Data Protection Advisory

Dear Member,

In June 2019, the Personal Data Protection Commission ("PDPC") imposed a financial penalty of $8,000 on a law practice for, *inter alia*, the unauthorised disclosure of its clients' personal data. Briefly, the data breaches arose from the sending of e-mail correspondence meant for a client in a conveyancing transaction: (a) to an incorrect e-mail address; and (b) with an attachment containing the names of two other clients involved in an unrelated matter. The PDPC found that the law practice had not complied with the principles of Protection and Openness Obligations and contravened certain statutory provisions in conjunction with these principles under the Personal Data Protection Act ("PDPA").

This is the first reported PDPC decision involving a data breach by a law practice ("the PDPC's Decision"). It was an unfortunate and regrettable first for the legal profession. The Council of the Law Society, together with the Law Society's Cybersecurity and Data Protection Committee, would take this opportunity to remind you and your law practice of your PDPA compliance obligations and compliance with other relevant regimes on information security.

In particular, we would urge you and your law practice to take special note of the following salient learning points from the PDPC's Decision and, as a follow-up, implement such additional systems, policies and controls as may be reasonable to protect clients' personal data and its security adequately.

<u>Learning points from the PDPC's Decision</u>

1. **The management /owners of law practices are liable for their employees' acts and conduct**: The PDPC's Decision noted at [18] that under section 53(1) of the PDPA, a law practice is liable for the acts and conduct of its employees in relation to the unauthorised disclosure of its clients' personal data. This is also consistent with principles of vicarious liability. Hence, it is no answer for law practices to abdicate their own role via a wholesale delegation to their employees to carry out their duties diligently to safeguard against unauthorised disclosure of personal data. In this regard, law practices must implement reasonable security arrangements as required under section 24 of the PDPA "commensurate with the sensitivity of the data in question" (at [15]; see also point 3 below).

2. **Understand the duties of a Data Protection Officer**: Under section 11(3) of the PDPA, it is mandatory for a law practice to designate at least one individual to be the Data Protection Officer ("DPO") responsible for ensuring that the law practice complies with the PDPA. DPOs should undergo proper training and be the key contact point if a data breach is discovered. For more information on the duties of a DPO and how a DPO should be appointed, refer to the PDPC's Guide to Developing a Data Protection Management Programme (updated 22 May 2019).

3. **Identify and protect personal data that is of a sensitive nature**: Though the PDPA does not have a special or separate category of "sensitive" personal data, the case law confirms that that the PDPC will take a stricter view when considering a case where the personal data compromised is of a sensitive nature. A client's financial information, together with other identifying information, can constitute "sensitive" personal data. Disclosure of such data may expose the client to the risk of fraud and identity theft. In certain situations, personal data of a sensitive nature may be subject to a higher standard of protection: see [13]-[14] of the PDPC's Decision. That said, the PDPC recognised that "implementing additional checks and controls when handling sensitive personal data is not a mandatory requirement but one that should be adopted where appropriate" and that "[u]ltimately the facts of the case and the type of personal data being handled will influence whether or not the current checks and controls implemented in the particular organisation are sufficient": see [15] of the PDPC's Decision and also section 11(1) of the PDPA. On the facts narrated in the PDPC's Decision, the PDPC found that as the organisation in question was a law practice and its staff handling conveyancing matters handled personal data of a sensitive nature on a day-to-day basis, it was foreseeable that there were risks of inadvertent disclosure of such personal data and given the nature of the law practice's work, the law practice "ought to be subject to a higher level of care and responsibility for its clients' personal data": see [20] of the PDPC's Decision.

4. **Implement suitable checks and controls before sending out letters and e-mails containing personal data of a sensitive nature**: Accidentally or inadvertently sending letters and e-mails containing personal data to the wrong recipient is a major cause of data breaches. Refer to the PDPC's Guide to Preventing Accidental Disclosure When Processing and Sending Personal Data for suggested processes on how to prevent such accidental disclosures.

5. **Exercise vigilance and institute remedial measures quickly**: Law practices and their staff members should be vigilant in handling clients' personal data, especially if they handle large volumes of such data on a daily basis. Once a data breach has occurred, remedial measures should be put in place immediately to ensure no recurrence of the breach. Refer to the PDPC's Guide to Managing Data Breaches 2.0 (issued on 22 May 2019) for more information to consider when formulating a framework for managing and minimising data breaches, including reporting to the PDPC.

6. **Conduct data protection risk assessments**: Law practices should carry out risk assessment on specific departments that handle large volumes of personal data. Such assessments should help to identify and address the specific risks that exist in their operational processes and to put in place effective risk mitigation measures. Refer to the PDPC's Guide to Data Protection Impact Assessments for more information.

7. **Avoid using scrap paper containing personal data**: Law practices should have a system or process to segregate scrap paper containing personal data from other scrap paper that can be reused by staff. Law practices should avoid

using scrap paper containing personal data and exercise due diligence when using other reusable scrap paper to ensure that it does not contain personal data. As a matter of good practice, law practices should avoid using scrap papers when sending documents to clients. Refer to the PDPC's Guide to the Disposal of Personal Data on Physical Medium for more information.

8. **Provide clear written data protection policies for staff**: The PDPC's Decision noted at [23] that organisations should have some form of written data protection policy or practice in place, especially if complex processes are involved or the organisation frequently deals with personal data of a sensitive nature on a daily basis. Significantly, the PDPC noted (*ibid)* that "even if verbal briefings were indeed given, this in itself would not be sufficient for the Organisation to discharge its obligations under section 12 of the PDPA". A written policy would help reduce the risk of misunderstandings or miscommunication. The PDPC said that this could take the form of written standard operating procedures setting out how employees should deal with personal data (especially for complex processes) to prevent data protection breaches. Refer to the PDPC's Guide to Developing a Data Protection Management Programme (updated 22 May 2019) for more information on what a data protection policy should contain.

9. **Conduct data protection training sessions for all lawyers and staff, including senior management**: Training for lawyers and staff, including senior management, on data protection is a necessary aspect of protecting clients' personal data under section 53(2) of the PDPA. Indeed, the PDPC's Decision involved a mistake by the Managing Partner who was also the DPO of the law practice. As the PDPC reiterated in another recent PDPC decision, data protection training seeks to "inculcate the right employee culture and establish the right level of sensitivity to personal data amongst staff".[1] The PDPC's Guide to Developing a Data Protection Management Programme (updated 22 May 2019) contains useful tips for law practices on how to develop their training and communication initiatives, including the role of senior management in managing data protection risks.

10. **Speed and Manner of Response to Notice to Require Production of Documents and Information ("NTP") /Co-operate with the PDPC during investigations into a data breach**: Being implicated in a data breach is an unpleasant experience for any law practice. Should such a crisis eventuate however, it is important to co-operate with the PDPC during their investigations. Law practices issued with a NTP should respond to the PDPC speedily as the PDPC is empowered under section 50(2) read with paragraph 1 of the Ninth Schedule of the PDPA to demand information as part of their investigation. A failure to comply with the NTP may constitute an offence under section 51(3) read together with subsection (4) or (5) of the PDPA. On the facts narrated in the PDPC's Decision, two NTPs with deadlines were sent to the law practice, and the law practice failed to ask for an extension of time within the deadlines, let alone respond substantively. The investigating officer had to call the law practice to ask why it had failed to respond to the second NTP. Even though the investigating officer granted the law practice a further extension of time to respond, the law practice failed to comply with the new deadline. The investigating officer had to call the law practice again. This is clearly unacceptable. It is recommended that any law practice that requires an extension of time should inform the PDPC immediately. The PDPC takes into account the level of co-operation by the organisation in question in assessing the breach and determining the directions to be imposed.

This advisory only sets out the key learning points from the PDPC's Decision. You

should refer to the PDPC's website for detailed information on other measures that you and your law practice can take to ensure that your clients' personal data are adequately protected in specific circumstances. You should also keep up to date with relevant PDPC decisions to understand the PDPC's expectations of the reasonable security arrangements required under the PDPA to protect personal data.

Apart from data protection issues, as a practising lawyer, you should also keep in mind your legal duties of confidentiality, as well as your ethical obligations under the Legal Profession (Professional Conduct) Rules 2015, including but not limited to rules 5 (competence and diligence), 32 (responsibility for staff of law practice) and 35 (responsibilities in relation to management and operation of law practice).

To assist you in complying with your PDPA and other related obligations, the Law Society will conduct a seminar on cybersecurity, data breaches and business e-mail compromise on 30 September 2019 (2.30pm to 4.30pm). More details will be released in due course. We strongly encourage you to attend this seminar, so that you can raise your awareness of these issues and understand how to take appropriate measures to minimise the risks to your clients' personal data and confidential information.

The Council of the Law Society
12 July 2019

---

[1] *SLF Green Maid Agency* [2018] SGPDPC 27 at [12].