GIR KNOW HOW DATA PRIVACY & TRANSFER IN INVESTIGATIONS

Singapore

Farhana Sharmeen, Esther C. Franks and Gen Huong Tan
Latham & Watkins LLP

OCTOBER 2021

GIR

SCOPE OF DATA PROTECTION LAWS RELEVANT TO CROSS-BORDER INVESTIGATIONS

1. What laws and regulations in your jurisdiction regulate the collection and processing of personal data? Are there any aspects of those laws that have specific relevance to cross-border investigations?

The collection, use and disclosure of personal data in Singapore is regulated by the Personal Data Protection Act 2012 (PDPA) and associated subsidiary legislation, including the Personal Data Protection Regulations 2021. The Personal Data Protection Commission (PDPC) is responsible for administering and enforcing the PDPA.

Under the PDPA, the collection, use or disclosure of personal data typically requires an individual's prior informed consent. However, in the context of an investigation, companies may seek to rely on the legitimate interests exception. Under paragraph 3 of Part 3 of the First Schedule to the PDPA, companies are not required to seek an individual's consent if the collection, use or disclosure (as the case may be) of personal data about the individual is 'necessary for any investigation or proceedings'.

Under the PDPA, investigation means:

- a breach of an agreement;
- a contravention of any written laws of Singapore, or any rule of professional conduct or other requirement imposed by any regulatory authority in exercise of its powers under any written laws of Singapore; or
- a circumstance or conduct that may result in a remedy or relief being available under any law.

Under the PDPA, proceedings means any civil, criminal or administrative proceedings by or before a court, tribunal or regulatory authority relating to the allegation of:

- a breach of an agreement;
- a contravention of any written laws of Singapore or any rule of professional conduct or other requirement imposed by any regulatory authority in exercise of its powers under any written laws of Singapore; or
- a wrong or a breach of a duty for which a remedy is claimed under any law.

An organisation must not transfer any personal data to a country or territory outside Singapore unless it has taken appropriate steps to ensure that the overseas recipient is bound by legally enforceable obligations or specified certifications to provide the transferred personal data a standard of protection that is comparable to that under the PDPA.

2. What other laws and regulations, besides data protection laws, may prevent data sharing in the context of an investigation?

Companies should consider sectoral rules in Singapore that may prevent or restrict data sharing pertaining to an investigation. For example, in the context of licensed banks, banking secrecy in Singapore is governed by section 47 of the Banking Act (Cap. 19) (the Singapore Banking Act).

Banks and banking officers in Singapore cannot disclose customer information to any other person, except as expressly provided under the Singapore Banking Act. Parts I and II of the Third Schedule to the Singapore Banking Act specify the circumstances and conditions in which a bank can disclose customer information. For example, disclosures are permitted if they are necessary for the bank to comply with an order or request from a duly authorised Singapore police officer or public officer, with the purpose of providing information for an investigation or prosecution into alleged or suspected offences under written Singapore laws.

3. What constitutes personal data for the purposes of data protection laws?

Personal data protected by the PDPA only relates to personal data of natural persons. The definition of personal data is broad and includes 'data, whether true or not, about an individual who can be identified either from that data alone or from a combination of that data and other information to which an organisation has, or is likely to have, access'. However, key data categories are excluded from the definition, including:

- business contact information (information about an individual that the individual has not provided solely for their personal purposes, such as: name, position name or title, business telephone number, business address, business electronic mail address or business fax number and other similar information);
- personal data about an individual that is contained in a record that has been in existence for at least 100 years; and
- personal data about a deceased individual who has been dead for more than 10 years.

4. What is the scope of application of data protection laws in your jurisdiction? What activities trigger the application of data protection laws, to whom do they apply and what is their territorial extent?

The PDPA applies to organisations that have personal data in their possession or control and where they collect, use or disclose personal data.

Although the PDPA does not contain specific territorial provisions, the PDPC's Advisory Guidelines on Key Concepts in the PDPA (Revised 1 February 2021) provide that the obligations under the PDPA apply to organisations (whether or not they are in Singapore) carrying out activities involving personal data in Singapore. When personal data is collected overseas and transferred into Singapore, the PDPA will apply to any activities in Singapore involving that personal data.

Under the PDPA, a data intermediary is an organisation that processes data on behalf of another organisation, similar to a data processor under the GDPR, and is subject to fewer obligations than organisations under the PDPA.

5. What are the principal requirements under data protection laws that are relevant in the context of investigations?

Consent Obligation: A company is only allowed to collect, use or disclose an individual's personal data if the individual gives, or is deemed to have given, their consent for the collection, use or disclosure of that personal data. This obligation does not apply if the collection, use or disclosure of an individual's personal data is required or authorised under the PDPA, for example, under the legitimate interests exception, which includes where such collection, use or disclosure is necessary for 'any investigation or proceedings'.

Purpose Limitation Obligation: A company may only collect, use or disclose personal data about an individual: (i) for purposes that a reasonable person would consider appropriate in the circumstances; and (ii) if applicable, for purposes for which the company has informed the individual.

Notification Obligation: If a company intends to rely on consent to collect, use or disclose an individual's personal data, it must inform individuals of the purposes for which their personal data will be collected, used and disclosed.

Access Obligation: Individuals may request access to their personal data that is in the possession of or under the control of the company carrying out the investigation. The company is not required to provide such information if an exception applies, including if the information is subject to legal privilege, or if the investigation and associated proceedings and appeals have not been completed.

Protection Obligation: A company should make reasonable security arrangements to protect personal data in its possession or control, to prevent: (i) unauthorised access, collection, use, disclosure, copying, modification or disposal or similar risks; and (ii) the loss of any storage medium or device on which personal data is stored.

Retention Limitation Obligation: A company should cease to retain documents containing personal data, or remove the means by which the personal data can be associated with particular individuals, as soon as it is reasonable to assume that the purpose for which that personal data was collected is no longer served by retaining the personal data, and retention is no longer necessary for legal or business purposes.

Transfer Limitation Obligation: A company must not transfer any personal data to a country or territory outside Singapore, unless it has taken appropriate steps to ensure that the overseas recipient is bound by legally enforceable obligations or specified certifications to provide the transferred personal data a standard of protection comparable to that under the PDPA.

Data Breach Notification Obligation: Singapore has implemented a mandatory data breach notification regime, which requires data breaches to be notified to the PDPC if certain requirements and thresholds are met.

If a company has credible grounds to believe that a data breach has occurred (whether through self-discovery, alert from the public or notification by its data intermediary), the company is required to take reasonable and expeditious steps to assess whether the data breach is notifiable under the PDPA.

6. Identify the data protection requirements relevant to a company carrying out an internal investigation and to a party assisting with an investigation.

A company carrying out an internal investigation would likely be considered an organisation under the PDPA, and would therefore be subject to the PDPA's full requirements, including:

Consent Obligation. The company is allowed to collect, use or disclose an individual's personal data if the individual gives, or is deemed to have given, their consent for the collection, use or disclosure of that personal data. This obligation does not apply if the collection, use or disclosure of an individual's personal data is required or authorised under the PDPA, for example, under the legitimate interests exception, which includes if such action is 'necessary for any investigation or proceedings'.

Another specified legitimate interest may apply if the investigation relates to company employees and if the collection, use or disclosure of the personal data is reasonable for the purpose of 'managing or terminating the employment relationship' with the individual.

Purpose Limitation Obligation. The company may collect, use or disclose personal data about an individual only: (i) for purposes that a reasonable person would consider appropriate in the circumstances; and (ii) if applicable, for purposes about which the company has informed the individual.

Notification Obligation. If the company intends to rely on consent to collect, use or disclose an individual's personal data, it must inform individuals of the purposes for which their personal data will be collected, used and disclosed.

Access and Correction Obligations. Individuals may request access to their personal data, and may request corrections to their personal data, that is in the possession of or under the control of the company carrying out the internal investigation. The company is not required to provide or correct such information if an exception applies, for example if the personal data is in a document related to a prosecution, and if all proceedings related to the prosecution have not been completed.

Accuracy Obligation. The company should make a reasonable effort to ensure that personal data collected by or on behalf of the company is accurate and complete, if the personal data: (i) is likely to be used by the company to make a decision that affects the individual to whom the personal data relates; or (ii) is likely to be disclosed by the company to another organisation.

Protection Obligation. The company should make reasonable security arrangements to protect personal data in its possession or control, to prevent: (i) unauthorised access, collection, use, disclosure, copying, modification or disposal or similar risks; and (ii) the loss of any storage medium or device on which personal data is stored.

Retention Limitation Obligation. The company should cease to retain documents containing personal data, or remove the means by which the personal data can be associated with particular individuals, as soon as it is reasonable to assume that the purpose for which that personal data was collected is no longer served by retention of the personal data, and retention is no longer necessary for legal or business purposes.

Transfer Limitation Obligation. The company must not transfer any personal data to a country or territory outside Singapore, unless it has taken appropriate steps to ensure that the overseas recipient is bound by legally enforceable obligations or specified certifications to provide the transferred personal data a standard of protection comparable to that under the PDPA.

Data Breach Notification Obligation. Singapore has implemented a mandatory data breach notification regime, which requires data breaches to be notified to the PDPC if certain requirements and thresholds are met.

If the company has credible grounds to believe that a data breach has occurred (whether through self-discovery, alert from the public or notification by its data intermediary), the company is required to take reasonable and expeditious steps to assess whether the data breach is notifiable under the PDPA.

Accountability Obligation. The company should have internal measures in place to help meet its obligations under the PDPA. These include: (i) appointing a data protection officer; (ii) developing and implementing data protection policies and practices; and (iii) developing a process to receive and respond to complaints that may arise with respect to the application of the PDPA.

Data intermediaries

A party assisting with an investigation would likely be considered a data intermediary of the company carrying out the investigation.

A data intermediary is subject to a more limited set of obligations under the PDPA for the personal data it processes on behalf of a company, namely the Protection and Retention Obligations.

In addition, if a data intermediary has reason to believe that a data breach has occurred in relation to personal data that it is processing on behalf of the company carrying out the investigation, it must, without undue delay, notify the company of the data breach.

RIGHTS OF INDIVIDUALS

7. Is the consent of the data subject mandatory for the processing of personal data as part of an investigation?

No. A company could seek to rely on the legitimate interests exception.

Paragraph 3 of Part 3 of the First Schedule to the PDPA, refers to instances in which the collection, use or disclosure of personal data about an individual is 'necessary for any investigation or proceedings'.

Under the PDPA, investigation relates to:

- a breach of an agreement;
- a contravention of any written laws of Singapore, or any rule of professional conduct or other requirement imposed by any regulatory authority in exercise of its powers under any written laws of Singapore; or
- a circumstance or conduct that may result in a remedy or relief being available under any law.

Under the PDPA, proceedings means any civil, criminal or administrative proceedings by or before a court, tribunal or regulatory authority that relates to the allegation of:

- a breach of an agreement;
- a contravention of any written laws of Singapore or any rule of professional conduct or other requirement imposed by any regulatory authority in exercise of its powers under any written laws of Singapore; or
- a wrong or a breach of a duty for which a remedy is claimed under any law.

Another specified legitimate interest may apply if the investigation relates to company employees and if the collection, use or disclosure of the personal data is reasonable for the purpose of 'managing or terminating the employment relationship' with the individual.

PDPC guidelines suggest that, from an employer's perspective, monitoring how an employee uses company computer network resources and conducting audits on an employee's finance claims could fall within 'managing or terminating an employment relationship'.

8. If not mandatory, should consent still be considered when planning and carrying out an investigation?

Consent may still be considered when a company is planning an investigation. The company should determine whether an individual previously consented to the processing of their personal data for the purposes of internal investigations, for example, through on-boarding documents at the start of employment.

However, under the PDPA, individuals may at any time withdraw their consent in respect of the collection, use or disclosure of their personal data for any purpose. Parties cannot contract out of this right, which poses difficulties in the context of an investigation, and therefore it may be easier for the company to rely on a consent exception.

If an individual withdraws consent, employers may continue collecting, using or disclosing the personal data by relying on other PDPA exceptions, such as the necessary for any investigation or proceedings exception. Per section 16(4) of the PDPA, the organisation is not required to cease collecting, using or disclosing the personal data if such activities (without the consent of the individual) are required or authorised under the PDPA or other Singapore law.

If an investigation relates to certain offences such as money-laundering, drug-trafficking or corruption, the company should consider whether seeking consent from the relevant individual(s) might alert such individual(s) of the investigation, and whether this would constitute the tipping-off offence under section 48(1) of the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act.

9. Is consent given by employees likely to be valid in an investigation carried out by their employer?

Yes, provided that the employee is informed that the employers may collect, use or disclose their personal data for the purposes of investigations, on or before collection of the personal data, and the purposes set out are those that a reasonable person would consider appropriate in the circumstances.

This consent does not need to be specific and separate, and could be included alongside other processing activities in an employee-facing privacy policy.

Consent will not be valid if the organisation obtains or attempts to obtain consent by providing false or misleading information, or by using deceptive or misleading practices.

10. How can consent be given by a data subject? Is it possible for data subjects to give their consent to processing in advance?

The PDPC does not prescribe a specific form for obtaining consent. Typical methods for obtaining consent include asking the data subject to sign a consent form, or to acknowledge a privacy policy containing a description of the collection, use or disclosure of their personal data.

Data subjects can consent to the processing of their personal data in advance.

11. What rights do data subjects have to access or verify their personal data, or to influence or resist the processing of their personal data, as part of an investigation?

Data subjects may submit an access request to a company. However, companies are not required to accede to such requests if an exception from the Access Obligation applies. Exceptions to the Access Obligation that may be relevant in the context of an investigation include:

- opinion data kept solely for evaluation (including assessments of the suitability, eligibility or qualifications of an individual for employment, promotion, removal from employment or office, or for awarding of contracts, awards or other similar benefits);
- a document related to a prosecution if all proceedings related to the prosecution have not been completed;
- personal data that is subject to legal privilege;
- personal data that, if disclosed, would reveal confidential commercial information that could, in a reasonable person's opinion, harm the organisation's competitive position; and
- personal data collected, used or disclosed without consent for the purposes of an investigation if the investigation and associated proceedings and appeals have not been completed.

In addition, if an organisation has disclosed personal data to a prescribed Singapore law enforcement agency without consent, as authorised under the PDPA or other Singapore law, the PDPA requires that it must not inform the individual about such disclosure. This obligation does not extend to disclosures to foreign law enforcement agencies, though the organisation may refuse to disclose such information if another exception to the Access Obligation applies.

EXTRACTION, LEGAL REVIEW AND ANALYSIS BY THIRD PARTIES, INTERNATIONAL TRANSFER

12. Are there specific requirements to consider where third parties are appointed to process personal data in connection with an investigation?

Depending on the scope of work and the nature of the arrangement, such third parties may be considered the data intermediaries of the appointing organisation under the PDPA.

An organisation appointing such third parties should be aware that, if a data intermediary processes personal data on its behalf, the organisation is subject to the same personal data obligations under the PDPA as it would be if it processed the personal data itself.

The PDPC recommends that such organisations: (i) undertake an appropriate level of due diligence to ensure that a potential data intermediary is capable of complying with the PDPA; and (ii) emphasise in written contracts the scope of work that the data intermediary will perform on its behalf and for its purposes.

13. Is it permitted to share personal data with law firms for the purpose of providing legal advice?

Yes. A company may either obtain consent from the individual(s) involved or seek to rely on the legitimate interests exception. For example, if the collection, use or disclosure (as the case may be) of personal data about an individual is: (i) necessary for the provision of legal services by the organisation to another person, or for the organisation to obtain legal services; or (ii) necessary for any investigation or proceedings.

14. What is the position and status of law firms under data protection laws? Are law firms directly accountable for data processing under data protection laws, or is responsibility for processing by law firms shared between the law firm and the client?

Law firms do not have a specific or special status under the PDPA. Whether a law firm is directly accountable, or has shared responsibility with the client, is a fact-specific question that depends on whether the law firm is acting as (i) an organisation or (ii) a data intermediary.

If a law firm is processing data for its own purposes, and those purposes are outside the scope of the contract between the firm and the client, then the firm likely will be considered an organisation and will be required to comply with the full obligations of the PDPA.

If a law firm is processing data on behalf of a client for the purposes set out in a contract between the law firm and client, then the law firm likely will be considered a data intermediary and will only be subject to the Protection and Retention Obligations, and will need to notify the client of potential data breaches.

Under such arrangements, the client would have the same obligations under the PDPA in respect of personal data processed on its behalf by the law firm, as if the personal data were processed by the client itself.

15. What is the position and status of legal process outsourcing firms under data protection laws?

Assuming that a legal process outsourcing firm is processing data only on behalf of a client for the purposes of an investigation, the firm will be considered a data intermediary and will only be subject to the Protection and Retention Obligations.

Under such arrangements, the client would have the same obligations under the PDPA in respect of personal data processed on its behalf by the legal process outsourcing firm, as if the personal data were processed by the client itself.

16. Are there any additional requirements, beyond those specified above, that regulate the disclosure of data to third parties within your jurisdiction for the purpose of reviewing the content of documents, etc?

Companies should consider sectoral rules in Singapore that may regulate disclosure. For example, financial institutions in Singapore should comply with the Guidelines on Outsourcing issued by the Monetary Authority of Singapore, if the arrangement with the third party can be considered an outsourcing arrangement.

17. What rules regulate the transfer of data held in your jurisdiction to a third party in another country for the purpose of reviewing the content of documents, etc?

An organisation must not transfer personal data to a country or territory outside Singapore unless it has taken appropriate steps to ensure that the overseas recipient is bound by legally enforceable obligations or specified certifications to provide the transferred personal data a standard of protection that is comparable to that under the PDPA (the Transfer Limitation Obligation).

18. Are there specific exemptions, derogations or mechanisms to enable international transfers of personal data in connection with investigations?

For an organisation to transfer personal data outside of Singapore, the Transfer Limitation Obligation can be discharged in the following ways:

- Comparable law. The disclosing entity can assess and determine that it considers the recipient entity is subject to laws that are comparable to the PDPA and document this assessment.
- Data processing clauses. The recipient entity can execute data processing clauses requiring it to provide PDPA-equivalent protection to the transferred data. The PDPC has endorsed the ASEAN Model Contractual Clauses for Cross Border Data Flows (which is a similar concept to the European Standard Contractual Clauses) for such purposes.
- Consent. The disclosing entity can obtain consent from the relevant data subjects to transfer their personal data to the recipient entity outside Singapore. Prior to this consent, the disclosing entity must provide the data subject a reasonable summary in writing of the extent to which the personal data to be transferred to that country or territory will be protected to a standard comparable to the PDPA.
- Binding Corporate Rules (BCRs). If there are BCRs that apply to both the disclosing entity and recipient entity (similar in concept to the GDPR BCRs), then this could discharge the Transfer Limitation Obligation. The following conditions must apply:
    - The two entities must be related (ie, one controls the other, or both entities are under the control of a common person);
    - The BCRs must require every recipient of the transferred personal data to provide a standard of protection for the transferred personal data that is comparable to that of the PDPA; and
    - The BCRs must specify: (i) the recipients of the transferred personal data to which the BCRs apply; (ii) the countries and territories to which the personal data may be transferred under the BCRs; and (iii) the rights and obligations provided by the BCRs.
- Specified certifications. If the recipient entity holds a specified certification under the Asia-Pacific Economic Cooperation Privacy Recognition for Processors System or the Asia-Pacific Economic Cooperation Cross Border Privacy Rules System, as applicable, then the Transfer Limitation Obligation would be fulfilled.

TRANSFER TO REGULATORS OR ENFORCEMENT AUTHORITIES

19. Under what circumstances is the transfer of personal data to regulators or enforcement authorities within your jurisdiction permissible?

The transfer of personal data to regulators or enforcement authorities within Singapore is permissible if the organisation complies with the usual obligations under the PDPA.

An organisation seeking to transfer the personal data should ensure that: (i) the organisation has the individual's express or deemed consent for the transfer; or (ii) an exception applies that permits the disclosure of personal data without the individual's consent.

Possible exceptions:

- If the disclosure of personal data about an individual is necessary for any investigation or proceedings;
- If the disclosure of personal data about an individual is to an officer of a prescribed law enforcement agency (applicable if the organisation receives written authorisation signed by the head or director of that prescribed law enforcement agency or a person of a similar rank, certifying that the personal data is necessary for the purposes of the functions or duties of the officer)

The list of prescribed law enforcement agencies is set out under subsidiary legislation and includes the following Singapore authorities: (i) Casino Regulatory Authority of Singapore; (ii) Central Narcotics Bureau; (iii) Immigration & Checkpoints Authority; (iv) Internal Security Department; (v) Singapore Civil Defence Force; (vi) Singapore Police Force; (vii) Singapore Prison Service; and (viii) the Corrupt Practices Investigation Bureau.

Information-gathering powers of Singapore regulators and enforcement authorities

The PDPA provides that other Singapore legislation provisions shall prevail over the PDPA, to the extent that there are inconsistencies.

Accordingly, if an organisation: (i) receives a request or written notice from a Singapore regulator or enforcement authority requesting a transfer of personal data; and (ii) such request or written notice is made validly pursuant to powers granted to the Singapore regulator or enforcement authority under other Singapore legislation, then the organisation would not be able to rely on compliance with the PDPA as a sufficient reason for refusing such a request or written notice.

20. Under what circumstances is the transfer of personal data held within your jurisdiction to regulators or enforcement authorities in another country permissible?

Transferring personal data to regulators or enforcement authorities outside of Singapore is permissible if an organisation complies with the usual obligations under the PDPA.

An organisation seeking to transfer the personal data should ensure that: (i) the organisation either has the individual's express or deemed consent for the transfer; or (ii) an exception applies that permits the disclosure of personal data without the individual's consent.

While the PDPA stipulates that other Singapore legislation shall prevail over the PDPA to the extent that there are inconsistencies, this does not extend to foreign legislation or to the powers granted to non-Singapore regulators or enforcement authorities. Foreign regulators or enforcement authorities are also not considered prescribed law enforcement agencies, which benefit from a PDPA exemption.

Possible exceptions:

- If disclosing personal data about an individual is necessary for any investigation or proceedings (though the definitions restrict this exception in certain cases to contraventions of Singapore law, not foreign law).
- If the foreign regulator or enforcement authority seeks assistance from the Attorney General's Chambers under the Mutual Assistance in Criminal Matters Act or an applicable Mutual Legal Assistance Treaty.

An organisation is not required to notify the PDPC of personal data transfers to regulators or enforcement authorities in other countries.

21. What are some recommended steps to take on receipt of a request from a regulator for disclosure of personal data?

Organisations should take steps to verify that the request is legitimate and that the request is from the regulator that it purports to be from. For example, the PDPC has alerted the Singapore public to impersonation scams involving individuals pretending to be PDPC officers.

Recipients should check that the email address has the appropriate suffix and is from a Singapore government email address, or whether the sender and their email address is listed in the Singapore Government Directory, available here.

The recipients should then assess the legal basis for the request to ensure that the request is duly authorised under Singapore legislation.

ENFORCEMENT AND SANCTIONS

22. What are the sanctions and penalties for non-compliance with data protection laws?

The PDPC may require an organisation to pay a financial penalty of up to SG$1 million for non-compliance with the PDPA.

Following an update to the PDPA, this maximum penalty will be amended to be either SGD 1 million or 10 per cent of the organisation's annual turnover in Singapore, whichever is higher. This amendment will take effect on a further date to be notified, and no earlier than 1 February 2022.

The PDPC may also issue directions to an organisation to secure compliance with the PDPA, including to:

- stop collecting, using or disclosing personal data in contravention of the PDPA
- destroy personal data collected in contravention of the PDPA;
- prevent or reduce the possibility of harm (or further harm) to individuals who are (or may be) affected by the organisation's contravention; and
- pectify an organisation's processes, for example, by requiring the infringing organisation to take certain measures so that it will be brought into compliance with the PDPA.

Individuals may be criminally prosecuted in certain limited circumstances for the egregious mishandling of personal data, including:

- knowing or reckless unauthorised disclosure of personal data;
- knowing or reckless unauthorised use of personal data for a wrongful gain or a wrongful loss to any person; and
- knowing or reckless unauthorised re-identification of anonymised data.

Individuals found guilty of any of these offences are subject to a fine not exceeding SGD 5,000 or to imprisonment for a term not exceeding two years, or both.

RELEVANT MATERIALS

23. Provide a list of relevant materials, including any decisions or guidance of the data protection authority in your jurisdiction regarding internal and external investigations, and transfers to regulators or enforcement authorities within and outside your jurisdiction.

The authors are not aware of case law or specific guidance from the PDPC regarding internal and external investigations and transfers to regulators or enforcement authorities.

The PDPA is available here.

The PDPC's Advisory Guidelines are available here.

The list of published PDPC enforcement decisions is available here.

Farhana Sharmeen

Latham & Watkins LLP

Farhana Sharmeen is a partner in the Corporate Department of Latham & Watkins' Singapore office and heads the firm's Singapore law practice. Ms. Sharmeen primarily handles corporate (mergers and acquisitions, investment funds and debt capital markets) and finance (acquisition finance, structured finance and leveraged finance) transactions. Ms. Sharmeen also advises on general corporate matters, including regulatory compliance and corporate governance issues. She has particular experience representing clients in real estate, financial institutions, and the luxury goods industry.

Ms. Sharmeen is recognised as a leading lawyer for corporate M&A in Singapore by Chambers Asia-Pacific, which highlights her 'active public takeovers practice with expertise regarding fund formation and regulatory work'. In addition she is noted by The Best Lawyers in Singapore for her work in corporate law.

Esther C. Franks

Latham & Watkins LLP

Esther Franks is an associate in the Data & Technology Transactions and Data Privacy & Security Practices in the Singapore office of Latham & Watkins.

Ms. Franks primarily handles technology, data privacy and cybersecurity, intellectual property, and commercial law matters. She advises on complex commercial, technology, and intellectual property arrangements, including licensing and joint ventures, procurement, and outsourcing as well as on intellectual property matters, e-commerce, consumer protection, and data privacy and cybersecurity (including the PDPA and the GDPR) legislation.

Ms. Franks has a wide range of experience advising clients from various sectors, with a particular focus on AdTech, e-commerce and online services, health, technology, financial services and the entertainment industries.

Ms. Franks previously spent four years in Latham's London office, and she has worked in-house on secondment at a global social network focusing on data protection and cybersecurity as well as a major global retail company and a multinational consumer goods company, acting as legal counsel for the respective global procurement functions, focusing on technology-related procurement.

Gen Huong Tan

Latham & Watkins LLP

Gen Huong Tan is an associate in the Singapore office of Latham & Watkins. He advises clients on the full spectrum of corporate finance transactions, mergers and acquisitions, and technology, media and commercial transactions.

His technology, media, and commercial experience includes advising on: Fintech and payments, including payment processing, online payments, offline payments, mobile payments and electronic wallets; Data privacy and compliance, including coordinating data privacy advice across Asia-Pacific and GDPR compliance; E-commerce, advising online platforms on consumer protection in relation to e-commerce and preparing user terms and privacy policies. Mr. Tan trained in the firm's Singapore and London offices.

Latham & Watkins LLP

Latham is dedicated to working with clients to help them achieve their business goals and overcome legal challenges anywhere in the world. From a global platform spanning 14 countries, Latham lawyers help clients succeed

9 Raffles Place
#42-02 Republic Plaza
Singapore 048619
Tel: +65.6536.1161
Fax: +65.6536.1171

www.lw.com

Farhana Sharmeen
farhana.sharmeen@lw.com

Esther C. Franks
esther.franks@lw.com

Gen Huong Tans
genhuong.tan@lw.com