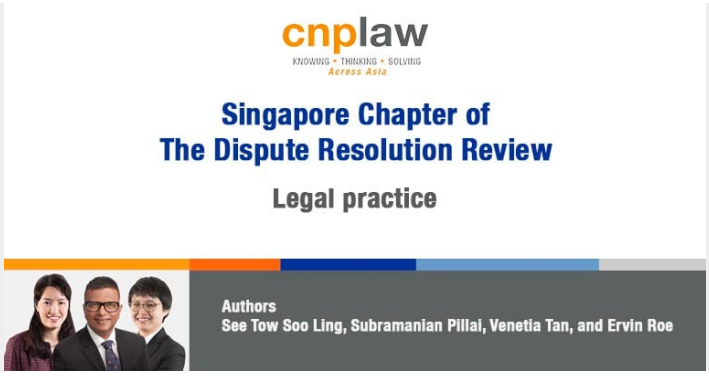
LEGAL PRACTICE

Posted on April 5, 2021



Category: Singapore Chapter of The Dispute Resolution Review

Authors and Contributors: See Tow Soo Ling, Subramanian Pillai, Venetia Tan, **Ervin Roe and Lim Shu-Yi.**

i. Conflicts of interest and Chinese walls

Legal practitioners are subject to the Legal Profession Act and the Legal Profession (Professional Conduct) Rules 2015. Duties of loyalty and confidentiality are owed to each of a solicitor's clients before, during and after his or her engagement.

Where a solicitor intends to act for two or more parties and a diversity of interests exists or may reasonably be expected to exist between them, he or she must communicate to the parties how their interests diverge or may diverge. Where one party may be disadvantaged in the transaction, the solicitor must explain that party's position before the transaction. Solicitors must advise each party to obtain independent legal advice. Otherwise, written confirmation or a record detailing that the party has declined independent legal advice must be sought and obtained.

Throughout the course of the retainer for the matter, the solicitor must be vigilant and inform each party of a conflict or potential conflict that arises. If the solicitor has difficulty dealing with a party's diverging interests, he or she must cease to act, unless he or she ceases to act for all other relevant parties and all other relevant parties have given their informed consent in writing for the solicitor to continue to act in the matter.

The court of three judges in *Law Society of Singapore v. Ezekiel Peter Latimer* set out guiding principles in cases involving conflicts of interest: misconduct arising from a conflict of interest is reprehensible because it entails a grievous violation of a lawyer's duty of unflinching and undivided loyalty to a client. This duty is a 'foundational responsibility on which the integrity of the legal profession and the public interest in securing proper legal representation depend'. In view of the trust and confidence that is reposed by a lay client in his or her solicitor, sanctions on misconduct are required to be imposed to uphold public confidence in the legal profession where there has been misconduct that tends to compromise the interests of a client. Three categories of conflicts were identified:

1. category 1 cases: where a solicitor has preferred his or her own interests over that of the client. The misconduct in such cases is presumptively more serious and deserving of a more severe sanction than the other categories of conflicts of interest;
2. category 2A cases: where a solicitor acts for multiple parties with diverging interests and prefers the interest of one party over another; and
3. category 2B cases: where a solicitor's concurrent representation of clients with conflicting interests would have given rise to a potential conflict of interests but the interests of either client would not in fact have been subordinated to those of the other.

Category 2A cases presumptively involve both greater harm and culpability than category 2B cases by virtue of the actual subordination and undermining of at least one client's interests.

ii. Money laundering, proceeds of crime and funds related to terrorism

There are several statutory provisions that impose an obligation on legal practitioners to protect against money laundering and financing of terrorism. Generally, where a legal practitioner knows or has reasonable

grounds to suspect that any property may be directly or indirectly connected to a criminal activity, or a client may be engaged in money laundering or the financing of terrorism, the legal practitioner is required to file a suspicious transaction report to the Suspicious Transaction Reporting Office as soon as reasonably practicable. The failure to make a suspicious transaction report may constitute an offence and disciplinary proceedings may be taken against the legal practitioner.
Legal practitioners are also required to perform customer due diligence measures as prescribed in the Legal Profession (Prevention of Money Laundering and Financing of Terrorism) Rules, such as identifying and verifying the identity of a client. Additionally, all documents relating to each matter and material obtained from customer due diligence measures must be kept for at least five years after the completion of the matter. The Council of the Law Society of Singapore has the powers to carry out an inspection either on its own motion or upon receiving a complaint, to ensure that the rules for prevention of money laundering and financing of terrorism are being complied with.

iii. Data protection
The Personal Data Protection Act 2012 (PDPA) is the main source of data protection law in Singapore. The scope of the PDPA is wide: it governs the collection, use and disclosure of individuals' personal data by organisations, including storage and processing of data. Personal data is defined as any data, whether accurate or not, about an individual who can be identified from that data, or from that data and other information to which the organisation has or is likely to have access, whether stored electronically or non-electronically.
Organisations are required to develop and implement policies and processes to meet the following obligations of the PDPA:

1. Under the consent obligation, an organisation may only collect, use or disclose personal data for purposes for which an individual has given his or her consent. The individual may withdraw his or her consent at any time with reasonable notice. An amendment to the PDPA was passed in November 2020 in response to Singapore's evolving digital economy needs. The amendment will provide exceptions to the consent obligation for local businesses to use consumer data without consent in advance for a limited number of purposes, including the use, collection or disclosure of data for legitimate interests and for business improvement. In addition, individuals who have provided personal data to an organisation for the purposes of entering into an agreement with the organisation will be deemed to have consented to the collection, use and disclosure of such personal data where it is reasonably necessary for the purposes of fulfilling the contract. The amendment also introduces 'deemed consent by notification': organisations may use or disclose personal data provided they have notified the individual of the new use of personal data, have provided the individual with a reasonable opt-out period and have conducted an assessment to determine that the new use is not likely to have an adverse effect on the individual.
2. Under the purpose limitation obligation, an organisation may collect, use or disclose personal data about an individual only for the purposes that a reasonable person would consider appropriate in the circumstances, and for which the individual has given consent.

3. Under the notification obligation, organisations are required to inform individuals of the purposes for which they are intending to collect, use or disclose their personal data on or before such collection, use or disclosure of personal data.
4. Under the access and correction obligation, organisations are required to provide upon request by an individual the personal data of that individual, and information about the ways in which his or her personal data has been or may have been used or disclosed by an organisation within a year of the date of the request.
5. Under the accuracy obligation, organisations are required to make a reasonable effort to ensure that personal data collected by them or on their behalf is accurate and complete if it is likely to be used by the organisation to make a decision that affects the individual to whom the personal data relates, or if it is likely to be disclosed to another organisation.
6. Under the protection obligation, organisations must protect personal data in their possession or under their control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks. Many breaches of the PDPA have involved organisations' ignorance of the protection obligation and the failure to take adequate or proactive steps to protect personal data.
7. Under the retention limitation obligation, organisations are required to cease to retain their documents containing personal data when it is reasonable to assume that the purpose for which that personal data was collected is no longer being served by retention of the personal data and retention is no longer necessary for legal or business purposes.
8. Under the transfer limitation obligation, if organisations are transferring personal data to a country or territory outside Singapore, they must do so in accordance with the requirements under the PDPA to ensure the standard of protection of the personal data will be comparable to that under the PDPA.
9. Under the openness obligation, organisations are to make information about their data protection policies, practices and complaints process available on request.

The PDPA also requires that every organisation designate an individual (known as the data protection officer) to oversee the practices and policies of the organisation, and who is responsible for ensuring that the organisation complies with the PDPA. The importance of the role of the data protection officer has been stressed by the Personal Data Protection Commission (PDPC); failure to appoint one is a breach of the PDPA.

Individuals have a right of private action against organisations that are in breach of the obligations in the PDPA, but enforcement of the PDPA is largely a complaint-based regime involving the PDPC's exercise of its powers conferred by the PDPA. If an organisation is found in breach of the PDPA, it may be fined up to S$1 million. The PDPC also has the power to make directions, give warnings, make advisory notices and accept undertakings from organisations to take a certain course of action.

The PDPA establishes the national Do Not Call Registry. Individuals may register their local telephone numbers to opt out of receiving telemarketing calls or text messages.

The main authority administering and enforcing the PDPA is the PDPC, which issues advisory guidelines to

supplement and aid the interpretation of the PDPA. Since September 2019, stricter guidelines were put in place to protect the personal data of Singaporeans. Organisations are barred from the collection, use and disclosure of National Registration Identity Card (NRIC) numbers, including collecting a full number or making a copy of an NRIC. Organisations may still legally request sight of an individual's NRIC to verify the person's age or identity, as long as no personal data is retained.

Table of Content