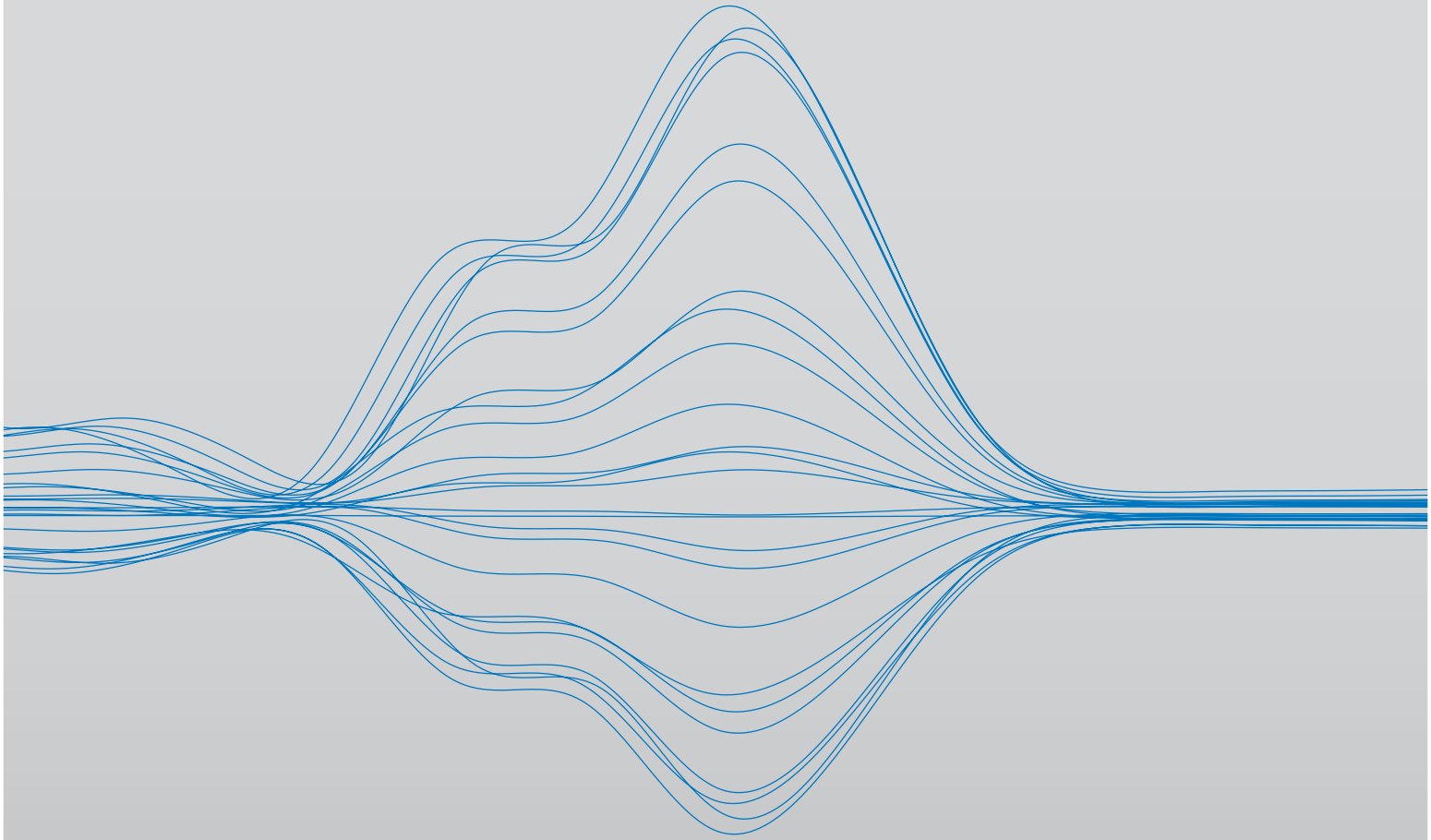
DATA PROTECTION GROUP

Practical Global Privacy



Data compliance in Asia: the localization and regionalization challenge

DLA PIPER

Data compliance in Asia: the localization and regionalization challenge

Is a pan-Asia approach to data protection possible? And how do you align regional compliance with your global data strategy?

Nowhere is the data protection landscape changing faster – and more fundamentally – than in Asia.

New laws have been introduced in Thailand, Sri Lanka, Brunei, Vietnam, Mongolia and Pakistan; and recent updates to regulations have come into force in Japan, Singapore and mainland China. Meanwhile, new laws are expected in Hong Kong, Malaysia, Australia and India.

In this rapidly evolving context, what should you know about how managing data in Asia jurisdictions, and how it can be moved across borders?

China tightens data laws

Data compliance teams will need to focus on mainland China in the coming months.

Asia's principal economic powerhouse has overhauled its data protection rule in recent years. Notably, this includes the Cybersecurity Law, Data Security Law and Personal Information Protection Law; and more recently, new rules on cross-border transfers of personal information and "important data".

Together, they govern how organizations treat and transfer mainland China data; how to access it from abroad; and how and where to store it.

The bad news is that they're more restrictive than many predicted – and they're not just for the tech giants. They affect most businesses with mainland China operations, even those without a presence in China. Most organizations will need to engage with the Cyberspace Administration of China (CAC – the local regulator) in some form or another. They'll also need to put in place (or renegotiate) their existing data processor agreements to include new standard contractual clauses. Understanding flows of personal and non-personal data will be key.

"China's new cross-border data transfer rules are tougher than expected – and not just for the tech giants."

Know the ins and outs

Conventionally, businesses have sought to unify their approach to data compliance across the region – and worldwide – as far as possible. Their aim being to drive efficiencies, and reduce the strain on their legal resources.

Yet Asia's unique data protection landscape throws up a number of problems in this regard:

- There's little harmonization between jurisdictions, with each imposing a different degree of data sovereignty. For example, some tolerate cross-border transfers, while others (like mainland China and Vietnam) require data to be stored in-country, or regulatory approval to transfer it overseas.
- Some data protection frameworks may look similar to the EU's GDPR legislation. But in practice, they're being interpreted, applied and enforced in different ways by different regulators across Asia. This is partly due to different cultural attitudes to data among consumers, businesses and governments in Asia compared to Europe and the US.
- There's more emphasis on consent in Asia. In Europe, for example, privacy notices are all that's needed to inform individuals of the intent to collect and process their personal data. But in Asia, you must gain the express consent of each individual before doing so.

  Given the cultural attitudes to data in Asia, this brings opportunities for organizations to do more with consumer data – in line with the consent given, of course, and within a compliant framework.

  In practice, however, that can be fiddly for global businesses, which must comply with different notice and consent requirements in different parts of the world.
- Many jurisdictions (including mainland China) regulate non-personal data. As such, compliance programmes in Asia must cover more than personal data.

At the same time, global data teams need to understand Asia's cultural relationship with data – and how it differs to that in Europe and the US.

"Culturally, consumers, business and governments in Asia have a different attitude to data compared to Europe and the US."

Consumers in Asia understand the value of their personal data, and don't typically see personal privacy as an absolute human right, as enshrined in law in Europe. They're more willing to share their data, in return for convenience or a more personalized experience.

The steps to follow

What does all this mean for organizations' data compliance programmes in Asia?

In our experience, there are five critical success factors:

1. UNDERSTAND THE REALITY ON THE GROUND

Don't rely on unofficial English translations of Asia laws.

Also, don't assume that laws similar to those in other jurisdictions will be interpreted, applied or enforced in the same way.

Make sure your data team understands:

- each local regulator's approach to enforcing the rules
- when engagement with regulators will, and won't, help manage the outcome of investigations

This knowledge can underpin a risk-based approach in each jurisdiction, based on the realities of local enforcement practice.

2. IDENTIFY THE OPPORTUNITIES

Data compliance should be aligned to your business and customers. Don't ignore opportunities to do more with data in Asia, based on differing cultural attitudes to data and a compliant, consent-based framework.

3. GET CONSENT RIGHT

Requesting consent in a way that works for each market will boost trust among your customers.

That means adapting not just the legalities, but also the language and tone, in each location. Including data compliance experts in the product-design journey is vital to that process.

4. INVEST IN LOCAL RESOURCE

A dedicated, regional data compliance function will be critical.

When putting this in place, keep in mind that data compliance is a multi-disciplinary exercise. Your team should include:

- senior decision-makers who can set regional compliance strategy
- technical experts in data protection law and compliance
- software engineers to design and implement the technology needed to operationalize compliance
- communications teams to convey your approach to data processing to regulators and the market

Also think about the data infrastructure assets you'll require. Is it worth setting up a local data lake, which can remain unpolluted by data from outside Asia?

> *"Dedicated, regional data compliance resource will be critical."*

5. FIND THE OPTIMAL TRADE-OFF

How far should you align your Asia data programme with your global compliance strategy and operations?

This is a crucial strategic trade-off. Closer global alignment will make life easier for your compliance team – and cost less. On the other hand, localization should mean more effective compliance, while giving you a more competitive, customer-focused edge in Asia.

A balancing act

Ultimately, the crux of global data compliance is a cost-benefit analysis. The right balance between local, regional and global will be different for each organization. The challenge is to find your ideal position, and equip your compliance function to deliver it.

> *"Global data compliance is a strategic trade-off between localization and global alignment."*

DLA Piper's Data Protection, Privacy and Security team can help you formulate and achieve your global data protection strategy, and optimize your compliance programme. Please get in touch to discuss how we can support your organization.

Carolyn Bigg
Partner
T +852 2103 0576
carolyn.bigg@dlapiper.com

Venus Cheung
Registered Foreign Lawyer
T +852 2103 0572
venus.cheung@dlapiper.com