THE LAW SOCIETY OF SINGAPORE

LOCKTON

Professional Indemnity

Strictly for the internal use of The Law Society of Singapore members

Personal Data Protection – A Statutory Obligation

In the last issue of the Law Letter (July/September 2015), we looked at some of the risks associated with Information Technology. One of the risks dealt with was information security. In this issue, we will discuss security of client information in the context of the Personal Data Protection Act 2012 (the Act).

The Act governs the collection, use and disclosure of personal data by private organisations. The term "organisations" is defined to include any individual, company, association or body of persons, whether corporate or unincorporated. Accordingly, law firms structured as sole proprietorships, partnerships, law corporations or limited liability law partnerships, come within this definition. They must comply with the various obligations set out in the Act in relation to personal data of not only their clients but also of others such as their employees, clients' witnesses etc. We will look at these obligations in relation to clients, and how law firms can protect personal data in electronic medium.

Personal Data

"Personal data" means data, whether true or not, about an individual who can be identified from that data; or from that data and other information to which you have or are likely to have access. You are responsible for all personal data, whether in electronic or non electronic form which is in your possession or under your control (e.g. an outsourced entity).

As the provider of legal services, you routinely obtain personal particulars of your clients such as your clients' full name, NRIC number, residential address and contact telephone numbers. You may similarly obtain such particulars of your clients' witnesses. All these are now governed by the Act, because they are "personal data". Apart from your duty of client confidentiality, you now have to pay attention to and comply with the provisions in the Act regulating *inter alia* the collection, use and disclosure of personal data.

Your Core Obligations

There are three core obligations, linked to each other with which you must become familiar, if you have not already done so. These are set out below briefly.

Consent

The first and foremost obligation is consent. You must obtain the consent of your client before you collect, use or disclose his/her (henceforth for convenience we will use the masculine gender terms such as "he", "his", "him" as appropriate) personal data. The consent must be valid, which means you should notify the client of the purpose for which the same is required. In addition, the personal data you require must be reasonable.

Limitation of Purpose

You are allowed to collect, use or disclose your client's personal data provided you have informed him of the specific purpose in respect of the same. The purpose must be reasonable and appropriate.

Notification

Notification obligation is closely connected to purpose. You are required to notify your client about the purpose for which you are collecting, using or disclosing his personal data. Should there be other purposes, you must notify your client of the same. All purposes must be reasonable and lawful.

If it is necessary to disclose your client's personal data to another organisation (e.g. another law firm), you must inform your client about it.

Other Obligations

Access and Correction

Do take note that if your client requests access to his personal data in your possession or under your control, you must accede to it. Additionally, if the client asks you to correct any error or omission in his personal data, you must do so.

Accuracy

The Act also imposes on you the obligation to take reasonable efforts to ensure that the personal data you have collected is accurate and complete, if there is a likelihood of you using it to make a decision that affects the client; or if you are likely to disclose it to another organisation.

Retention

You should not keep your client's personal data after the purpose for which it was required has been completed. In this regard and including any other individual's personal data you have in your possession, you should be guided by the appropriate law/rules for retention of the same.

Protection Obligation

As mentioned earlier, you are responsible for the protection of personal data (electronic and non-electronic forms). The Act requires you to protect personal data in your possession or under your control by having in place security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks.

This is a critical obligation, especially where personal data is in electronic form. Law firms using information technology systems such as e-mails, computers, lap tops, mobile phones, memory sticks etc to record, store and disseminate personal data have a high risk of exposure to data breach because of the ease with which electronic information can be accessed either by staff or outsiders such as hackers.

Here are some basic security measures you can take to protect your client data in electronic form:

- Encrypt e-mails and mobile devices
- Install latest virus scanners and firewalls
- Install updates and patches (i.e. software designed to *inter alia* update a computer program including fixing security vulnerabilities)
- Allow limited access (i.e. give access only to those who need to know a particular client's data)
- Carry out a regular audit to determine any vulnerability including who is accessing what data
- Erase all personal data which is not required any more, with the appropriate software
- Do not discard any electronic device containing personal data before complete erasure of such data

Transfer outside Singapore

Personal data which may have to be transmitted outside of Singapore is also subject to the Act. If for instance, you handle a legal transaction with an overseas law firm, and you have to transfer your client's personal data to that law firm, you must ensure that the latter accords protection of comparable standards to that of the Act. You can fulfill this requirement by having a standard written contract containing the personal data provisions in the Act, and sending it over to the overseas party for its consent before transmitting your client's personal data.

Take note that this obligation also extends to any office you may have overseas. Having in place internal guidelines on personal data protection for compliance by all your offices will help compliance with this obligation.

Be Compliant

Get familiar with the Act, and take the necessary steps for compliance with its provisions. For this purpose, the Act requires you to appoint one or more persons with responsibility to ensure compliance. You must also have in place appropriate policies and practices to meet your obligations. The person you appoint must familiarise himself with the provisions of the Act, and any guidance that is or may be issued. You can also give that person the following tasks:

- Draw up a written data protection policy and ensure that all members of your law firm are aware of, understand and comply with it;
- Regularly audit your firm's use of personal data and check compliance;
- Proactively ensure that access and correction requests as well as other legitimate requests by data subjects are attended to in a timely manner.

Make sure that your data protection policy covers the following; and is made available to your data subjects:

- General principles of the Act
- Contact details of the person(s) responsible for compliance and the circumstances in which they should be contacted or consulted
- Procedures for dealing with both internal and external requests for access and correction of personal data
- Procedures for complaints – to whom complaints should be made and how they will be responded
- Your information security measures – that reasonable physical, technical and administrative security measures are in place to protect personal information from loss, misuse, alteration or destruction.

For the purpose of auditing your firm's use of personal data, it will be helpful if you keep the following information:

- Different categories of individuals (e.g. clients, employees) about whom you process personal information
- Whether you receive that information directly from the individuals concerned or indirectly through others
- Where do you keep the information (e.g. central data store, on local machines, in e-mail accounts etc.)
- Who has access to it, with whom is the information shared, and how it is used

Do not take your statutory responsibilities lightly. The Act confers on individuals the right to claim inter alia damages against you if you are in breach of your obligations. Further, certain breaches can amount to offences. For instance, if you hide or alter a client's data in order to evade his request for access to and/or correct it, you would be committing an offence.

Be Compliant!
Secure Personal Data!