



EXECUTIVE SUMMARY

Regional Privacy Frameworks and Cross-Border Data Flows

How ASEAN and APEC can Protect Data and Drive Innovation

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.¹

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.

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

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.

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

Technical options	Political options	Cross-regional adequacy options
Introduce APEC CBPR implementation measures into ASEAN framework	Get remaining ASEAN states in APEC to join CBPR	Rely on data protection authorities to broker MoUs
Develop formal equivalence mechanisms (MoU or MRA)	Extend APEC mechanisms to non-member countries	Introduce Binding Corporate Rules

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, 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.

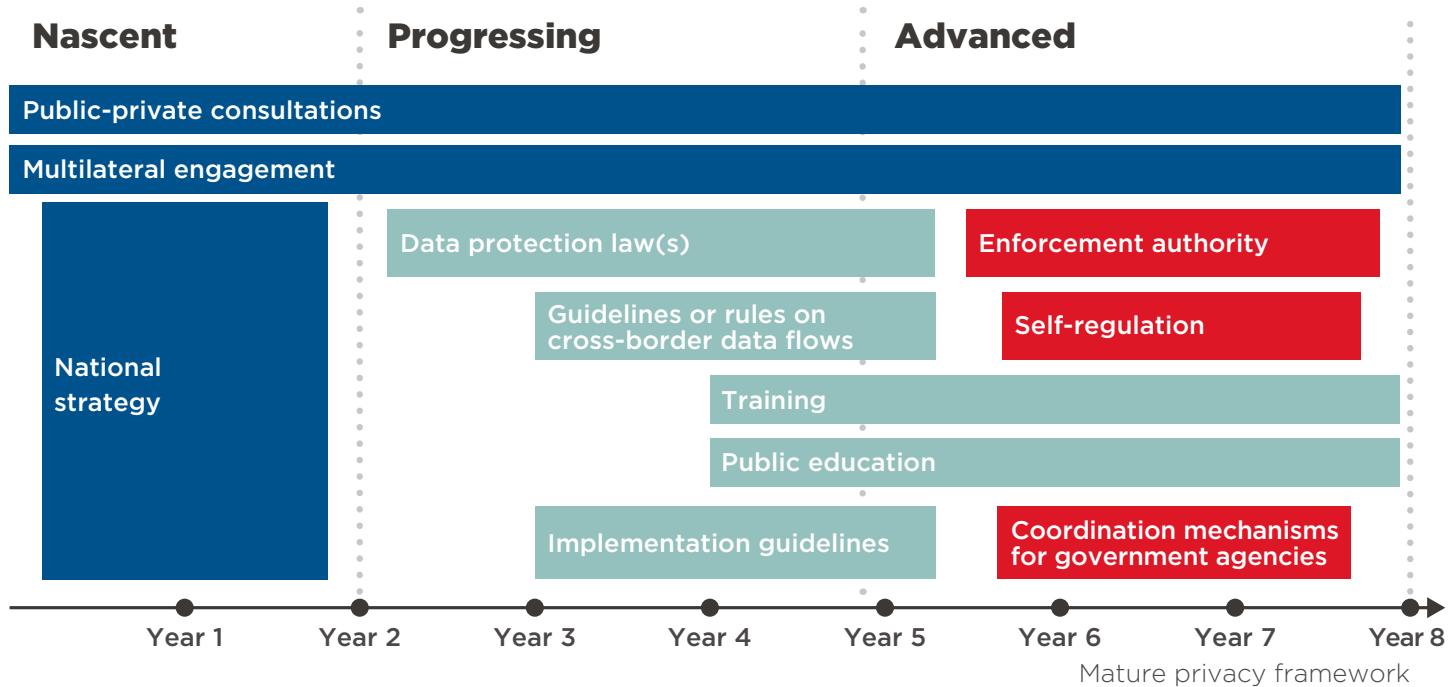
The first process is to understand where a country currently stands in terms of data privacy. This can be done by considering the various elements of a mature data privacy framework, and then checking to see which elements a country may already have in place and which ones it still may need.

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.