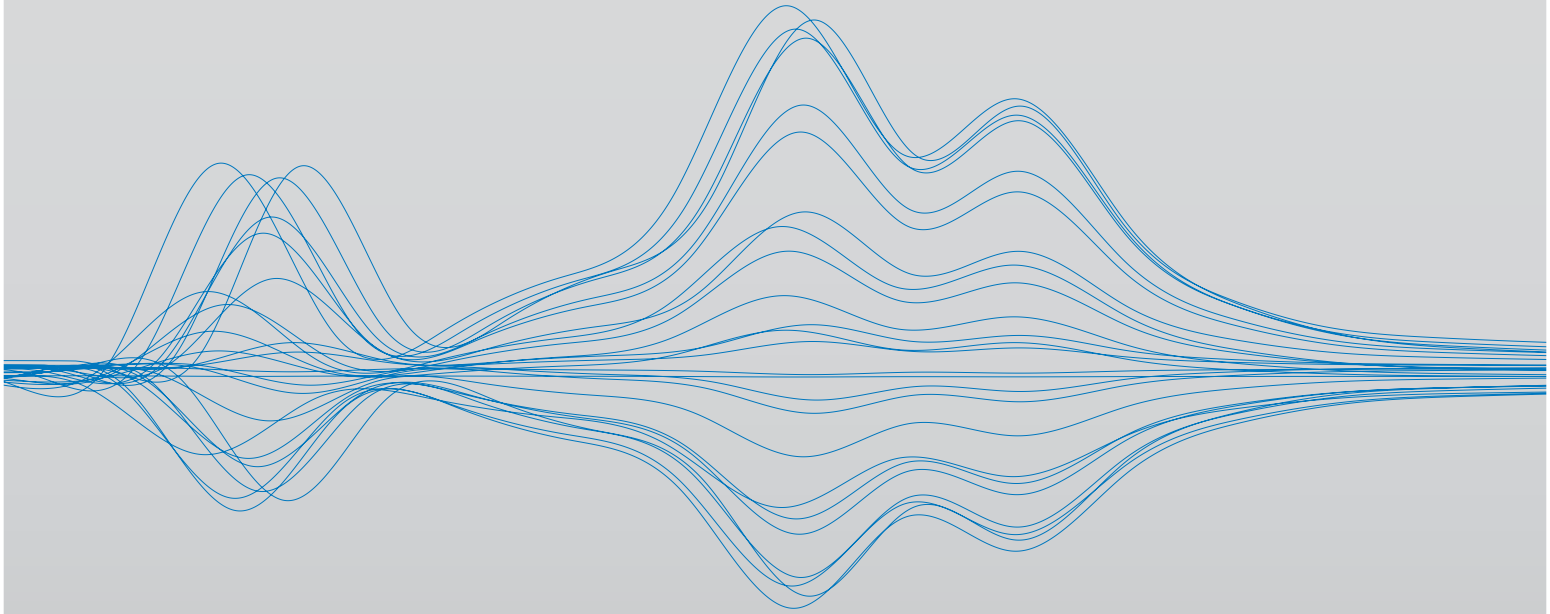
DECEMBER 2021

# SEAChange



DLA PIPER

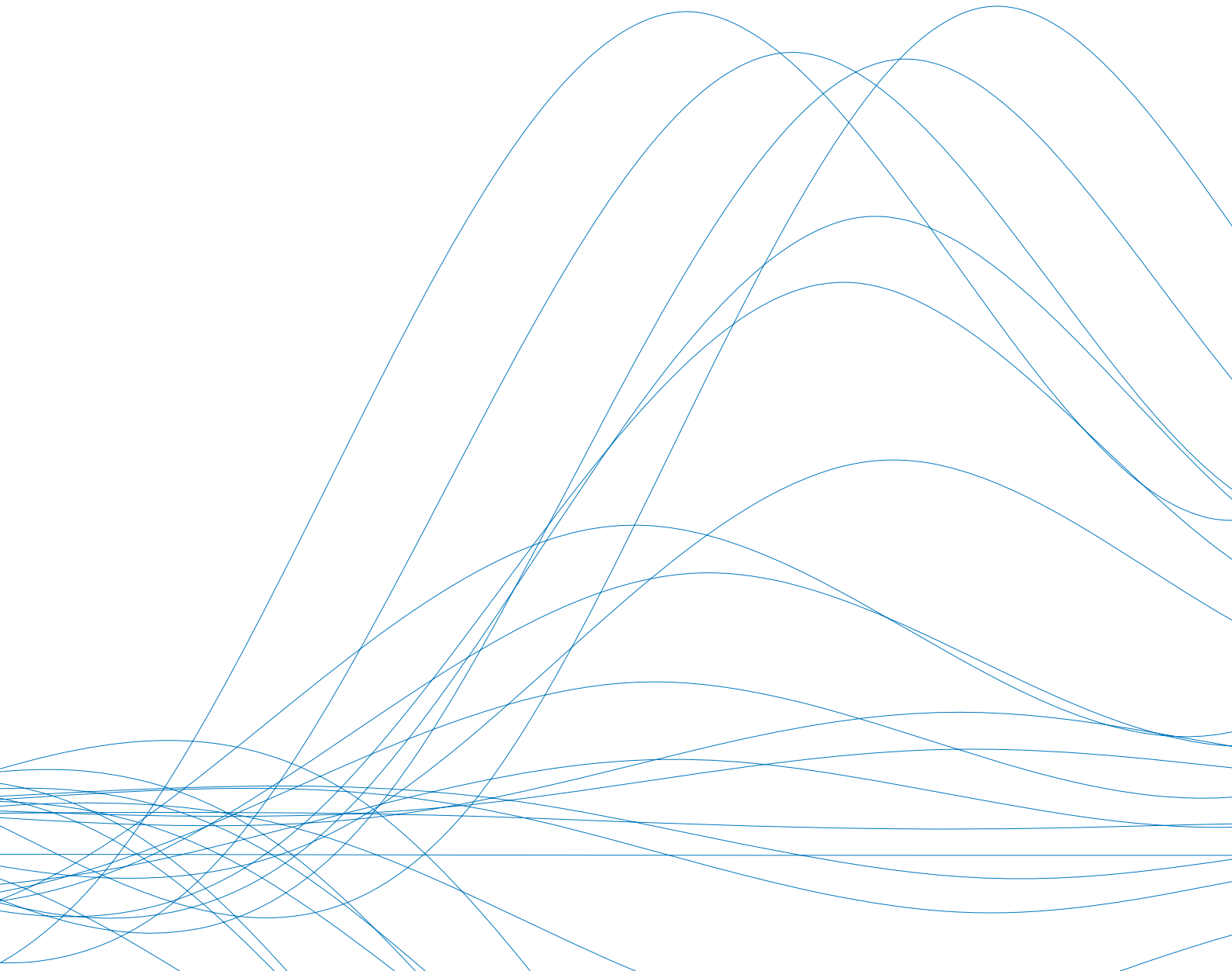
# Contents

# SEAChange – investigations, compliance, and regulatory developments in Asia

Our second issue focuses on a varied set of regional updates, cutting across areas of data protection, cybersecurity, and the environment. Data protection and cybersecurity concerns remain a focus of legislators and enforcement agencies across Asia.

In this issue we cover:

- Challenges and implications for corporates in handling cross-border investigations with a nexus to China as a result of China's new Personal Information Protection Law;
- The impact of Thailand's newly-issued notification on private entities pursuant to its Cyber Security Act;
- The hefty compliance requirements arising from India's Data Protection Bill which has been inspired by the EU's GDPR; and
- Indonesian courts taking a tougher stance in holding the government and its representatives liable for environmental failures.



# Navigating Through Uncertainty: New Challenges of Conducting Cross-border Investigations under China's Personal Information Protection Law

By Christine Liu and John Zhang

China's Personal Information Protection Law **("PIPL")** came into effect on November 1, 2021. With an array of obligations and liabilities imposed, the PIPL's omnibus restrictions on the collection, use, and transfer of personal information will complicate the cross-border investigations for multinational companies doing business in China, adding legal and regulatory challenges for businesses that are striving to comply with both China and foreign privacy laws.

The PIPL has extra-territorial effect and applies to data processing activities within China and processing Chinese residents' data outside of China. The fact that a business has no subsidiary or presence in China does not necessarily exempt it from the jurisdiction of the law.

Penalties on violating the PIPL can be severe. Viewed as the Chinese counterpart to the EU General Data Protection Regulation **("GDPR")**, the PIPL imposes administrative fines up to 5% of the company's annual revenue of the previous year or up to CNY 50 million (USD 7.8 million) for the most serious violations.

Notified consent remains the primary basis for processing data that contains personal information for an investigation. In addition, "separate consent" must be obtained if the data collected contains sensitive personal information such as financial accounts, medical health information, geographic location, and tracking data, or the data containing personal information needs to be transferred outside of the mainland China. The PIPL does not define "separate consent" or what form of "separate consent" constitutes valid consent. If the personal information is to be transferred across border, companies should also apply for personal information protection certification or to adopt contract template of the Cyberspace Administration of China **("CAC")** for data transfer.

Companies conducting internal investigations should take a risk-based approach when handling evidence that contains personal information of its China employees, customers, suppliers or other third-parties.

Simply relying on the "waivers" of obtaining notified consent from the data subject might be insufficient because it remains unclear whether conducting an internal investigation would constitute carrying out human resources management or performing a legal responsibility or obligation under the PIPL. A waiver might not be valid if the data contains personal information disclosed by the investigation subject on a "quasi-social media platform" such as WeChat Moment because it remains unclear whether such disclosure would be deemed as being disclosed to the public.

Once an investigation begins, obtaining separate and explicit consent from those who are under investigation becomes challenging. The data subject could withdraw their consent at any time, which might jeopardize the investigation. If the investigation turns out to go beyond its internal nature, provision of any personal information to foreign judiciary or law enforcement agency, such as the DOJ or SEC of the United States, requires approval of a designated Chinese authority.

Before clearer guidance is issued, companies conducting cross-border investigations should retain data processors located within the mainland China to collect, process and review employee's emails and financial transaction records stored in China. When in doubt, companies should avoid transferring data containing personal information outside of China through proper redaction and anonymization procedures.

# Are you Subject to Thailand's Cyber Security Laws? Know Your Rights and Obligations

By Santipap Dumprapai, Prin Laomanutsak, Sammy Fang, Rishikeesh Wijaya

Thailand's Cyber Security Act B.E. 2562 (2019) **(the "CSA")** came into effect on 28 May 2019. The CSA imposes a variety of obligations upon public and private organizations which are considered "Organizations of Critical Information Infrastructure" **("OCII")** i.e., an organization, either public or private, which provides "Critical Information Infrastructure" **("CII")** services.

Up until recently, the ambiguity as to whether a service provider was considered an OCII remained a live issue, requiring further clarity. In an attempt to provide clarity, on 23 August 2021, the CSA's regulator (i.e., the National Cybersecurity Committee **("NCC")**) issued a **"Notification"**[1] which systematically categorizes specific types of businesses into CII service-providers, and delegates supervisory authority to different regulators **("Supervising Organizations")**.

A list of selected CII services under Thai law may be found here.

Key obligations of OCIIs under the CSA are as follows:

1. Observing compliance with the CSA Code of Practice and standard framework for maintenance of cybersecurity.
2. Examining operations to ensure compliance with the minimum cybersecurity standards prescribed by the relevant Supervising Organization.
3. Conducting annual risk assessments on "Maintaining Cybersecurity." These risk assessments should be conducted by the OCII's information security auditor, internal auditor or external independent authority, and the results must be submitted to the Office of the NCC.
4. Upon learning that it is a subject of a "cyber threat", the OCII must report to the Office of the NCC and the relevant Supervising Organization. The OCII must then carry out appropriate investigations and examinations relating to the "cyber threat."

The obligations imposed on OCIIs are in some ways aligned with those of other jurisdictions such as Singapore and China, as seen here.

OCIIs are also subject to the jurisdiction of the Office of the NCC, should there be a "cyber threat" that reaches a "critical level." Among other obligations in the context of a "cyber threat", OCIIs will be required to cooperate during a dawn raid, respond to requests for information as well as respond to subpoenas for information, evidence, or witnesses.

An OCII's failure to comply with obligations under the CSA will result in fines. However, a failure to cooperate with orders issued by the Office of the NCC may result in a fine and/or imprisonment. Notably, offences under the CSA may extend to a director and/or person responsible for the operation of an organization, if it is established that the commission of the offence was a result of an order or omission of such person(s).

Furthermore, private organizations subject to a "cyber threat" resulting in a data leak may be subjected to reporting obligations under Thailand's Personal Data Protection Act B.E. 2562 (2019), which is scheduled to come into effect on 31 May 2022, should such an organization be considered a "Data Controller" under that law.

[1] NCC Notification Re Characteristics of Organization with a Mission or Service to Provide CII and Delegation of Supervision Authority B.E. 2564 (2021)

# Privacy by design – India gears up for an overhaul of its data protection laws

By Apoorvaa Paranjpe

## Background

India is on the anvil of a comprehensive overhaul of its current data privacy regime once the Personal Data Protection Bill, 2019 **("Bill")** is enacted. The recent spate of serious data breach incidents in India, exacerbated by home working, made the introduction of the new data framework timely and highly anticipated.

## Highlights of the Bill

The Bill is inspired by the European Union General Data Protection Regulations **("GDPR")** but also introduces **novel provisions** making it a unique legislation. Consequently, compliance with GDPR would not necessarily mean compliance with the Bill.

### *APPLICABILITY*

The Bill proposes to apply to personal data[1] that has been processed within the territory of India by the Indian government, any company or entity incorporated in India and foreign companies dealing with personal data of individuals in India provided certain nexus requirements are met.[2]

### *SUPERVISING AUTHORITY*

The Bill contemplates creation of a Data Protection Authority **("DPA")** entrusted with wide-ranging rule-making, administrative and quasi-judicial functions.

### *OBLIGATIONS OF DATA FIDUCIARIES*

The Bill imposes major compliance obligations on data fiduciaries[3] including providing data principals[4] with detailed notice (in multiple languages where necessary and practicable) prior to data collection and obtaining their valid consent; processing data only for a clear, specific and lawful purpose and in a fair and reasonable manner; retaining data only until the purpose of collection is completed and implementing measures to demonstrate transparency and accountability. If there is a breach while processing data which is likely to cause harm to the data principal, the data fiduciary is required to notify the DPA who may determine if the data principal should also be notified of such breach.

Significant data fiduciaries[5] must comply with additional accountability requirements including registration with the DPA, record keeping, appointment of a data protection officer, conducting data protection impact assessment prior to significant processing activities and independent data audits.

### *DATA LOCALIZATION AND CROSS-BORDER TRANSFERS*

The Bill mandates different localization rules for different categories of personal data. Sensitive personal data[6] may be transferred outside India for processing if expressly consented to by the individual and subject to certain additional conditions

---

[1] Personal data is defined as "*data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, whether online or offline, or any combination of such features with any other information, and shall include any inference drawn from such data for the purpose of profiling.*" (Section 3(28))

[2] The Bill is designed to have extra-territorial applicability if the processing of data by foreign companies is "*(i) in connection with any business carried on in India, or any systematic activity of offering goods or services to data principals within the territory of India; or (ii) in connection with any activity which involves profiling of data principals within the territory of India.*" (Section 2(A)(c))

[3] Data fiduciary is defined as "*any person, including the State, a company, any juristic entity or any individual who alone or in conjunction with others determines the purpose and means of processing of personal data.*" (Section 3(13))

[4] Data principal is defined as "*the natural person to whom the personal data relates*" (Section 3(14))

[5] The DPA may notify any data fiduciary as a significant data fiduciary having regard to "*(a) volume of personal data processed;(b) sensitivity of personal data processed;(c) turnover of the data fiduciary;(d) risk of harm by processing by the data fiduciary;(e) use of new technologies for processing; and (f) any other factor causing harm from such processing.*" (Section 26(1))

[6] Sensitive personal data is defined as "*such personal data, which may, reveal, be related to, or constitute—(i) financial data; (ii) health data; (iii) official identifier; (iv) sex life; (v) sexual orientation; (vi) biometric data; (vii) genetic data; (viii) transgender status; (ix) intersex status; (x) caste or tribe; (xi) religious or political belief or affiliation; or (xii) any other data categorised as sensitive personal data under section 15.*" (Section 3(36))

but must continue to be stored in India. Critical personal data[7] can only be processed in India. Personal data that does not fall under the aforementioned categories is not subject to cross-border transfer restrictions.

*ENFORCEMENT*

The Bill envisages enforcement through civil compensation to individuals for harm suffered as a result of infringement, financial penalties which may extend to the higher of approximately USD 2 million or 4% of the total worldwide turnover of the data fiduciary and criminal penalties (fines and/or imprisonment for 3 years) for re-identifying de-identified data without appropriate consent.

## Comment

India is an important player in the global data economy. The Bill has implications for investors and businesses particularly in data-intensive sectors like software, education, pharmaceutical, health care and banking.

Interesting times lie ahead as we await the final form of the Bill which may undergo further changes before enactment. Watch this space for further updates.

## Major differences between the Personal Data Protection Bill, 2019 & GDPR

| TOPIC | GDPR | BILL |
|---|---|---|
| Processing data | The legal bases on which personal data may be processed are (a) consent of the data subject (b) performance of contract to which the data subject is party (c) compliance with legal obligation of data controller (d) protecting vital interests of data subject (e) performance of a task carried out in the public interest (f) legitimate interests pursued by the controller or third party (Article 6(1)) | The legal bases on which personal data may be processed are (a) consent of data principal (b) compliance with legal obligation (c) medical emergency involving a threat to the life or a severe threat to the health of the data principal or any other individual (d) medical treatment or health services to any individual during an epidemic, outbreak of disease or any other threat to public health (e) measures to ensure safety of, or provide assistance or services to, any individual during any disaster or any breakdown of public order (f) employment purposes (g) such reasonable purpose as specified by regulations to be notified by DPA (Sections 11 - 14)<br><br>Significantly, performance of a contract and legitimate interests basis are not grounds for processing data without consent. Organisations rely on these two grounds for a wide range of activities which require consent under the Bill. |
| Registration of significant data fiduciaries | No requirement for registration | Significant data fiduciaries are required to register with the DPA as per the regulations (Section 26(2)) and comply with greater additional accountability requirements |
| Data localisation | There is no data localization requirement | Sensitive personal data must be stored in India but may be transferred outside India if there is explicit consent and if transfer is part of a DPA-approved contract or intra-group scheme for transfer or if the Indian government has deemed a country or class of entities to be providing adequate protection (Section 34(1)). Critical personal data must be processed only in India, except under emergency situations or where the Indian government approves (Section 34(2)) |
| Anonymized data | Anonymized data falls outside the scope of GDPR. | The Indian government may, in consultation with the DPA, direct any data fiduciary to provide anonymized data "*to enable better targeting of delivery of services or formulation of evidence-based policies*" (Section 91(2)) |

[7] Critical personal data is defined as "*such personal data as may be notified by the Central Government to be the critical personal data.*" (Section 33(2))

# Clearing the Air: Indonesian Courts Decide to Hold Officials Liable for Jakarta's Air Pollution

By Ahmad Aji Sukma

On September 16, 2021, the District Court of Central Jakarta released its judgment on a lawsuit concerning air pollution in Jakarta. Following extensive legal proceedings and delays, the court found that various branches and representatives of the Indonesian government, including the President, the Minister of Environment and Forestry, the Ministry of Home Affairs, the Health Minister, and the Governors of Jakarta, West Java and Banten, are liable over Jakarta's chronic and notorious air pollution.

Legal proceedings began in July 2019 when the civil alliance submitted its class action, arguing that Indonesian officials violated Law 32 of 2009 on Environmental Protection and Management. The plaintiffs in this class action specifically argued that Indonesian officials failed to undertake immediate measures in addressing Jakarta's air pollution crisis, which has resulted in escalating health concerns for Jakarta's citizens.

We anticipate that this decision will create a notable precedent. Specifically, this ruling will likely inspire plaintiffs to bring other civil claims against public officials, state-owned companies and/or private sectors in the future, specifically in relation to environmental claims. Consequently, this decision will likely have a significant impact on businesses and investments in Indonesia – which foreign investors and companies operating in Indonesia should be aware of. Industries that are fossil-fuel intensive, or involve intense infrastructure development, high carbon-emissions, agriculture, large waste incineration, and other forms of extensive construction may potentially be subjected to claims (including class-action lawsuits) by affected communities and NGOs.

Based on the court's decision, the Indonesian government will likely set high environmental standards, and tighten thresholds relating to air quality, carbon emissions, and more broadly, environmental compliance frameworks.

Based on our review of the judgement, there are some key takeaways for foreign investors and corporates operating in Indonesia:

- Foreign entities seeking to invest or operating in extractive and manufacturing sectors should be aware of environmental risks and potential liability. Adequate risk-based due diligence (e.g., through environmental impact assessments) should be conducted pre-transaction and periodically. Such due diligence should be in line with relevant Indonesian law, including Indonesia's latest Omnibus law.
- Undertaking adequate insurance (with appropriate coverage) that ideally should cover such bases of liability as they relate to environmental issues.
- Broadly, strengthening environmental, social, and governance ("**ESG**") frameworks to identify and mitigate the risks related to environmental degradation and human rights issues (e.g., impact of projects on indigenous communities) in Indonesia. In so doing, investors and corporates will be taking pre-emptive action to mitigate any reputational and litigation risk litigation which may arise in the future.

# Authors


**Christine Liu**
Partner
+852 2103 0668
Christine.liu@dlapiper.com

**Sammy Fang**
Partner
+852 2103 0649
sammy.fang@dlapiper.com

**John Zhang**
Consultant
+861085200791
john.zhang@dlapiper.com

**Apoorvaa Paranjpe**
Senior Associate
+65 6512 9595
apoorvaa.paranjpe@dlapiper.com

**Santipap Dumprapai**
Senior Associate
+66 2 686 8532
santipap.dumprapai@dlapiper.com

**Ahmad Aji Sukma**
Associate
+442077966436
ahmad.aji.sukma@dlapiper.com

**Prin Laomanutsak**
Associate
+6626868562
prin.laomanutsak@dlapiper.com


## Key contact


**Maurice Burke**
Partner
+65 6512 9560
maurice.burke@dlapiper.com


## Editorial team


**Rishikeesh Wijaya**
Associate
+65 6512 9515
rishikeesh.wijaya@dlapiper.com

**Vekaneshvari Jayabal**
Paralegal
+65 6512 9518
vekaneshvari.jayabal@dlapiper.com