CLIFFORD
CHANCE

APAC DATA REGULATORY THEMES AND STRATEGIES

— THOUGHT LEADERSHIP

JUNE 2024

APAC DATA REGULATORY THEMES AND STRATEGIES

Data regulation is rapidly developing across the Asia Pacific (APAC) region. Businesses need to understand how these regulations will affect their strategies and how to balance mitigating risk with building consumer trust and fostering innovation. In this extract from a recent Clifford Chance webinar, we explore data transfers and localisation, cybersecurity and the latest regulatory developments and enforcement trends in APAC.

Different jurisdictions, different approaches

Jurisdictions across the APAC region are embracing disruptive technologies such as AI. However, this poses new challenges and risks around cybersecurity and data privacy; as a result, some of these countries are adopting comprehensive cybersecurity regulation and data protection laws including data breach notification requirements and restrictions on transfer. “In India and in Vietnam, comprehensive data protection laws were passed last year. The Vietnamese government has since unveiled a strategy to position Vietnam as a digital nation by 2030 and further data laws will emerge soon,” says Stella Cramer, a Clifford Chance Partner based in Singapore who leads the firm's APAC Tech Group. Thailand has issued two new notifications this year under its existing data protection law, which regulates cross-border data transfers, and Singapore is in the process of amending its Cybersecurity Act which will expand the types of entities regulated by the Cybersecurity Agency to include digital information infrastructure providers amongst others. “As a result, there will be additional requirements on incident response and in respect of cybersecurity standards and requirements amongst others,” she adds.

The importance of data mapping and oversight

“Data is a very valuable asset and where that data is located and how it is transferred are an important part of wider data strategies for our clients,” says Clarice Yue, a Clifford Chance Counsel based in Hong Kong. The data lifecycle consists of five stages: data collection, data storage, processing transfers, retention and destruction, and the questions that organisations need to consider at each stage include:

- Where is the data collected from? Is it directly from individuals or indirectly through third parties? Is it collected online or offline? Is it collected in one or multiple locations?
- Where is the data stored? Is it on-premise or in the cloud? Is it stored by the client or a third-party service provider? Is it stored in one or multiple locations?
- How is the data processed? Is it processed by the client or a third-party processor? Is it processed for the original purpose or a new purpose? Is it processed in one or multiple locations?
- How is the data transferred? Is it transferred within an organisation or to external parties? Is it transferred to controllers or processors? Is it transferred within the same jurisdiction or across borders? Is consent required for the transfer?
- How is the data retained and destroyed? Is it retained for the minimum necessary period or for longer? Is it destroyed securely or in a way that allows recovery? Is it retained or destroyed in one or multiple locations?

“Unlike Europe, APAC does not have one consolidated and overarching piece of data regulation like the GDPR. Instead, there is a broad spectrum

of laws and regulations around the region with different varying degrees of restrictions relevant to data transfers and data localisation. That is why, in terms of mapping the data flows, it is important to consider the relevant laws and regulations," says Yue.

Cross-border data transfer restrictions

"Cross-border transfer restrictions are one of the most critical issues for companies formulating data strategies in the region," says Yue. The legal landscape is evolving rapidly and the requirements for transfers vary depending on the types of data, the recipient (and where the recipient is located) and the circumstances of transfer. Most jurisdictions in APAC have transparency requirements for data transfers that require data controllers to notify the relevant individuals of who they might transfer data to and where the recipients might be located. "In terms of the more fluid requirements for cross-border transfers, they are very broadly divided into two extremes," Yue adds. There are jurisdictions that require consent as a requirement for cross-border transfers. These include, for example, South Korea and Mainland China – although Mainland China now places greater emphasis on adequacy requirements, which is the other extreme and are more common in other APAC jurisdictions. Adequacy requirements refer to whether the recipient provides an adequate level of protection for the personal data that is transferred to them. Different jurisdictions have different ways of determining and enforcing adequacy. Some jurisdictions, such as Hong Kong and Thailand, adopt a whitelist approach, where the government lists the countries that are deemed to have adequate data protection laws or standards. However, neither Hong Kong nor Thailand have published their whitelist yet, although they have the legal mechanisms to do so. India takes the opposite approach and has a blacklist.

Many jurisdictions require standard contractual clauses (SCCs) to ensure data protection when transferring data across borders. Hong Kong, for example, has model contractual clauses that are recommended but not mandatory, as Section 33 of its Personal Data Privacy Ordinance (PDPO) is not yet in force. Mainland China and Hong Kong also have a special arrangements in respect of data transfers within the Greater Bay Area (GBA), which involves a different set of SCCs that are more lenient than the broader SCCs applicable for transfers outside of Mainland China. "It simplifies the transfers of data from China to Hong Kong, whilst Hong Kong companies are encouraged to do the same when transferring data to the GBA and to China," says Yue.

What's the position on data transfer in Singapore, Indonesia and Vietnam?

"In Singapore, there are no strict data localisation rules," says Sian Smith, a Clifford Chance Senior Associate based in Tokyo. "An organisation can transfer personal data overseas provided that it has taken appropriate steps to ensure that the recipient of that data is bound by legally enforceable obligations to provide that data with comparable protection to what is required under Singapore's Personal Data Protection Act (PDPA)." Indonesia takes a similar approach: an organisation may transfer personal data outside of Indonesia if it has ensured that the recipient country has protection equivalent or higher to that of Indonesia's Personal Data Protection Law. Vietnam is taking a more onerous approach to data transfers and organisations need to undertake a transfer impact assessment before any transfers of personal data can be made from Vietnam. These assessments must include comprehensive information, including the objectives, types of data, security measures, consents from data subjects and mitigation methods implemented with regards to the data transfer. The assessment must be filed with the regulator within 60 days of processing and the Vietnamese Ministry of Public Security has powers to stop data transfers in certain situations.

India's blacklisting approach

India has passed its first comprehensive data protection law – the Digital Personal Data Protection (DPDP) Act – but it has yet to be implemented. “It takes an interesting approach to regulating data transfers and has opted for blacklisting, which means that there will be a limited set of countries to which data transfers will be restricted,” says Arnav Joshi, a London-based Senior Associate. “It's not clear yet whether it's going to be a blanket restriction, we expect some rules around that later this year,” he says. “And we expect that there will be special rules in relation to transfers of sensitive forms of data such as health and financial information data anywhere in the world, with the minimum guarantee of the same standard as is applicable under Indian law.”

The Chinese perspective

“In China, there is a great deal of legislation, rulemaking and enforcement activity around data. Its data laws not only focus on the privacy of individuals, but also on national security. Data is considered as a strategic asset and an important resource for economic activities,” says Kimi Liu, an international Partner at Shanghai-based law firm He Ping, who was a guest speaker. Chinese regulators have very strict controls about cross-border data transfer. “However, when China implemented regulations last year on security assessments and SCCs, it received thousands of applications and now has a backlog. As a result, China has taken the practical step of introducing several exemptions to cross-border data transfers, which means that provided there is no personal information or important data involved in the transfer, regulators will not intervene.” Regulators will also not intervene where data is collected from outside China, processed within China and then exported after processing, provided it does not include any onshore data or important data. Where data transfer is necessary for executing and performing a contract, an exemption is also available in some cases. “I think a typical scenario will include cross-border e-commerce, cross-border delivery and cross-border payments and remittances, for example, airline tickets and hotel reservations,” he says.

An important exemption focuses on human resources. If the data concerns employees' personal information, and if the processing and cross-border data transfer are in response to genuine demand for human resources management under internal labour policies that are formulated in accordance with law, and if the data does not include any important data, the cross-border data transfer can benefit from the exemption. “This exemption is very important for many multinational companies that operate in China,” Liu says.

Another exemption is based on the quantity of data transferred – this allows data processors to transfer data overseas if they are not critical information infrastructure operators, do not transfer sensitive personal information, and keep their volume below 100,000 records per year. “These key exemptions will help reduce much of the complex burden on data processors,” he says.

Data storage

A major question for companies is for how long should data be kept and where it should be located. That depends on data protection laws, local laws, industry requirements and business needs. “In APAC, not many jurisdictions have mandatory data localisation requirements, although Vietnam and China do,” says Clarice Yue. Vietnam imposes a data localisation requirement on certain entities to store data within the country and that data must be stored for at least 24 months upon notification from a competent authority.

In China, data localisation is viewed as a matter of national security. Two types of institutions need to consider data localisation: Critical Information Infrastructure Operators and data processors who process personal information beyond a certain threshold, currently 1,000,000 records, although this might be increased in the future. “Another important concept in China is 'important data'," says Kimi Liu. “The ambiguity of the definition of 'important data' has caused a lot of issues. However, the cyberspace regulator recently confirmed

that there will be an identification process which will help to clarify matters," he says.

What else do companies need to consider when setting their data strategies?

- Following a comprehensive data mapping exercise assessing what data is held by the organisation and where (including personal data, commercial information and other confidential and sensitive information) it is then important to conduct a comprehensive regulatory review across the various countries in which the organisation operates or in which it is looking to transfer or store data. That review will set out the legal risks of holding data in those countries.

- The next step is both to produce and implement policies and controls to ensure that data is handled in accordance with those applicable laws as well as being aligned with the organisation's internal risk appetite.

- Another important consideration is what does the organisation want to do with its data and how that will impact the strategy? Questions organisations should ask include: How is the data categorised? Who owns each dataset? Will it be licensed to any third parties? If so, who and where and what rights will they have to use that data, and is it regulated? And finally, what technologies does the company want to use with that data? Will it be running AI through it? If so, what is the position around AI governance and regulation in the relevant countries, and are there any other technology-specific rules to be aware of?

"These sorts of questions are helpful to ask as early as possible in the process to be able to structure the relevant projects and to minimise, compliance issues upfront," says Sian Smith.

Cybersecurity notification regimes across APAC

"Across the region we are seeing increased scrutiny around cybersecurity and operational resilience, and this has resulted in the expansion of data breach notification obligations," explains Sian Smith. In India, for example, under the Digital Personal Data Protection Act (DPDP), organisations must notify the India Computer Emergency Response Team (CERT-In) within six hours of a data breach. "Until now, there has been very little by way of enforcement and penalties in India," says Arnav Joshi. "That is about to change significantly with rigorous obligations for cybersecurity breach reporting and no threshold for the severity or impact of the incident, so we may see significant numbers of incidents beginning to be notified. I think we can expect huge compliance uplifts for organisations working in or with India as processors – the penalty for non-reporting of breaches is up to US$24 million per instance."

By contrast, Hong Kong does not yet have a mandatory data breach notification regime. Currently, the Office of the Privacy Commissioner for Personal Data (PCPD) encourages voluntary notification, and many companies do notify the PCPD in the event of breaches and incidents. "But we anticipate that this will change as the PCPD is being revamped – although there is no timetable for that yet," says Clarice Yue. "Hong Kong also does not have a cybersecurity law. However, a bill is currently on the agenda for the Legislative Council in July 2024. So potentially more stringent requirements in relation to protection of cybersecurity for critical information infrastructure operators may be introduced."

In Mainland China, the rules for a cybersecurity breach are less clear than in some other jurisdictions. In 2023 it issued detailed rules for the reporting of cybersecurity breaches for public comments and, given that the regulator has taken steps to address cross-border data transfer, it's likely that the focus will now shift to other areas including cybersecurity breach notification. "This will be a very important area to watch out for in the year ahead," says Kimi Liu.

CONTACTS

Stella Cramer
Partner
Singapore
T: +65 6410 2208
E: stella.cramer@cliffordchance.com

Clarice Yue
Counsel
Hong Kong
T: +852 2825 8956
E: clarice.yue@cliffordchance.com

Sian Smith
Senior Associate
Tokyo
T: +81 3 6632 6320
E: sian.smith@cliffordchance.com

Arnav Joshi
Senior Associate
London
T: +44 207006 1303
E: arnav.joshi@cliffordchance.com

CLIFFORD

CHANCE

www.cliffordchance.com

Clifford Chance, 10 Upper Bank Street, London, E14 5JJ

2405-011281