forward. Key challenges cited include:

- How to effectively balance between privacy protections and ICT adoption that drives innovation;
- Costs, skills and time needed to advance privacy frameworks;
- Need to access information;
- Enforcement issues;
- How to implement accountability mechanisms; and
- Lack of understanding and awareness around privacy.

The summary of views below attempts to consolidate these further and offer guidance based on a proposed roadmap for how best to address these challenges and leverage new opportunities.

**Table 4**

## Survey perspectives and roadmap solutions

**1**

### There are benefits in having a dedicated privacy or data protection law

All the regulators we interviewed saw the benefit of having a dedicated regulatory instrument to manage privacy. Some of the benefits include having a comprehensive law that covers all sectors, providing a baseline requirement for organisations to meet regarding data protection and privacy, relying on a single authority that can coordinate between agencies and sectors, and being empowered to impose penalties in the event of a breach.

**SOLUTION**

**Laws on data protection + implementing guidelines  
+ guidelines or rules on cross-border data flows + enforcement authority**

**2**

### Barriers to progressing privacy frameworks: costs, skills and time

Establishing laws and implementation strategies are not without challenges. The recurrent themes we gathered include costs, the need to build capacity within the government, and the need to have sufficient resources for enforcement. Another challenge includes the long lead time it takes to introduce laws.

**SOLUTION**

**Coordination mechanisms for government agencies + training  
+ enforcement authority + implementation guidelines**

## 3

## Balance between privacy and ICT adoption that drives innovation

Regulators see the merits of establishing laws that accord necessary protections for data subjects, but also respect the need to provide enough room for business to innovate. Getting to a win-win solution is challenging, but doable through approaches that are based on principles, risk, and accountability, and which provide the necessary flexibility for innovation and protection of individuals.

## SOLUTION

**Public-private engagement + multilateral engagement  
+ laws on data protection + guidelines or rules on cross-border data flows**

## 4

## Regulators need access to information

Some regulators cited the need to maintain access to information, especially in situations such as criminal investigations, as a key challenge; others emphasized the need to put in place adequate safeguards to prevent abuse or unauthorised disclosure of or access to the information. Again, getting the balance right is important. When done poorly, this can create conflicting requirements in privacy laws that require the destruction of data versus law enforcement requirements that require the retention of data. This issue can be mitigated by introducing carefully crafted provisions that provide exemptions for access to data in certain situations based on legal due process requirements, as well as better harmonisation of legal requirements across jurisdictions.

## SOLUTION

**Laws on data protection + enforcement authority  
+ guidelines or rules on cross-border data flows + multilateral engagement**

## 5

## Regional privacy frameworks are useful to standardise varying privacy laws

Regional privacy frameworks, such as the APEC CBPR or even an ASEAN equivalent, are deemed useful, as they can help standardize different privacy laws and facilitate data transfer for businesses. Regulators are also supportive of the idea of harmonising the different privacy frameworks, with the caveat that the adequacy mechanism should accord high standards of protection.

## SOLUTION

**Guidelines or rules on cross-border data flows + multilateral engagement  
+ laws on data protection**



## 6

## Existence of candidates for accountability mechanisms is useful

In some countries, each sector has a trust mark provider that provides certifications to businesses that meet certain standards. The existence of such companies makes it easier for some countries to appoint a third-party organisation to assist in the accountability process. For countries that do not have organisations dedicated to the issue of privacy nor a deep pool of privacy professionals, appointing a third-party accountability agent may not be as straightforward. Regulators can share guidance for criteria that a suitable organisation should possess and consider entities based not just in their country but also in their region.

## SOLUTION

**Guidelines or rules on cross-border data flows + multilateral engagement  
+ laws on data protection**

## 7

## Lack of understanding and awareness around privacy

Regulators broadly share the challenge of increasing awareness around the issues and risks inherent in privacy and data protection – across both consumers and businesses. This challenge is lessening somewhat as privacy scandals continue to grow and people become more aware. However, educating consumers and organisations about data is vital. Governments can learn from each other's campaigns to determine what has worked to raise awareness, build these into their national strategies, and ultimately enhance compliance towards an improved environment for data sharing and protection.

## SOLUTION

**National strategy + public-private engagement  
+ implementing guidelines + public education**

---

# Next steps for data privacy and cross-border data flows in Asia

---

Governments and societies face significant challenges when determining the best approach to data governance. The immense economic opportunities arising from the digital economy and data flows are indisputable, as are the potential perils of ignoring privacy concerns. Governments in Asia who may be grappling with how to best proceed can seek guidance from multinational data privacy frameworks, especially those already established in Asia. These frameworks can help governments balance the various interests at stake and devise rules that offer strong data protections while also allowing data to flow across borders in ways that drive economic growth and innovation. As regulators draw on those frameworks to guide changes at the national level, they can in parallel seek to evolve regional frameworks to better match their ambitions for a more harmonised regional approach to data and privacy in Asia. This report is intended to offer some guidance on both counts.

---

At the regional level, this report describes a range of options for ASEAN and APEC governments to consider implementing towards a pan-Asian approach to privacy. These include everything from joint ASEAN-APEC members taking up joint requirements to formal equivalence mechanisms like MoUs and MRAs between ASEAN and APEC. The region may also draw on some of the cross-regional adequacy models that have been agreed elsewhere, and adapt them to an Asian context. Whichever approach is adopted, ASEAN and APEC governments should include actionable steps and a timeframe to ensure participation across all countries, including less-developed states. Harmonisation should also be sensitive to the status of various data privacy regimes, as well as the cultural and socio-political nuances across the different jurisdictions. At the national level, the roadmap included in this report may help to serve Asian governments identify where they stand in terms of the maturity of their data privacy regime, and provide guidance on potential next steps to bolster and harmonise best practices among and between their respective national systems. This includes the complex process of translating high-level principles into actual legislation, as well as a long-term strategy that considers the current landscape, sets goals, and lays out an execution plan. Governments can consider the experience of others in the region as they consider where they stand, and where they ultimately want to go.

ASEAN and APEC governments and enforcement authorities should at a minimum bolster their interaction with one another in ways that can spur deeper collaboration and cross-learning. These engagements – either through their respective organisations or bilaterally – serve as platforms for sharing problems and discussing innovative regulatory solutions to address them. Governments should also draw on non-government data privacy experts in the private sector, civil society, and academia to inform their approaches. These experts can substantially aid governments in their quest to improve public policy in a very complex area that requires a detailed understanding of policy nuances, incentives, and the practical implementation aspects and impact of regulation.

Regardless of which way governments in ASEAN and APEC proceed, they will not be alone. All manner of stakeholder in every jurisdiction across the world is considering the issue of data flows and data privacy. Given Asia's economic size, varying levels of development, and cultural diversity, the way the region's governments approach cross-border data flows and data privacy may serve as an inspiration to governments around the world who wish to craft and implement their own legal frameworks and regulation that are flexible enough to adapt to their own context. In this sense, decisions made in Asia may have positive influence on the direction of global policy relating to data flows and data privacy.



# Call to action

1

ASEAN and APEC governments should attempt to bridge the differences between their respective privacy frameworks by considering technical, political and cross-regional adequacy options.

2

ASEAN and APEC governments should advance harmonisation of national-level privacy regimes. To do so, they can:

- Conduct a landscape analysis to see where they stand in terms of privacy;
- Set goals and objectives for where they want to go based on the elements of a privacy roadmap;
- Execute a plan to evolve privacy elements based on where they stand on the privacy roadmap; and
- Review the experience and case studies of other regional governments to understand common challenges and potential paths forward.

3

ASEAN and APEC governments and privacy enforcement authorities should bolster their interaction with one another to spur deeper collaboration and cross-learning, as well as to build trust and confidence.

4

ASEAN and APEC governments should also draw on non-government privacy experts in the private sector, civil society, and academia to inform their approaches.







# Annex A

Discussions over data protection and data privacy began in the mid-1960s where the use of technology such as surveillance cameras and listening devices started to gain momentum. In the US, there were congressional hearings that were held due to rising concerns from the public. Across the Atlantic, the British parliament began to take interest in the topic and Sweden was the first country to pass a national data protection law in 1973.<sup>92</sup> At the supranational level, data protection rules or guidelines can be traced back to the 1980s with the original OECD guidelines and Convention 108 by the Council of Europe. From these early days, data privacy frameworks have evolved at different levels in many jurisdictions.

## **A1 ASEAN Framework on Personal Data Protection (2016)**

As a diverse region with different levels of development, ASEAN reached a milestone when it adopted a regional ASEAN Declaration on Human Rights that contained provisions concerning data privacy in 2012.<sup>93</sup> Four years later, ASEAN Ministers adopted the ASEAN Framework on Personal Data Protection that indicates a set of principles to guide the implementation of data protection measures at both national and regional levels.<sup>94</sup>

The ASEAN Framework seeks to foster regional integration and cooperation, and to propel ASEAN towards a secure, sustainable and transformative

digitally-enabled economy. It recognises that to achieve this goal, it is essential to strengthen personal data protection and contribute to the promotion and growth of trade and flow of information within and among ASEAN member states in the digital economy.

In turn, Participants (to the Framework) endeavor to cooperate, promote and implement the Principles of Personal Data Protection set out in the Framework in their domestic laws and regulations, and facilitate the free flow of information among them (see table A1). Economies implementing the Framework at a domestic level may adopt exceptions that suit their particular domestic circumstances and the Framework does not create legally-binding domestic or international obligations of any type.

<sup>92</sup> David Vincent, *Privacy*, Wiley, 2016, 286–287.

<sup>93</sup> ASEAN, “ASEAN Human Rights Declaration” (November 2012), <http://asean.org/asean-human-rights-declaration/>, Article 21: Every person has the right to be free from arbitrary interference with his or her privacy, family, home or correspondence including personal data, or to attacks upon that person’s honour and reputation.

<sup>94</sup> ASEAN, “Framework on Personal Data Protection” (16 November 2016), <http://asean.org/storage/2012/05/10-ASEAN-Framework-on-PDP.pdf>.

Table A1

## ASEAN Framework on Personal Data Protection Principles

Principle	Description
<b>Consent, notification and purpose</b>	<p>Pursuant to this principle, an organisation should not collect, use or disclose personal data about an individual unless:</p> <ul style="list-style-type: none"> <li><b>a</b> The individual has been notified of and given consent to the purpose(s) of the collection, use or disclosure of his/her personal data;</li> <li><b>b</b> The collection, use or disclosure without notification or consent is authorised or required under domestic laws and regulations.</li> </ul> <p>Further, an organisation may only collect, use or disclose personal data about an individual for purposes that a reasonable person would consider appropriate in the circumstances.</p>
<b>Accuracy of personal data</b>	<p>Personal data should be accurate and complete to the extent necessary for the purpose(s) for which it is to be used or disclosed.</p>
<b>Security safeguards</b>	<p>Provides that personal data should be appropriately protected against loss and unauthorised access, collection, use, disclosure, copying, modification, destruction or similar risks.</p>
<b>Access and correction</b>	<p>This principle grants individuals the right to request from organisations:</p> <ul style="list-style-type: none"> <li><b>a</b> Access to their personal data (which is in the possession or under the control of the organisation) within a reasonable period of time; and</li> <li><b>b</b> The correction of an error or omission in their personal data (unless domestic laws and regulations require or authorise the organisation not to provide access or correct the personal data in particular circumstances).</li> </ul>
<b>Transfer to another country or territory</b>	<p>According to this principle, organisations should obtain individuals' consent before transferring their personal data to another country or territory, or they should take reasonable steps to ensure that the receiving organisation will protect the personal data consistently with these Principles.</p>
<b>Retention</b>	<p>An organisation should not retain documents containing personal data or should remove the means by which the personal data can be associated with particular individuals as soon as it is reasonable to assume that the retention is no longer necessary for legal or business purposes.</p>
<b>Accountability</b>	<p>An organisation should be accountable for complying with measures which give effect to the Principles. Moreover, an organisation should, on request, provide clear and easily accessible information about its data protection policies and practices with respect to personal data in its possession or under its control. An organisation should also make available information on how to contact the organisation about its data protection policies and practices.</p>

## A2 APEC Privacy Framework (2004, 2015)

In November 2004, Ministers for the 21 APEC member economies endorsed the APEC Privacy Framework. The Framework comprises nine guiding principles to help APEC member economies develop a consistent domestic approach to protection of personal information (see table A2). The second iteration of the Framework was published in 2015. This version is consistent with the core values of the OECD Privacy Framework (2013), and it forms the basis for the development of a regional system called the APEC Cross-Border Privacy Rules (CBPR) that seeks to ensure the continued free flow of personal information across borders, while establishing meaningful protection for the privacy and security of personal information.

The APEC CBPR system is one of the Framework's implementing measures. It was endorsed by APEC Leaders in 2011 and it plays a critical role in the region by promoting a policy framework designed to ensure the continued free flow of personal information across borders, while establishing meaningful protection for the privacy and security of personal information. Six countries currently participate in CBPR: Canada, Japan, Korea, Mexico, Singapore and the U.S.

The CBPR system consists of four elements:

- 1 Set criteria for bodies to become recognised as CBPR system Accountability Agents;
- 2 A process for information controllers to be certified as APEC CBPR system compliant by a recognised Accountability Agent;
- 3 Assessment criteria for use by recognised Accountability Agents when reviewing whether an information controller meets CBPR system requirements; and
- 4 Arrangements for enforcing CBPR system requirements through complaints processes provided by recognised Accountability Agents backed up by a Privacy Enforcement Authority (PEA) that is a participant in the APEC Cross-border Privacy Enforcement Arrangement (CPEA).

Compared to the OECD Framework, the APEC CBPR system takes a step further as it provides a formal system that member economies can participate in to enable its local companies to gain a formal certification that shows they provides a minimum level of privacy protection. Though it is voluntary for companies to participate in the CBPRs, commitments are legally enforceable once a company is included in the system. One ASEAN privacy authority surveyed for this report noted that joining the APEC CBPR could “assist the Commission in its compliance and enforcement functions.”<sup>95</sup>

It is important to note that the CBPR system does not displace or change a country's domestic laws and regulations. The commitments which an organisation carries out in order to participate in the CBPR system are separate from any domestic legal requirements that may be applicable. Where there are no applicable domestic privacy protection requirements in a given country, the CBPR system is intended to provide a minimum level of protection. Where requirements of the CBPR system exceed the requirements of domestic law and regulation, an organisation will need to voluntarily carry out such additional requirements in order to participate.

95 Anonymous quote from the GSMA survey of Asian governments across APEC and ASEAN that was conducted to inform this report.

Table A2

APEC Information Privacy Principles<sup>96</sup>

Principle	Description
<b>Preventing harm</b>	Recognises that one of the primary objectives of the Framework is to prevent misuse of personal information and consequent harm to individuals. Therefore, privacy protections, including self-regulatory efforts, education and awareness campaigns, laws, regulations, and enforcement mechanisms, should be designed to prevent harm to individuals from the wrongful collection and misuse of their personal information. Hence, organisational controls should be designed to prevent harms resulting from the wrongful collection or misuse of personal information, and should be proportionate to the likelihood and severity of any harm threatened by the collection, use or transfer of personal information.
<b>Notice</b>	Personal information controllers should provide clear and easily accessible statements about their practices and policies with respect to personal information. This has the objective of ensuring individuals are able to know what information is collected about them and for what purpose it is to be used. By providing notice, personal information controllers may enable an individual to make a more informed decision about interacting with the organisation.
<b>Collection Limitation</b>	According to this principle, the collection of personal information should be limited to information that is relevant to the purposes of collection and any such information should be obtained by lawful and fair means, and where appropriate, with notice to, or consent of, the individual concerned. <sup>85</sup>
<b>Use of personal information</b>	Limits the use of personal information, including the transfer or disclosure of personal information, to fulfilling the purposes of collection and other compatible or related purposes.  The only exceptions to the application of this principle are: <ul style="list-style-type: none"> <li><b>a</b> When the individual whose personal information is collected has given their consent;</li> <li><b>b</b> When the use (of information) necessary to provide a service or product requested by the individual; or</li> <li><b>c</b> By the authority of law and other legal instruments, proclamations and pronouncements of legal effect.</li> </ul>
<b>Choice</b>	Seeks to ensure that individuals are provided with choice in relation to collection, use transfer and disclosure of their personal information. Whether the choice is conveyed electronically, in writing or by other means, notice of such choice should be clearly worded and displayed clearly and conspicuously. The mechanisms for exercising choice should be accessible and affordable to individuals
<b>Integrity of personal information</b>	Personal information controllers are obliged to maintain the accuracy and completeness of records and keep them up to date as necessary to fulfil the purposes of use
<b>Security safeguards</b>	Recognises that individuals whose personal information is entrusted to others are entitled to expect that their information be protected with reasonable security safeguards.
<b>Access and corrections</b>	Includes specific conditions for what would be considered reasonable in the provision of access, including conditions related to timing, fees, and the manner and form in which access would be provided. What is to be considered reasonable in each of these areas will vary from one situation to another depending on circumstances, such as the nature of the information processing activity. Access will also be conditioned by security requirements that preclude the provision of direct access to information and will require sufficient proof of identity prior to provision of access.
<b>Accountability</b>	Provides that when transferring information, personal information controllers should be accountable for ensuring that the recipient will protect the information consistently with these Principles. Thus, information controllers should take reasonable steps to ensure the information is protected, in accordance with these Principles, after it is transferred.

96 APEC, "APEC Cross-Border Privacy Rules System," <https://www.apec.org/Groups/Committee-on-Trade-and-Investment/-/media/Files/Groups/ECSG/CBPR/CBPR-PoliciesRulesGuidelines.ashx>, accessed on 28 May 2018.

97 The principle also recognises that there are circumstances where providing notice to, or obtaining consent of, individuals would be inappropriate. These cases are limited and specific.



In addition to the CBPR, APEC’s implementing measures include the Privacy Recognition for Processors System (PRP) that employs a similar accountability system to CBPR, with the focuses on data processors instead of data controllers, as well as a multilateral mechanism to encourage coordination among data privacy authorities through the Cross-Border Privacy Enforcement Arrangement (CPEA). These are mutually reinforcing measures. For example, a country must first agree to participate in CPEA before it can join the CBPR.

The Guidelines recognise a common interest in promoting and protecting the fundamental values of privacy, individual liberties and the global free flow of information. They reflect an acknowledgment of the increased privacy risks brought about by more extensive and innovative uses of personal data. They evidence the need for improved interoperability among privacy frameworks as well as strengthened cross-border cooperation among privacy enforcement authorities, as amplified by the continuous flows of personal data across global networks. Further, they aim to prevent the creation of unjustified obstacles to the development of economic and social relations among member countries. To achieve this, they adopt a risk-based approach for the development of policies and safeguards to protect privacy.

### A3 OECD Privacy Framework (1980, 2013)

The OECD privacy framework was developed in 1980 and was updated in 2013 to modernise its approach.<sup>98</sup> The original framework represents the first international consensus on how best to balance effective privacy protection with the free flow of personal data. Crafted towards a technology-neutral and flexible set of official guidelines that allow for various means of compliance, the framework has served as a key reference for a large number of national regulatory and self-regulatory instruments, including many in Asia.

The Guidelines encourage member countries to demonstrate leadership and commitment to the protection of privacy and free flow of information at the highest levels of government. They also promote the implementation of the Guidelines through processes that include all relevant stakeholders. On the other hand, non-members are invited to adhere to the recommendations issued in the Guidelines and to collaborate with member countries in their implementation across borders.

The Guidelines include 8 now widely accepted privacy principles:

Table A3

## The OECD Privacy Principles<sup>99</sup>

Principle	Description
<b>Collection limitation</b>	The collection of personal information should be limited, should be obtained by lawful and fair means, and, where appropriate, with the knowledge or consent of the individual.
<b>Data quality</b>	Personal information should be relevant to the purpose for which it is collected, and should be accurate, complete, and current as needed for that purpose.
<b>Purpose specification</b>	The purposes for the collection of personal information should be disclosed before collection and upon any change to those purposes, and the use of the information should be limited to those purposes and compatible purposes.
<b>Use limitation</b>	Personal information should not be disclosed or otherwise used for other than a specified purpose without the consent of the individual or legal authority.
<b>Security safeguards</b>	Personal information should be protected with reasonable security safeguards against risks such as loss or unauthorised access, destruction, use, modification or disclosure.
<b>Openness</b>	The public should be informed about privacy policies and practices, and individuals should have ready means of learning about the use of personal information.
<b>Individual participation</b>	Individuals should have the following rights: to know about the collection of personal information, to access that information, to request correction, and to challenge the denial of those rights.
<b>Accountability</b>	Individuals controlling the collection or use of personal information should be accountable for taking steps to ensure the implementation of these principles.

98 OECD, “The OECD Privacy Framework” (2013), <http://www.oecd.org/sti/ieconomy/privacy-guidelines.htm>; the updated framework focused on the practical implementation of privacy protection due to the incredible volume of personal data being collected, used and stored, the range of analytics leveraging data, the value of data, the evolving threats to privacy, and the global availability of data, while also addressing the global dimension of privacy through improved interoperability.

99 OECD, “The OECD Privacy Framework” (2013), <http://www.oecd.org/sti/ieconomy/privacy-guidelines.htm>.

The OECD Guidelines also suggest that countries should not restrict personal data flows between countries where each country observes the Guidelines, or where sufficient safeguards exist to ensure commensurate levels of protection. Further, the Guidelines mandate that any restrictions to transborder flows of personal data should be proportionate to the risks presented, taking into account the sensitivity of the data, and the purpose and context of the processing.

The Guidelines call for member countries to take appropriate measures to facilitate cross-border privacy law enforcement cooperation, in particular by enhancing information sharing among privacy enforcement authorities. They urge member countries to support the development of international

arrangements that promote interoperability among privacy frameworks that give practical effect to the Guidelines.

The OECD also suggests a number of steps towards implementing the Guidelines, such as developing a national privacy strategy, adopting privacy laws, and establishing a privacy enforcement authority. These steps also encourage self-regulation, appropriate sanctions and remedies, means to exercise individual rights and ensure no unfair discrimination of data subjects, consideration of the roles of various actors, and adoption of complementary measures like education and skills training.



## A4 The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) (1981)

Building on the OECD’s work, Convention 108 was signed in 1981 by Member States of the Council of Europe seeking to reconcile the fundamental values of the respect for privacy and the free flow of information between countries. Parties to the Convention commit to take the necessary measures in their domestic law to provide for enforcement of the basic principles for data protection. They also agree not to prohibit or subject to special authorisation any transborder flows of personal data going to the territory of another Party, solely for the purpose of the protection of privacy.

Through this effort, the Convention seeks to establish minimum standards. However, it does not limit or otherwise affect the possibility for a Party to grant data subjects a wider measure of protection than that stipulated in the Convention.

Further, Parties agree to render each other mutual assistance in order to implement the Convention. Specifically, they agree to each designate one or more authorities to oversee the Party’s commitments under the Convention, which shall provide information to other designated authorities on request on its law and administrative practice in the field of data protection.

Convention 108 has also recently been adopted by several countries outside of Europe: Uruguay in 2013, Mauritius and Senegal in 2016, and Tunisia in 2017.

Table A4

### Convention 108 Basic Principles for Data Protection<sup>100</sup>

Principle	Description
<b>Quality of data</b>	<p>Personal data undergoing automatic processing shall be:</p> <ul style="list-style-type: none"> <li><b>a</b> Obtained and processed fairly and lawfully;</li> <li><b>b</b> Stored for specific and legitimate purposes and not used in a while incompatible with those purposes;</li> <li><b>c</b> Adequate, relevant and not excessive in relation to the purposes for which they are stored;</li> <li><b>d</b> Accurate and, where necessary, kept up to date;</li> <li><b>e</b> Preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.</li> </ul>
<b>Data security</b>	<p>Appropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination.</p>
<b>Additional safeguards for the data subject</b>	<p>Any person shall be enabled:</p> <ul style="list-style-type: none"> <li><b>a</b> To establish the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file;</li> <li><b>b</b> To obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in the automated data file as well as communication to him of such data in an intelligible form;</li> <li><b>c</b> To obtain as the case may be, rectification or erasure of such data if these have been processed contrary to the provisions of domestic law giving effect to the basic principles set out in the Convention;</li> <li><b>d</b> To have a remedy if a request for confirmation or, as the case may be, communication, rectification or erasure as referred to in paragraphs b and c of this article is not complied with.</li> </ul>

100 Council of Europe, “Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data” (1981), <https://rm.coe.int/1680078b37>.



## A5 Madrid Resolution (2009)

In 2009, data protection authorities from over 50 countries approved the “Madrid Resolution” on international privacy standards. This resolution brought together multiple approaches to the protection of the right to privacy, integrating legislation from all five continents. It was intended to constitute the foundation for the development of an internationally binding tool that would contribute to a greater protection of individuals’ rights and freedoms at a global level.<sup>101</sup>

The Madrid Resolution offers a set of standards that represent international minimums, including a set of principles and rights to allow for the achievement of a greater degree of international consensus that would serve as reference for those countries that do not have a legal and institutional structure for data protection. It also offers proactive measures to encourage States to promote better compliance with applicable data protection laws. Such measures include the establishment of procedures aimed at the prevention and detection of offences; the periodic offering of awareness, education and training programs; and the establishment of authorities to guarantee and supervise individuals’ rights. The Resolution proposes its international standards based on a series of principles, rights and obligations that any privacy protection legal system must strive to achieve to guarantee the effective protection of privacy at an international level, as well as to ease the international flow of personal data. Among others, these basic principles include loyalty, legality, proportionality, quality, transparency, responsibility, access, rectification, cancellation and objection.

In addition, the Madrid Resolution determines the requirements that must be met for the legal collection, preservation, use, revelation or erasure of personal data – for example, the prior obtaining of the free,

unequivocal and informed consent from the person providing the data. It also includes obligations such as security of personal data, through those measures that are considered appropriate in each case, or confidentiality, which affects the controller as well as anyone who participates in any of the stages in which personal data is managed. On the other hand, the text recalls that, as a general rule, international personal data transfers may be performed when the State to which the data is transferred offers, at least, the level of protection foreseen in the document; or when whoever wants to transfer the data can guarantee that the addressee will offer the required level of protection, for example, through appropriate contractual clauses. Finally, it points to the need for the existence of supervisory authorities, and for the different states to cooperate and coordinate their activities.

## A6 General Data Protection Regulation (2016)

The European Union finalised its General Data Protection Regulation (GDPR) in 2016 and it is effective from 25 May 2018.<sup>102</sup> The GDPR has several key elements (principally large fines) and principles (extra-territoriality) that have changed the global regulatory landscape in terms of data privacy, control, processing and localisation.

The GDPR extends the jurisdiction of its regulatory landscape of data privacy, as it applies to companies processing the personal data of individuals residing in the EU, regardless of the company’s location. The GDPR places strict conditions on both the entity determining how and why personal data is collected and processed (“controllers” for its purposes) and the one that processes it on behalf of the controller (“processors”).<sup>103</sup>



**In a February 2018 address to the Asia Business Law Institute, Singapore’s Honourable Chief Justice Sundaresh Menon highlighted how the GDPR will have “far-reaching extra-territorial effects” and bring increased “pressure” for companies to adhere to the requirements imposed under the regulation.**

101 The intention was for the Madrid Resolution to become a “soft law” tool, widely demanded by international companies, in order to respect the minimum privacy needs of citizens worldwide.

102 European Data Protection Supervisor, “The History of the General Data Protection Regulation,” <https://goo.gl/4e8UTN>, accessed on 28 May 2018; the GDPR updated the EU’s previous Data Protection Directive of 1995.

103 Where the activities relate to: offering goods or services to EU citizens (irrespective of whether payment is required) and the monitoring of behavior that takes place within the EU. Non-EU businesses processing the data of EU citizens will also have to appoint a representative in the EU.



Unlike under other regimes, under the GDPR, processors will have significantly more obligations – and liability in the event of a breach. The GDPR also places further obligations on controllers to ensure their contracts with processors comply with the GDPR. Organisations in breach of GDPR can be fined up to 4 per cent of annual global turnover or €20 million (whichever is greater).<sup>104</sup> GDPR also calls for privacy by design and default. Data protection should be included from the onset of the designing of systems, rather than an addition, and the system should be designed so that only personal data necessary for a specific purpose should be processed. Certain organisations will also be required to appoint an internal Data Protection Office (DPO), if their core activities consist of processing operations which require regular and systematic monitoring of data subjects on a large scale or of special categories of data, or data relating to criminal convictions and offences.

The GDPR also strengthens the conditions for consent and accountability. Request for consent must be given in an intelligible and easily accessible form, with the purpose for data processing attached to that consent,<sup>105</sup> while also creating mandatory breach notification requirements.<sup>106</sup> A key innovation of GDPR in relation to previous data protection laws is the emphasis on accountability as a core principle. This requires organisations to introduce appropriate technical and organisational measures to demonstrate their compliance with the law. Such measures could include adequate documentation on what personal data is processed, how it is processed, to what purpose, how long it will be stored for, and whether a Data Protection Officer is properly integrated in the organisation planning and operations. Finally, GDPR updates the EU’s longstanding rights-based approach to privacy (in table A5).

Table A5

## GDPR Data Subject Rights<sup>107</sup>

Right	Description
<b>Right to be informed</b>	The right to be informed encompasses the obligation to provide ‘fair processing information’, typically through a privacy notice. It emphasises the need for transparency over how personal data is used.
<b>Right of access</b>	Individuals have the right to obtain: confirmation that their data is being processed; access to their personal data; and other supplementary information.
<b>Right of rectification</b>	Individuals are entitled to have personal data rectified if it is inaccurate or incomplete.
<b>Right to erasure</b>	Also known as ‘the right to be forgotten’. The broad principle underpinning this right is to enable an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing.
<b>Right to restrict processing</b>	Individuals have a right to ‘block’ or suppress processing of personal data. When processing is restricted, data controllers or processors are permitted to store the personal data, but not further process it.
<b>Right to data portability</b>	The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.
<b>Right to object</b>	Individuals have the right to object to: processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling); direct marketing (including profiling); and processing for purposes of scientific/historical research and statistics.
<b>Right in relation to automated decision making and profiling</b>	The GDPR provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention.

104 This is the maximum fine that can be imposed for the most serious infringements. There is a tiered approach to fines. It is important to note that these rules apply to both controllers and processors.  
 105 It must be a freely given, specific, informed and unambiguous indication of the individual’s wishes. There must be some form of clear affirmative action – or in other words, a positive opt-in – consent cannot be inferred from silence, pre-ticked boxes or inactivity. Consent must also be separate from other terms and conditions. Additionally, it must be as easy to withdraw consent as it is to give it.  
 106 This must be done within 72 hours of first having become aware of the breach. Data processors will also be required to notify their customers, the controllers, “without undue delay” after first becoming aware of a data breach.  
 107 Council of Europe, “Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data” (1981), <https://rm.coe.int/1680078b37>.

## A7 EU-U.S. Privacy Shield (2016)

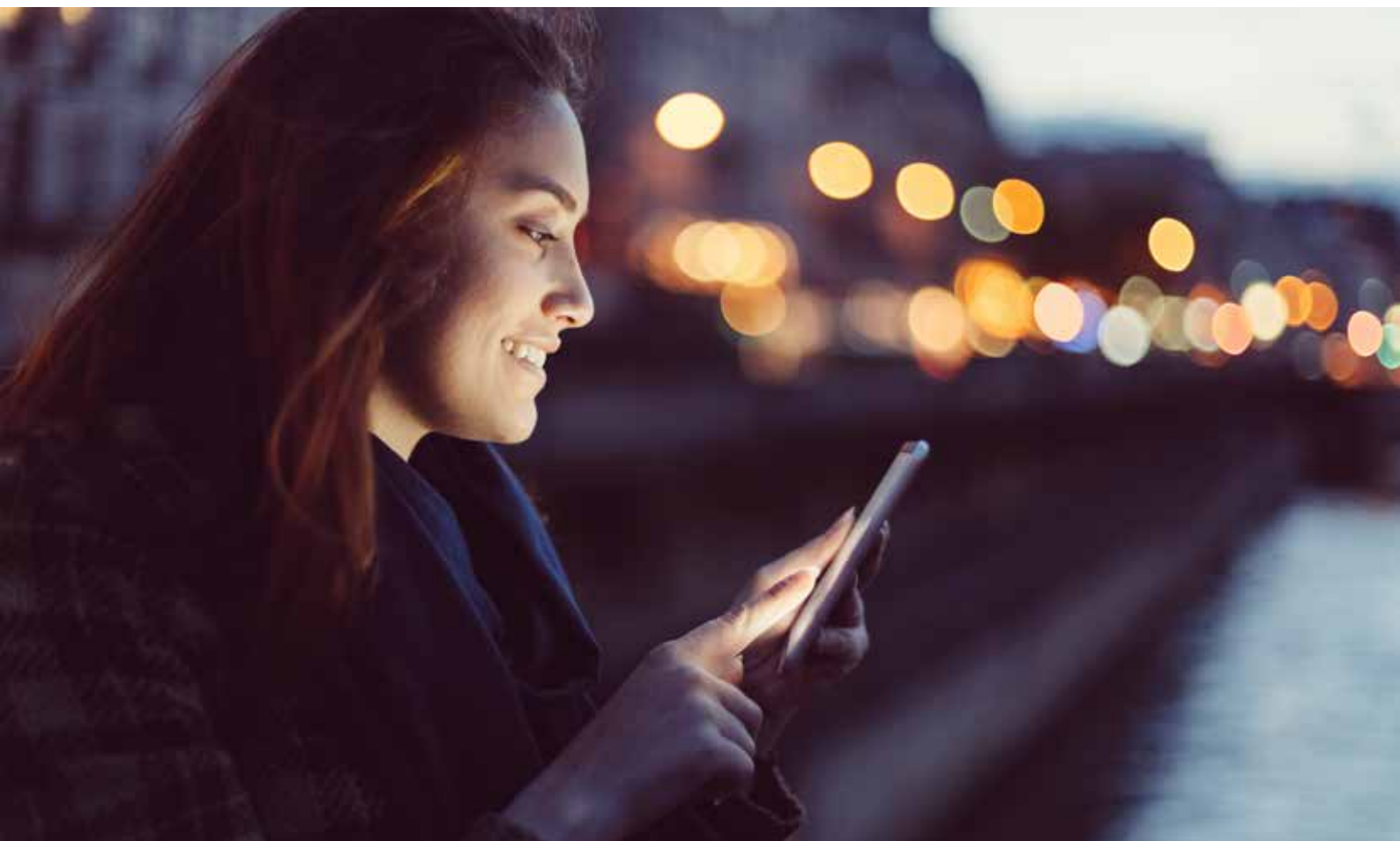
In February 2016, the European Commission and the U.S. Department of Commerce adopted the EU-U.S. Privacy Shield to facilitate transatlantic exchanges of personal data for commercial purposes. It was formally adopted on 12 July 2016, after a predecessor agreement was struck down at the Court of Justice of the European Union (CJEU) in 2015. The agreement represents an important and working model of a cross-regional approach to privacy.

The EU-U.S. Privacy Shield aims to protect the fundamental rights of individuals where their data is transferred to the U.S. and ensure legal certainty for businesses. It builds on the previous U.S.-EU Safe Harbor Framework and imposes stronger obligations on companies in the U.S. to protect the personal data of individuals and stronger monitoring and enforcement by the U.S. Department of Commerce and Federal

Trade Commission, including an increased cooperation with the European data protection authorities.<sup>108</sup>

The Privacy Shield includes written commitments and assurance by the U.S. that any access by public authorities to personal data transferred under the new arrangement on national security grounds will be subject to clear conditions, limitations and oversight, preventing generalised access. It also includes several dispute resolution mechanisms, which are intended to handle and solve complaints or enquiries raised by EU individuals. U.S. companies that manage data in Europe must undergo a yearly self-assessment that they meet the high data protection standards set out by the arrangement.

It should be noted that the Irish High Court has referred questions to the CJEU on whether the EU-U.S. Privacy Shield, or standard contractual clauses, respects European citizens' right to privacy under the EU's Charter of Fundamental Rights. The CJEU has yet to issue its binding opinion.



<sup>108</sup> The U.S. Department of Transportation enforces the EU-U.S. Privacy Shield in the context of airlines and ticket agents.

---

# Annex B

## Economic impact of cross-border data flows and data localisation in the Asia Pacific

---

Desk research of reports from international organisations, such as the World Economic Forum, trade associations and research think tanks including the European Centre for International Political Economy and the Asia-Pacific MSME Trade Coalition, provides some insights on the economic benefits of cross-border data flows as well as the impact of barriers such as data localisation on the economy.

---

### Economic benefits of cross-border data flows

#### **Cross-border data flows enable rapid economic growth, and Asia has benefited substantially**

Data flows are the lifeblood of the global internet economy. Countries that enable cross-border data flows see growth in the e-commerce sector, engage in broader digital trade and adopt technology faster. All of these factors empower economic growth, social development and confidence in international markets.

Below is an indication of the scope of these benefits:

- Over the past decade, international data flows have increased global GDP by 10.1 per cent, and data flows now account for US\$2.8 trillion of global GDP (2014), a larger share than global trade in goods.<sup>109</sup>
- Between 2005 and 2015, global flows of data grew 45 times,<sup>110</sup> while by the end of 2016, the raw volume of global data flows reached 400 terabits

109 James Manyika, et al., "Digital Globalisation: The New Era of Global Flows," McKinsey Global Institute, (February 2016), <https://goo.gl/5jvm1a>, 10 and 76.

110 Ibid, 30.

per second.<sup>111</sup> Projections suggest that cross-border data flows will increase another nine-fold by 2020.<sup>112</sup> This growth in data flows contrasts the growth of traditional value flows of physical goods and services, which have barely managed to grow at the pace of worldwide nominal GDP.

- Current trade statistics significantly underestimate the magnitude and growth of cross-border data flows, and as a result, the contributions of cross-border data flows to global growth and to small businesses are significantly underestimated.<sup>113</sup>
- According to UNCTAD, world trade in IT and ICT-enabled services amounted to approximately US\$1.6 trillion or 48 per cent of all traded services in 2007.<sup>114</sup>
- In India, cross-border data flows have been a driver of innovation. Several of India's most innovative companies, including Zoho Corp., Myntra, Flipkart, and Fortis Healthcare, utilise global cloud computing services, or operate data centres outside of India to improve the delivery of their respective proprietary services, as well as to reduce costs so that money is available to focus on strategic investments.<sup>115</sup>
- In Indonesia, the productivity improvements from digitising processes and using cross-border data flows including in manufacturing and retail are estimated to have a US\$34.4 billion and US\$24.5 billion contribution to GDP respectively.<sup>116</sup> Furthermore, cross-border data flows and cloud computing have allowed local firms like Go-Jek to springboard from a small operation in 2014 to a “unicorn” company in just a few short years, raising over a billion in investment and challenging global transportation giants like Uber.
- Worldwide, the shift to cloud computing could create nearly 14 million new jobs by 2015, with a majority of these new jobs potentially being in large emerging economies.<sup>117</sup>
- In the Philippines, one of the world's top business process outsourcing locations, the sector generates close to US\$25.5 billion annually, employs 1.4 million people and is built on low-cost and efficient cross-border data flows across all vertical sectors.<sup>118</sup>
- According to a 2016 study by the U.S. Chamber of Commerce:
  - Economies stand to reap multiple benefits if they take action on creating an open, competitive marketplace for cross-border ICT services by removing a number of identified barriers. By doing so, Asian countries can save up to US\$17.84 billion in Japan, US\$7.42 billion in South Korea, US\$3.04 billion in Indonesia and US\$0.22 billion in Vietnam.<sup>119</sup>
  - Global liberalisation of cross-border data flows creates new demand for ICT services, which in turn generates new businesses and creates new jobs. In the long-run it is estimated that global liberalisation will lead to the creation of 2.89 million companies and 23 million new jobs with over 361,000 new business and 2.8 million jobs being created in Japan, South Korea, Indonesia and Vietnam.<sup>120</sup>
  - Global liberalisation of cross-border data flows can potentially increase global GDP by US\$1.72 trillion. In Japan, South Korea, Indonesia and Vietnam, GDP is estimated to increase by US\$83.64 billion, US\$33.01 billion, US\$29.38 billion and US\$3.46 billion respectively.<sup>121</sup>
- A 2014 International Trade Commission (ITC) estimated that removing foreign digital trade barriers would increase U.S. GDP by US\$16.7 to US\$41.4 billion (0.1 to 0.3 per cent) and wages by 0.7 to 1.4 per cent in the seven digitally intensive sectors.<sup>122</sup>
- A 2016 study by the European Centre for International Political Economy shows that elimination of current data localisation measures in the EU can generate GDP gains of up to 1.1 per cent.<sup>123</sup>

111 McKinsey Global Institute, “The ascendancy of international data flows” (January 2017), <https://www.mckinsey.com/mgi/overview/in-the-news/the-ascendancy-of-international-data-flows>.

112 James Manyika, et al., “Digital Globalisation: The New Era of Global Flows,” 31

113 Michael Mandel, “Data, Trade, and Growth” Progressive Policy Institute (April 2014), [http://www.progressivepolicy.org/wp-content/uploads/2014/04/2014.04-Mandel\\_Data-Trade-and-Growth.pdf](http://www.progressivepolicy.org/wp-content/uploads/2014/04/2014.04-Mandel_Data-Trade-and-Growth.pdf).

114 United Nations Conference on Trade and Development, “Information Economy Report 2009” (2009), [http://unctad.org/en/Docs/ier2009\\_en.pdf](http://unctad.org/en/Docs/ier2009_en.pdf), xvi.

115 Ibid, 15.

116 Brookings Institute, “Regulating for a Digital Economy,” 34.

117 IDC, “Cloud Computing's Role in Job Creation” (March 2012), [https://news.microsoft.com/download/features/2012/IDC\\_Cloud\\_jobs\\_White\\_Paper.pdf](https://news.microsoft.com/download/features/2012/IDC_Cloud_jobs_White_Paper.pdf).

118 Ibid, 16.

119 U.S. Chamber of Commerce, “The Economic Impact of Cross-Border ICT Services” (2016), [https://www.uschamber.com/sites/default/files/executive\\_summary.pdf](https://www.uschamber.com/sites/default/files/executive_summary.pdf), 13.

120 Ibid, 14.

121 Ibid, 16.

122 United States International Trade Commission (USITC), “Digital Trade in the U.S. and Global Economies, Part 2” (August 2014), <https://www.usitc.gov/publications/332/pub4485.pdf>, 12.

123 Matthias Bauer, Martina F. Ferracane, Hosuk Lee-Makiyama, and Erik van der Marel, “Unleashing Internal Data Flows in the EU: An Economic Assessment of Data Localisation Measures in the EU Member States,” European Centre for International Political Economy (2016), II.



### Cross-border data flows enable APAC businesses to grow in a digital world, especially micro, small and medium enterprises (MSMEs) and start-ups

To compete in today's digital world, companies large and small, particularly in Asia, rely on free or low-cost digital tools. MSMEs need access to digital inputs such as pay-as-go and customisable cloud computing offerings that provide on demand computing power and software that was previously only accessible for large companies. Cloud and other preliminary and free digital services, like email, are online and cross-border in nature. Cross-border data flows enable the adoption of technology and the necessary tools that help businesses be more efficient, grow, and innovate. Examples of how cross-border data flows enable APAC businesses to grow in a digital world include

- Data from eBay across 22 countries shows that 97 per cent of technology-enabled small firms export, up to 100 per cent in some countries.

By comparison only 2–28 per cent of traditional (non-tech using) SMEs export for most countries.<sup>124</sup>

- In a 2017 Asia-Pacific MSME Trade Coalition study found that more than US\$339 billion can be saved by export-focused MSMEs through the utilisation of digital tools.<sup>125</sup>
- In Indonesia, MSMEs benefit from lower supply costs, immediate transactions, and far greater market reach – with digitalisation boosting overall revenues by up to 80 per cent.<sup>126</sup> This is because e-commerce has produced a net market expansion effect. Consumers are seeing an increase in consumer welfare due to improved information, product access, and lower prices.
- In 2014, Asia Pacific surpassed North America as the largest regional e-commerce market, with US\$525.2 billion in business-to-consumer e-commerce sales, compared with US\$482.6 billion in North America.<sup>127</sup>

## Case study How GO-JEK utilised cloud services to scale its business

When GO-JEK first launched its app in 2015, it had only 100 employees. But two and a half years later, it expanded rapidly into a 2,000 employee-strong organisation and offered a wider range of services from transport to logistics and payments across 25 Indonesian cities. The business provides services in 15 industry verticals and is the market leader in 13 of them.

During its period of growth, GO-JEK faced greater business complexity and yet it wanted to grow. So, it decided to shift its operations to a cloud platform to scale more rapidly and back hundreds of back-end services supporting its services that include ride services, food delivery, tickets and shopping.

Today, GO-JEK is running nearly all its services on cloud, including microservices, databases, enterprise service bus, and others. Had it not had access to cloud technology, GO-JEK would not have achieved the scalability required to support the growth that attracted hundreds of millions of dollars in private capital investment in the business.

Furthermore, the cloud system allows GO-JEK to automate all its key processes and free up resources to focus on its core business, as well as enable it to divert resources quickly to support any spikes in demand and still deliver an optimal customer service experience.

124 eBay, "Small Online Business Growth Report" (2016), San Jose CA: eBay Inc.

125 Asia-Pacific MSME Trade Coalition, "SMEs: The New Stakeholders of International Trade" (December 2017), <http://tradecoalition.org/resource/smes-the-new-stakeholders-of-international-trade/>.

126 Asia Cloud Computing Association, "Cross-Border Data Flows," 32.

127 Brookings Institute, "Regulating for a Digital Economy," 26.

## Cross-border data flows facilitate e-payments and digital transactions

To enable e-payments – which is a cross-border data flow – it is imperative that data moves freely. The free flow of data reduces transaction costs, reduces the constraints of distance, and increases organisational efficiencies, which can lead to the emergence of new enterprises. Financial services that provide e-payment systems such as Paypal, Paytm and others, provide digital means to capitalise on the opportunities of cross-border remittances and support e-commerce transactions. This produces easier, efficient and secure digital economic action.<sup>128</sup> The following examples illustrate how cross-border data flows facilitate e-payments and digital transactions:

- Electronic payments added US\$296 billion to GDP in 70 countries studied between 2011 and 2015. The increase in electronic payments resulted in almost the same percentage increase in GDP between 2011 and 2015 for emerging markets (0.11 per cent) as for developed countries (0.08 per cent).<sup>129</sup>
- Each 1 per cent increase in usage of electronic payments produces, on average an annual increase of -\$104 in the consumption of goods and services, a 0.04 per cent increase in GDP.<sup>130</sup>
- A McKinsey report estimates that the shift from cash to digital payments could increase GDP across developing economies by 6 per cent before 2025, adding US\$3.7 trillion and around 95 million jobs.<sup>131</sup>
- In the Philippines, according to IDC, six of the top ten fastest growing fintech companies were involved in the payments space. This highlights the importance of digital payments in, to and from the Philippines, and the growing potential of mobile e-commerce.<sup>132</sup>
- In India, the government has enforced a demonetisation scheme, encouraging the adoption of digital payment systems to increase money transfer efficiency and reliability. In the first quarter of 2017, smartphone and internet users drove mobile wallet transactions in India, amounting to US\$3.6 billion in transactions – a 60 per cent increase from the quarter prior.<sup>133</sup>
- Last year in APAC alone, around 1 billion people made an online purchase in 2017 and retail e-commerce sales in APAC are expected to reach US\$6.5 trillion in 2021.<sup>134</sup>
- By 2015, the digital economy of the 10 ASEAN economies was estimated to generate US\$150 billion in revenues annually, with the potential to add an incremental US\$1 trillion in GDP by 2025.<sup>135</sup>
- In Japan, free flows of data have facilitated demand for Japanese products and services from overseas, with Chinese consumers spending US\$6.6 billion on direct e-commerce purchases from Japan in 2015.<sup>136</sup>

128 Asia Cloud Computing Association, "Cross-Border Data Flows."

129 Moody's Analytics, "The Impact of Electronic Payments on Economic Growth" (February 2016), <https://usa.visa.com/dam/VCOM/download/visa-everywhere/global-impact/impact-of-electronic-payments-on-economic-growth.pdf>.

130 Ibid.

131 James Manyika, et al., "Digital Finance for All: Powering Inclusive Growth in Emerging Economies," McKinsey & Company (2016), <https://www.mckinsey.com/featured-insights/employment-and-growth/how-digital-finance-could-boost-growth-in-emerging-economies>.

132 Asia Cloud Computing Association, "Cross-Border Data Flows," 50.

133 Brookings Institute, "Regulating for a Digital Economy," 33.

134 eMarketer, "Retail Sales in Asia-Pacific Will Increase 7.7% this Year" (11 August 2017), <https://retail.emarketer.com/article/retail-sales-asia-pacific-will-increase-7-7-this-year/598dcca6ebd40003acdf2e02>.

135 Brookings Institute, "Regulating for a Digital Economy: Understanding the Importance of Cross-Border Data Flows in Asia" (April 2018), [https://www.brookings.edu/wp-content/uploads/2018/03/digital-economy\\_meltzer\\_lovelock\\_web.pdf](https://www.brookings.edu/wp-content/uploads/2018/03/digital-economy_meltzer_lovelock_web.pdf), 28.

136 Asia Cloud Computing Association, "Cross-Border Data Flows: A Review of the Regulatory Enablers, Blockers, and Key Sectoral Opportunities in Five Asian Economies: India, Indonesia, Japan, the Philippines, and Vietnam" (2018), [http://www.asiacloudcomputing.org/images/acca2018\\_cbdf\\_casestudies%201.pdf](http://www.asiacloudcomputing.org/images/acca2018_cbdf_casestudies%201.pdf), 34.

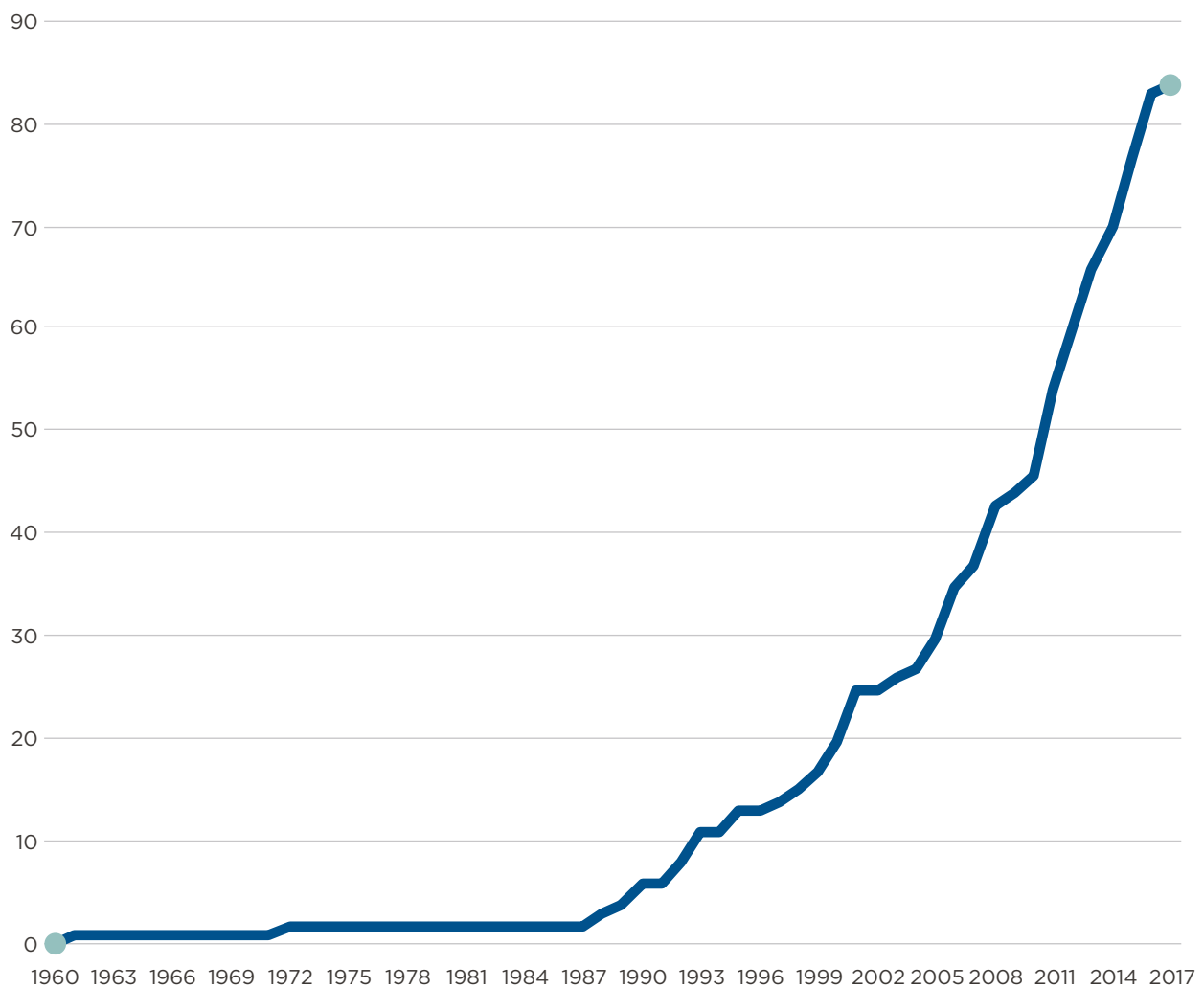
## Barriers to cross-border data flows

Requiring data to be stored locally or using local suppliers on the grounds of protecting national security or economic interests has several negative effects on economic growth. It eliminates the economic benefits of large-scale computing resources, preventing businesses from utilising tools such as global cloud. It cuts off access to foreign buyers, stifling international engagement and trade. It discourages potential investment opportunities and

capital inflows contrary to global growth strategies. More fundamentally, it has negative effects on economic factors including growth, foreign direct investment (FDI), and productivity. As shown in figure A1 below, the last decade has seen a worrying increasing trend of data localisation worldwide. From year 2000 to 2008 the number of data localisation measures more than doubled, and from 2008 to 2017, it doubled again.<sup>137</sup>

Figure A1

### Cumulative Number of Data Localisation Measures (1961–2016)<sup>138</sup>



Note: When the year of the law was not available, the year in which the measure was reported is considered. The graph does not include one measure for which the year was not available.

Source: ECIPE

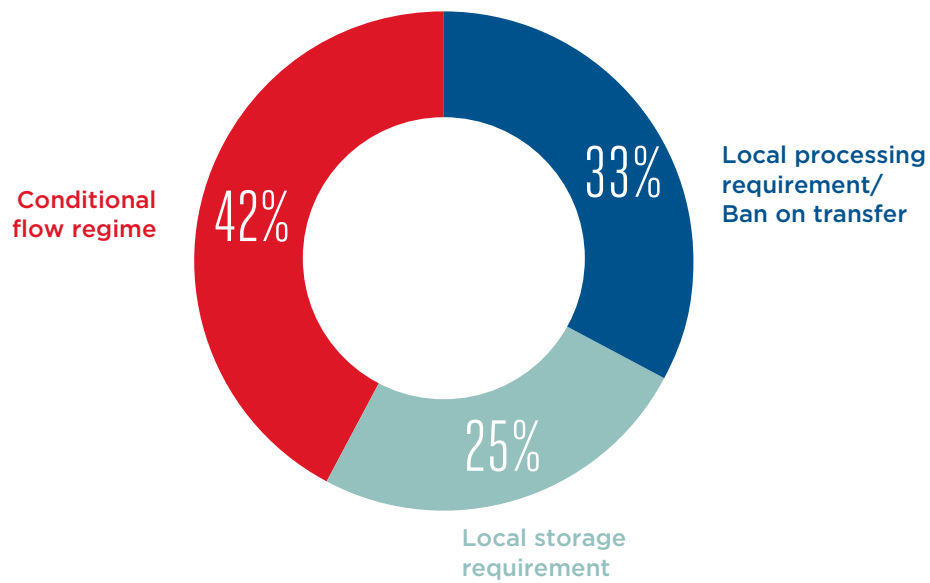
<sup>137</sup> Francesca, Lee-Makiyama and Marel, "Digital Trade Restrictiveness Index," European Centre for International Political Economy (ECIPE) (April 2018), <http://ecipe.org/app/uploads/2018/04/DTRI-final1.pdf>, 55.

<sup>138</sup> Ibid, 55.

- Out of the restrictions imposed, local storage requirement, local processing requirement, and conditional flow regime account for 25 per cent, 33 per cent and 42 per cent respectively.<sup>139</sup>

**Figure A2**

### Data localisation measures by type (%)<sup>140</sup>



Source: ECIPE

- The Digital Trade Restrictiveness Index (DTRI) sheds light on how countries compare with each other when it comes to data restrictions. As shown in figure A3, several Asian countries impose greater data restrictions than the average; those countries include China, Indonesia, Vietnam, Korea and Thailand.

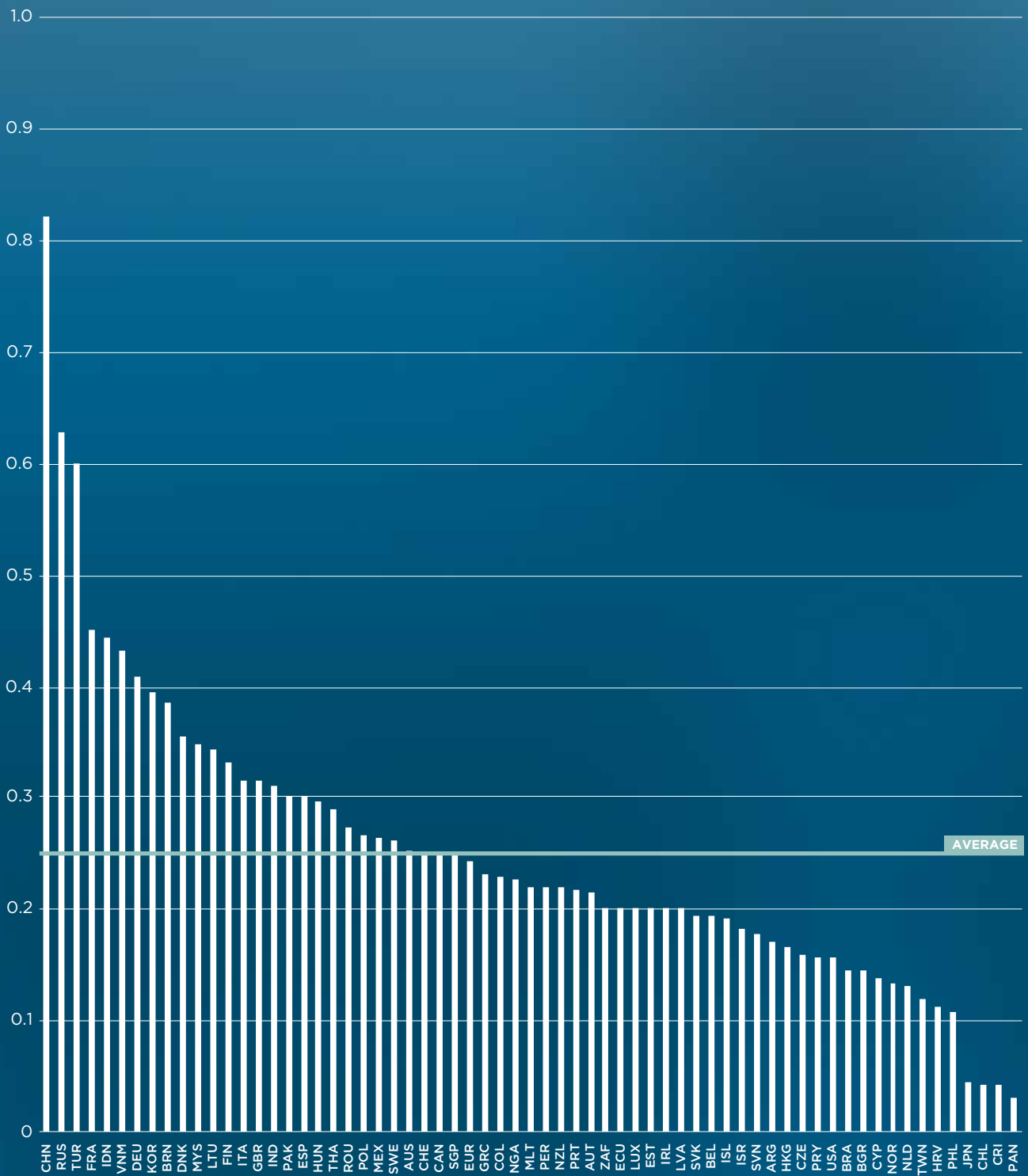
<sup>139</sup> Ibid, 56.

<sup>140</sup> Ibid, 56.



Figure A3

# DTRI Cluster C - Restrictions on Data<sup>141</sup>



Source: ECIPE

141 Ibid, 18.

- Various studies show significant negative economic impact from data localisation. The estimates vary since the studies were conducted at different times, but they all indicate negative impacts:
  - A 2016 CIGI and Chatham House study’s econometric modelling shows that the lost Total Factor Productivity (due to data localisation or barriers) in downstream sectors, especially in the services sector, reduced GDP by 0.10 per cent in Brazil, 0.55 per cent for China, 0.48 per cent in the European Union, and 0.58 per cent in South Korea.
  - According to a 2018 Asia Cloud Computing Association report, data localisation and other barriers to data flows impose significant costs, reducing India’s GDP by 0.7 per cent to 1.7 per cent, Indonesia’s GDP by 0.5 per cent, and Vietnam’s GDP by 1.7 per cent.<sup>142</sup>
- For MSMEs, compliance-related cost effects are compounded as small companies typically lack the capital to invest in IT hardware and storage necessary to comply with data localisation schemes. A Leviathan Security group study shows that data localisation measures raise the cost of hosting data by 30-60 per cent.<sup>143</sup> This reduces capital allocations that might otherwise go towards investment in new inventions or innovative capacities of the company. MSMEs that utilise cross-border technologies, such as the internet to trade on global platforms, have a survival rate of 54 per cent, which is 30 per cent higher than that of offline businesses.<sup>144</sup> Restricting data flows prevents or limits MSMEs from accessing global markets and global capital.
- According to a 2015 report on quantifying the cost of forced localisation,<sup>145</sup> data localisation would cause cloud services to be more expensive in several markets:
  - If the European Union enacted data localisation, companies would have had to pay up to 36 per cent more to use higher end cloud servers (4GB and higher).
  - If Brazil had enacted data localisation as part of its “Internet Bill of Rights” in 2014, companies would have had to pay an average of 54 per cent more to use cloud services (of all categories) from local cloud providers compared with the lowest worldwide price. For example, for 1GB equivalent services Brazilian customers would have had to pay 37.5 per cent more, while for 2GB services the increase would be 62.5 per cent.
- A 2016 study by the European Centre for International Political Economy (ECIPE) shows that data localisation measures in the EU may cause losses in the GDP from -0.27 per cent to -0.61 per cent. The losses in the communication sector are greater where the losses were as high as -3.46 per cent.<sup>146</sup>

142 Asia Cloud Computing Association, “Cross-Border Data Flows,” 14, 28 and 57.

143 Leviathan Security Group, “Quantifying the Cost of Forced Localisation” (2015), <https://static1.squarespace.com/static/556340ece4b0869396f21099/t/559dad76e4b0899d97726a8b/1436396918881/Quantifying+the+Cost+of+Forced+Localization.pdf>, 3.

144 World Economic Forum, “Cross-border data flows, digital innovation and economic growth” (2016), <http://reports.weforum.org/global-information-technology-report-2016/1-2-cross-border-data-flows-digital-innovation-and-economic-growth/#view/fn-17>.

145 Brendan O’Connor, “Quantifying the Cost of Forced Localization” (Leviathan Security Group, June 2015), <http://www.leviathansecurity.com/blog/quantifying-the-cost-of-forced-localization>.

146 Matthias Bauer, Martina F. Ferracane, Hosuk Lee-Makiyama, and Erik van der Marel, “Unleashing Internal Data Flows in the EU: An Economic Assessment of Data Localisation Measures in the EU Member States,” European Centre for International Political Economy (2016), II.

**gsma.com**



To download this report, visit [gsma.com/CrossBorderDataFlows](https://gsma.com/CrossBorderDataFlows)

**GSMA Head Office**

Floor 2  
The Walbrook Building  
25 Walbrook  
London EC4N 8AF  
United Kingdom  
Tel: +44 (0)20 7356 0600  
Fax: +44 (0)20 7356 0601

